Uspostava sustava neprekinutosti poslovanja, temeljem analize utjecaja na poslovanje (BIA)

Marinović, Dražen

SVEUČILIŠTE U ZAGREBU
FAKULTET ORGANIZACIJE I INFORMATIKE
VARAŽDIN

DRAŽEN MARINOVIĆ

USPOSTAVA NEPREKINUTOSTI POSLOVANJA, TEMELJEM ANALIZE UTJECAJA NA POSLOVANJE

- ZAVRŠNI SPECIJALISTIČKI RAD-

VARAŽDIN, 2017.

PODACI O ZAVRŠNOM RADU

I. Autor

Ime i prezime	Dražen Marinović
Datum i mjesto rođenja	23.04.1967. Zagreb, Republika Hrvatska
Naziv fakulteta i datum diplomiranja	Fakultet strojarstva i brodogradnje, Sveučilište u Zagrebu, 2006
Sadašnje zaposlenje	Agencija za plaćanja u poljoprivredi, ribarstvu i ruralnom razvoju, Sektor za informacijsko upravljanje

II. Završni rad

Naslov	USPOSTAVA SUSTAVA NEPREKINUTOSTI POSLOVANJA, TEMELJEM ANALIZE UTJECAJA NA POSLOVANJE (BIA)
Broj stranica, slika, tabela, priloga, bibliografskih podataka	138 stranica, 19 slika, 15 tablica, 20 bibliografskih podataka, 4 priloga
Znanstveno područje, smjer i disciplina iz koje je postignut akademski stupanj	Područje društvenih znanosti, polje informacijskih znanosti
Mentor ili voditelj rada	Prof.dr.sc. Zdravko Krakar
Fakultet na kojem je rad obranjen	Fakultet organizacija i informatike Varaždin
Oznaka i redni broj rada	19

III. Ocjena i obrana

Datum prihvaćanja teme od Znanstveno-nastavnog vijeća	16. listopada 2017. godine
Datum predaje rada	30. listopada 2017. godine
Datum sjednice ZNV-a na kojoj je prihvaćena pozitivna ocjena rada	12. prosinca 2017. godine
Sastav povjerenstva koje je rad ocijenilo	Prof.dr.sc. Željko Hutinski, predsjednik Prof.dr.sc. Zdravko Krakar, mentor i član Prof.dr.sc. Miroslav Bača, član
Datum obrane rada	9. siječnja 2018. godine
Sastav povjerenstva pred kojim je rad obranjen	Prof.dr.sc. Željko Hutinski, predsjednik Prof.dr.sc. Zdravko Krakar, mentor i član Prof.dr.sc. Miroslav Bača, član
Datum promocije	

SVEUČILIŠTE U ZAGREBU
FAKULTET ORGANIZACIJE I INFORMATIKE
VARAŽDIN

DRAŽEN MARINOVIĆ

USPOSTAVA SUSTAVA NEPREKINUTOSTI POSLOVANJA, TEMELJEM ANALIZE UTJECAJA NA POSLOVANJE (BIA)

- ZAVRŠNI SPECIJALISTIČKI RAD -

Mentor: prof. dr. sc. Zdravko Krakar

VARAŽDIN, 2017.

ZAHVALA:

Želim se zahvaliti prvenstveno supruzi Ireni i djeci na požrtvovnosti i strpljenju koje su mi nesebično pružili tijekom studiranja, cijenjenom profesoru Zdravku Krakaru, mojim kolegama i svim poslovnim suradnicima na razumijevanju, pomoći i potpori tijekom studiranja na poslijediplomskom specijalističkom studiju „Sigurnost i revizija informacijskih sustava“ na Fakultetu organizacije i informatike.

PREDGOVOR:

Vrlo značajno područje sigurnosti danas zauzimaju "Sustavi upravljanja neprekidnošću poslovanja" (BCMS - Business Continuity Management System). Prvenstvena namjena BCMS-a je osiguranje dostupnosti vitalnih poslovnih aktivnosti organizacije u slučajevima prekida većeg značaja, održavanjem vitalnih resursa potrebnih za odvijanje tih aktivnosti te osigurati pravovremen oporavak istih. Uspostava takvih sustava prvenstveno ovisi o prirodi i potrebama same organizacije i moguće ju je činiti na različite načine. Razvijene su i primjenjuju se niz normi za ovo područje. Ono što im je zajedničko jest prvi korak u uspostavi BCM sustava, a to je detaljno upoznati vlastiti poslovni sustav na osnovi kritičnosti njegovih poslovnih procesa. Ispravno određivanje prioriteta poslovnih procesa, njihove kritičnosti i utjecaja prekida njihovog odvijanja na poslovanje organizacije predmet je analize utjecaja na poslovanje (BIA – Business Impact Analysis). Ukoliko se na pogrešan način procijene kritičnosti poslovnih procesa, daljnji razvoj BCMS-a činit će se na krivim pretpostavkama i na samome kraju biti će pogrešan. Isto tako nema dvojbe da su u današnje vrijeme svi poslovni procesi, funkcije i aktivnosti postali izuzetno ovisni od neprekidnosti informacijsko-telekomunikacijske (ICT) potpore. Zbog toga je danas nužno izgraditi i odgovarajuće BCM sustave i za ovu potporu. U svijetlu ovisnosti poslovnih procesa o ICT potpori, zahtjev za neprekidnošću poslovnih procesa nužno nameće i potrebu za neprekidnošću same ICT potpore. Stoga je od presudnog značaja detaljno poznavati i razumjeti potrebu poslovnih procesa neke organizacije za neprekidnošću svih ICT servisa koji oni koriste.

Unatoč postajanju više različitih normi u području upravljanja neprekidnošću poslovanja, još uvijek postoji mnogo lutanja i nerazumijevanja samih zahtjeva i primjene u praksi. Razlog tome uglavnom jest što norme uglavnom propisuju „što treba napraviti“ ali ne i „kako to napraviti“. Ovaj rad je pokušaj doprinosu razumijevanju zahtjeva i ciljeva i olakšavanju praktične primjene provedbe analize utjecaja na poslovanje, primijenjene na informatičke servise. Analiza utjecaja na poslovanje provest će se na primjeru informatičkih servisa Agencije za plaćanje u poljoprivredi, ribarstvu i ruralnom razvoju (u daljnjem tekstu Agencija). Agenciju bih predstavio kao ustanovu javne uprave čija je osnovna zadaća provođenje procesa isplata potpora poljoprivrednicima, tvrtkama i drugim subjektima, te potpora korištenju financijskih fondova EU, temeljem zakonodavnog okvira koji se oblikuje kroz rad nadležnog Ministarstva. Poslovni sustav Agencije sastoji se od niza poslovnih procesa koji su u cijelosti podržani ICT-em. Eventualni prekidi u pružanju ICT potpore, uvjetuju velike smetnje, pa i zastoje poslovnih procesa Agencije što je nedopustivo sa stajališta isplata potpora i korištenja EU fondova. Baš to je razlog da EU komisija, kroz obvezujuće regulative nalaže usklađenost poslovanja Agencija sa jednom od normi koje se bave područjem ISMS-a (Information Security Management System) za države članice EU-a koje kroz sustav potpora u poljoprivredi i ruralnom razvoju isplaćuju potpore veće od 400.000.000 EUR na godišnjoj osnovi. Agencija je od svih raspoloživih normi izabrala usklađivanje sa normom ISO/IEC 27001 [1]. Spomenuta norma je logičan slijed pošto je Agencija od svojeg osnutka uređivala način poslovanja prema smjernicama ISO/IEC 27002 [2] naputaka. Upravo zbog toga, cilj istraživanja ovog završnog rada jest načiniti BIA analizu primijenjenu na informatičke servise ove jedinice javne uprave. Ukoliko se ne provede ova faza, nije moguće razviti niti konzistentan sustav ICT potpore ključnim poslovnim procesima

Agencije, a i rezultati provedene analize također su osnova za postavljanje cjelokupne BCM strategije.

Svrha rada je prvenstveno definirati metodu provedbe analize utjecaja na poslovanje. Ista je provedena na određenom podskupu informatičkih servisa Agencije s naglaskom na način prikupljanja i obrade a ne na detalje samih rezultata. Isto tako informacije koje se odnose na poslovanje Agencije, pa tako i same informacije o informatičkim servisima Agencije, iznesene su samo u dijelu koji je već poznat u javnosti ili na način da ne otkrivaju povjerljive poslovne informacije sukladno zahtjevima poslovanja i već prije primijenjenih preporuka temeljenih na ISO/IEC 27002 u poslovanju Agencije.

SADRŽAJ

POPIS KRATICA

BCI	Business Continuity Institute
BCM	Business Continuity Management
BCP	Business Continuity Plan
BC/DR	Business Continuity/Disaster Recovery
BIA	Business Impact Analyses
BP	British Petroleum
BSI	British Standards Institution
CMT	Crises Management Team
DRII	Disaster Recovery Institute International
ICT	Information Communication Technology
IMP	Incident Management Plan
IMT	Incident Management Team
IT	Information Technology
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
MVTI	Maksimalno vrijeme tolerancije ispada
NFPA	National Fire Protection Association
PAS	Publicly Available Specifications
PDCA	Plan-Do-Check-Act
RPO	Recovery Point Objective
SAN	Storage Area Network
SLA	Service Level Agreement

POPIS SLIKA

POPIS TABLICA

1 UVOD

1.1 Ciljevi rada

U kontekstu upravljanja kontinuitetom poslovanja pažnja je na događajima koji mogu uzrokovati prekide poslovanja. Pri tome su osnovni kriteriji vrednovanja trajanje prekida poslovanja i kritičnost poslovnih procesa. Ispravno određivanje prioriteta, kritičnosti, poslovnih funkcija za samo poslovanje i njihovih međuzavisnosti predmet je analize utjecaja na poslovanje i predstavlja ključnu aktivnost pri izradi plana neprekidnosti poslovanja. Predmet ovog završnog rada zato je upravo aktivnost analize utjecaja na poslovanja i za cilj ima jasno definirati jedan takav postupak koji je lako primjenjiv u praksi. Postupak analize utjecaja na poslovanje proveden je na informatičkim servisima. Kako danas informatička tehnologija prožima sve poslovne funkcije bilo koje kompanije, kritičnost poslovnih procesa možemo preslikati na informatičke servise koji podupire te poslovne procese i kroz plan neprekidnosti informatičkih servisa planirati dobrim dijelom i neprekidnost poslovanja.

1.2 Struktura rada

U prvom dijelu rada objašnjeno je što je to upravljanje neprekidnošću poslovanja, veze za sličnim procesima kao što su planiranje oporavka od katastrofe, upravljanje kriznim situacijama i upravljanje rizicima. Također je razmotrena potreba i stanje primjene upravljanja neprekidnošću poslovanja sa osvrtom na veliku ovisnost poslovanja o informacijskim sustavima.

U drugom dijelu su izložene osnovne aktivnosti procesa upravljanja neprekidnošću poslovanja te okviri i zahtjevi sukladno smjernicama o najboljoj praksi ISO 27002.

Središnji dio rada jeste detaljan opis načina provedbe analize utjecaja na poslovanje primijenjene na informatičke servise te s praktičnom primjenom na informatički sustav Agencije.

Završni dio rada bavi se mogućim odgovorom sukladno rezultatima BIA analize, te analizom samog postupka, ocjenom njegove primjenjivosti i efikasnosti te eventualnim slabostima.

2 STANJE SUSTAVA UPRAVLJANJA KONTINUITETOM POSLOVANJA

Opstanak svakog poslovanja ovisi o tome koliko smo spremni osigurati neprekidnosti osnovnih poslovnih aktivnosti i podupirućih servisa. Poslovanja širom svijeta suočavala su se sa različitim vrstama prekida uzrokovanih prirodnim ili ljudskim djelovanjem. Mnoge kompanije pogođene su razornim učincima učestalih razornih katastrofalnih prirodnih nepogoda kao na primjer uragana Irma i svih drugih sličnih inačica, sve češćim i razornijim terorističkim napadima po cijelome svijetu kao npr. 11.09. u SAD-u, izbijanjem ratnih stanja i sličnih neželjenih događanja. Neželjeni događaj je i epidemija, na primjer izbijanje gripe A (N1H1) također je još jednom prisililo kompanije širom svijeta da ozbiljno razmotre mnoge aspekte kontinuiteta poslovanja. Prekidi poslovanja uzrokovani ovim i drugim nepogodama su se brzo proširile preko lanaca opskrbe potresajući čitave industrije. Pored ovih kratkoročnih događaja s katastrofalnim posljedicama za poslovanje potrebno je sagledavati i dugoročne utjecaje kao što su promjene u financijskom tržištu, politička stabilnost, demografiju radne snage, navikama ponašanja kupaca i drugih koji neće trenutno, ali zasigurno kroz duže vrijeme utjecati na poslovanje s mogućim katastrofalnim posljedicama.

2.1 Pojam "Upravljanje kontinuitetom poslovanja"

Postoji niz definicija BCM-a. Jedna od njih kaže da je svrha upravljanja neprekidnošću poslovanja (BCM – Business Continuity Management) osigurati pravovremen oporavak i odvijanje ključnih poslovnih aktivnosti u slučaju prekida većeg značaja održavanjem ključnih resursa potrebnih za odvijanje tih aktivnosti. [1]

Osnovni proizvod upravljanja kontinuitetom poslovanja jeste plan kontinuiteta poslovanja (BCP – Business Continuity Plan) i predstavlja postupke kojima bi se trebali umanjiti određeni rizici poslovanja kompanije. Primjenjuje se prvenstveno kod pojave takvih događaja koji imaju za posljedicu značajne prekide poslovanja.

Prekidom poslovanja nazivamo svaku situaciju kad naše poslovanje ne raspolaže ili nema pristup resursima za normalno odvijanje. Prekidi poslovanja koji su u žarištu upravljanja kontinuitetom poslovanja jesu oni događaji koji uzrokuju značajne prekide ili gubitak ključnih poslovnih procesa što ima za posljedicu vrlo visok negativan utjecaj i ozbiljne posljedice za kompaniju i mogu se nazvati ispadima poslovanja. Značajan prekid poslovanja je jedan od neželjenih događaja kojim se narušava temeljno načelo svih informacijskih sustava a odnosi se na raspoloživost sustava ili dijelova samog sustava. Temeljna načela informacijskih sustava koja ne smiju biti narušena su povjerljivost, integritet i raspoloživost (tzv. PIR). [2]

P – Povjerljivost: je zaštita informacija kod koje je potrebno spriječiti otkrivanje informacija od strane neovlaštenih osoba ili sustava. Ukoliko se informacijama koje su označene kao povjerljive ne rukuje na pravilan način, može doći do povrede povjerljivosti, tj. otkrivanja povjerljivih informacija (usmenim putem, ispisom, kopiranjem, slanjem informacija e-poštom, itd.). Najčešće prijetnje povjerljivim informacija su:

- **napadači** - korištenjem sigurnosnih propusta pokušavaju otkriti povjerljive informacije, zbog vlastite koristi ili kako bi te informacije javno prikazali putem Interneta,
- **lažno predstavljanje** - dobivanje pristupa povjerljivim informacijama putem lozinke drugog korisnika,

- **neovlaštena aktivnost** - korisnik sustava koristi (mijenja, briše, kopira, itd.) podatke za koje nema ovlasti,
- **kopiranje podataka na nezaštićene** lokacije - ugrožavanje povjerljivosti pri kopiranju podataka na sustave s nedovoljnom razinom zaštite,
- **zlonamjerni programi** - programi kojima je moguće ostvariti pristup sustavu koji sadrži povjerljive podatke ili otuđiti povjerljive podatke.

Gubitak povjerljivosti - Neovlašteno, neočekivano ili nenamjerno otkrivanje ili objavljivanje podataka može rezultirati gubitkom povjerljivosti sustava i podataka. Gubitak povjerljivosti može dovesti do teških povreda važećih propisa te utjecati na gubitak povjerenja javnosti i narušavanje reputacije tvrtke, a može prouzročiti i pokretanje sudskog postupka protiv tvrtke.

I – Integritet: Očuvanje integriteta podataka znači da korisnik podatke ne može izmijeniti bez odobrenja, tj. da su podaci potpuni i ispravni. Od velike je važnosti zaštititi povjerljive podatke od neovlaštenih izmjena, jer se u velikim sustavima često mogu dogoditi namjerni ili nenamjerni slučajevi narušavanja integriteta podataka. Očuvanjem integriteta podataka osigurava se točnost i ispravnost tih podataka, npr. podataka o građanima, platnim listama, itd. Kako bi se očuvao integritet podataka u velikim sustavima, važno je utvrditi identitet korisnika nekom vrstom autentikacije (npr. jednokratnim lozinkama, pametnim karticama, biometrijskim čitačima, itd.).

Također, pri rukovanju podacima potrebno je obratiti oprez kako se ne bi dogodile slučajne izmjene u povjerljivim podacima. Međutim, oprez često nije dovoljan, stoga je potrebno kod rukovanja povjerljivim podacima osigurati strogo povjerljivu okolinu koja umanjuje mogućnost namjernih i nenamjernih izmjena.

Gubitak integriteta - Integritet sustava i podataka odnosi se na potrebu da informacije budu zaštićene od neovlaštenih ili neispravnih izmjena. Neovlaštene ili neispravne izmjene dovode do gubitka integriteta. Ako integritet sustava ili podataka nije ponovo uspostavljen, nastavak korištenja takvim sustavom ili podacima može dovesti do netočnosti, prijevara ili pogrešnih odluka. Isto tako, povreda integriteta može biti prvi korak u narušavanju raspoloživosti ili povjerljivosti sustava. Zbog tih razloga gubitak integriteta smanjuje povjerenje u informacijski sustav.

R – Raspoloživost: Kako bi informacijski sustav služio svojoj svrsi, sadržane informacije moraju u svakom trenutku biti raspoložive tj. dostupne. Dostupnost se može definirati kao jamstvo ovlaštenim korisnicima da će im informacijski sustav biti na raspolaganju kada ga imaju potrebu koristiti. Kako bi informacijski sustav bio dostupan u svakom trenutku podrazumijeva se ispravan rad:

- sustava za pohranu i obradu informacija,
- zaštitnog sustava i
- komunikacijskih veza putem kojih se pristupa informacijama.

Dostupnost informacija najčešće je upitna zbog:

- DoS napada (eng. Denial of Service attack) i
- gubitka mogućnosti obrade podataka.

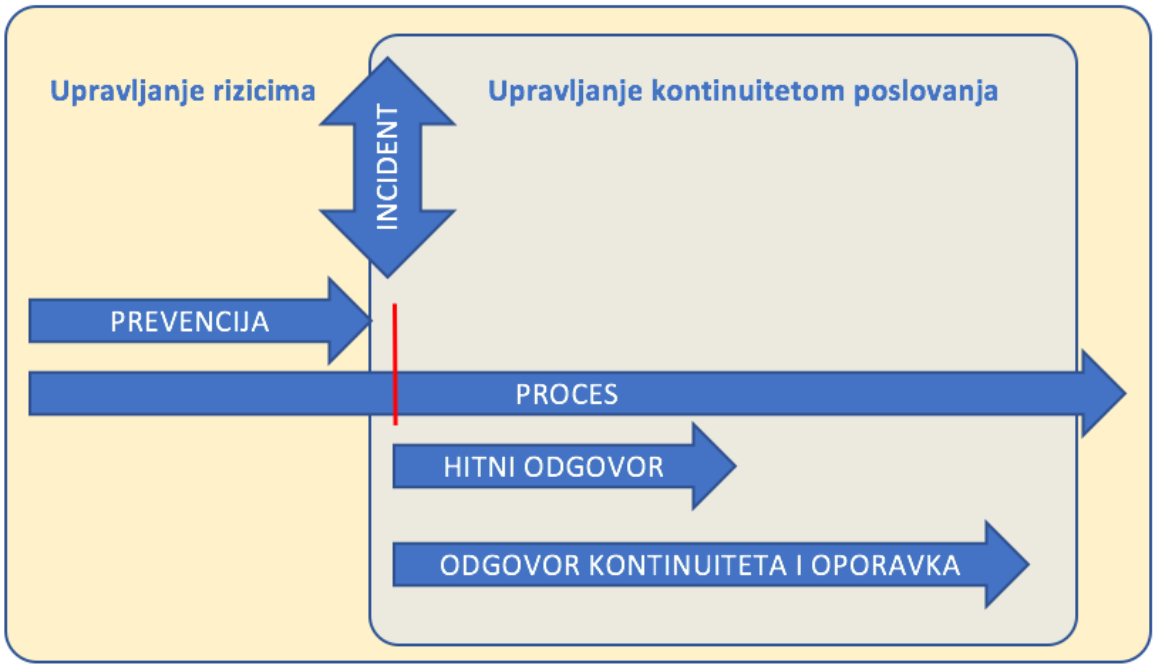
DoS napad, tj. napad uskraćivanjem usluge je svaki napad kojem je cilj onemogućiti korištenje poslužitelja ovlaštenim korisnicima. Jedan od načina DoS napada je da napadač pokušava onesposobiti informacijski sustav na način da sa velikog broja računala informacijskom sustavu šalje veliki broj zahtjeva, što onemogućava informacijski sustav da radi ispravno i ovlaštenim korisnicima onemogućava pristup podacima.

Gubitak raspoloživost - Neraspoloživost informacijskog sustava potrebnog za obavljanje zadatka može negativno utjecati na ciljeve banke i kontinuitet poslovanja te onemogućiti odvijanje vitalnih poslovnih procesa. Gubitak funkcionalnosti sustava i operativne djelotvornosti (učinkovitosti) može, primjerice, dovesti do narušavanja reputacije tvrtke, rezultirati gubitkom produktivnog vremena te onemogućiti krajnjeg korisnika u izvršavanju radnih zadataka.

Ispade je potrebno razlikovati od prekida poslovanja uzrokovanih zatajenjem opreme ili greškama koje se pojavljuju tokom redovnog pogona kao npr. kratkotrajni prekid komunikacijske veze koju je potrebno ponovno uspostaviti sa davateljem usluge. Koncept ispada uključuje pored vremenske dimenzije i dimenziju poslovnog procesa. Upravljanje kontinuitetom poslovanja uključuje utvrđivanje ukupnog maksimalnog vremenskog perioda za koju poslovna funkcija ili proces mogu biti prekinute prije nego ugrozi opstanak poslovanja kompanije. Ne bavi se toliko vjerojatnošću pojave određenog neželjenog događaja, već se više usredotočuje na posljedice. Vjerojatnost pojave događaja i

preventivne kontrole više su predmet upravljana rizicima. Upravljane kontinuitetom poslovanja daje odgovor na pitanje „Što će se desiti ako kontrole zakažu?“ i možemo reći da nadopunjuje proces upravljanja rizicima. Predstavlja aktivni preventivni pristup u kojem tvrtka osigurava kritične resurse kako bi osigurala da se kritične poslovne funkcije nastave odvijati nakon ispada poslovanja bilo koje vrste. Uvažava činjenicu da je rizik prisutan u svakoj odluci ili aktivnosti i da proporcionalno tim rizicima postoji mogućnost pojave prekida poslovanja te planira odgovor na pojavu tih prekida. Na slici br. 1 prikazan je položaj rizika i odgovora kontinuiteta poslovanja. Obično postoje tri opća odgovora u slučaju kriznih situacija koja možemo razlikovati, a zajedno čine upravljanje kontinuitetom poslovanja,

- ***hitni odgovor*** – To je odgovor na prekid koji obično uključuje zaštitu ljudi i imovine od izravne štete.
- ***odgovor kontinuiteta*** – To je odgovor osiguranja neophodnog minimuma procesa, mjera i resursa neposredno nakon prekida kako bi se omogućio nastavak odvijanja i isporuke kritičnih usluga i proizvoda,
- ***odgovor oporavka*** – To je odgovor ponovnog uspostavljanje procesa, mjera i resursa u mjeri koja će omogućiti normalno odvijanje poslovanja kao i prije prekida (business as usual).



Slika 1 - Odnos procesa upravljanja rizicima i upravljanja neprekidnošću poslovanja (Izvor[vlastiti rad])

U kontekstu upravljanja kontinuitetom poslovanja usredotočujemo se na utjecaje koje dovode do prekida poslovanja. Pri tome su osnovni kriteriji vrednovanja trajanje prekida poslovanja i kritičnost poslovnih procesa. Sustavni pristup upravljanju rizicima omogućuje razumijevanje rizika koji mogu dovesti do prekida poslovanja a plan kontinuiteta poslovanja može biti mjera za umanjenje utjecaja pojedinog rizika. Tako upravljanje rizicima i upravljanje kontinuitetom poslovanja možemo smatrati integriranim procesima gdje identifikacija, analiza i vrednovanje rizika predstavlja važan, prvi korak u razumijevanju rizika i određivanja opsega plana kontinuiteta poslovanja. [3]

2.2 Potreba za kontinuitetom poslovanja

Svake godine gotovo jedna od pet tvrtki u svijetu je pogođena raznim neželjenim događajima koji uzrokuju veće prekide poslovanja. Planiranje prevladavanja ovakvih situacija je široko prihvaćena praksa dobrog osjećaja vođenja poslovanja. Većina tvrtki već dugo razvija i održava planove za slučaj ostvarenja iznenadnih komercijalnih rizika koji uključuju događaje kao što su podbačaj kritičnih dobavljača, neočekivanih loših financijskih rezultata, pojave ozbiljne greške u proizvodu ili poslovnom procesu i slično.

Katastrofalni napad 11. rujna 2001. godine je pokazao da je i nakon događaja male vjerojatnosti pojavljivanja ali visokog utjecaja oporavak moguć. Iako su zgrade bile uništene i četvrti Menhattan-a pogođeni, tvrtke i institucije s dobrim i učinkovitim planovima neprekinutosti poslovanja su uspjele prebroditi taj katastrofalni događaj. Bombaški napadi u Londonu 2005. godine i mnogi drugi napadi slične vrste, također su dokaz da je terorizam stvarna i ozbiljna prijetnja. Terorizam ne mora biti uvijek fizičko razaranje, već može poprimiti oblik napada na vitalne informatičke i komunikacijske sustave uzrokujući prekide poslovanja i financijske gubitke, te gubitke u osoblju i osnovni mu je cilj uvesti opću nesigurnost u svakodnevni život. [4]

Planiranje kontinuiteta poslovanja (Business Continuity Planning) nije vođeno samo motivom rizika od terorizma već je korist od šireg značaja. Rizici uslijed promjena poslovnih procesa i tehnologija, katastrofalnih prirodnih nepogoda, pandemije i mnogi drugi, ukazuju na veću potrebu i pažnju za efikasnim planiranjem neprekidnosti poslovanja. Za ilustraciju ove tvrdnje vrlo dobro mogu poslužiti napadi na World Trade Center. U prvom, koji se dogodio 1993. godine, teroristi su postavili kamion-bombu ispod sjeverne kule s namjerom da sruše sjevernu kulu na južnu i tako razore obadvije zgrade. Iako plan nije uspio, došlo

je do velikog razaranja i požara koji su bjesnili u World Trade Center. Preko 44% organizacija ili tvrtki koje su bile smještene u zgradama prekinulo je svoje poslovanje barem privremeno, dok je 150 tvrtki od 350 potpuno prestalo poslovati. Nakon ovoga, mnoge tvrtke sa uredima u World Trade Center su razvile planove neprekidnosti poslovanja. Nakon napada 11.09.2001. godine, iako su mnoge kompanije ponovno potpuno prestale postojati, one tvrtke koje su imale detaljne planove neprekidnosti poslovanja su se oporavile i ponovo poslovale za samo nekoliko dana.

Brojni su razlozi za implementaciju plana neprekidnosti poslovanja među kojima najvažniji su slijedeći:

- Spašavanje života u trenutku kad, a ne ako, dođe do katastrofe,
- Opstanak kompanije ovisit će o postojanju, kvaliteti i uvježbanosti plana neprekidnosti poslovanja i samo je pitanje vremena kad će biti potrebno provoditi takve mjere,
- Predstavlja obavezu uvođenja minimalnog standarda brige i pripremljenosti prema svim interesnim grupama našeg poslovanja, tvrtkama, poljoprivrednicima i ostalim poslovnim partnerima,
- Vrlo često i sve više to je i zakonska obaveza i, bez planiranja neprekidnosti poslovanja, Agencija bi bila suočena sa kršenjem zakonskih obaveza, značajnim novčanim kaznama pa čak i gubitkom akreditacije za korištenje europskih financijskih fondova.
- To je način dobrog vođenja poslovanja i pomaže osiguranju isporuke usluga našim korisnicima, zaštiti zaposlenika te umanjuje financijske gubitke.

2.3 Stanje

Upravljanje neprekidnošću poslovanja kakvog danas poznajemo je, u stvari, proizašlo iz procesa koji je započeo ranih 1970-tih godina kao planiranje oporavka od katastrofe računalnih sustava a kasnijim razvojem se usredotočilo na poslovanje i upravljanje umjesto planiranje. U 1970-tima planovi oporavka od katastrofe su bili vođeni isključivo od računalnih stručnjaka. Tako je tim za planiranje kompanije Shell, među prvima razmotrio opasnost od gubitka kritičnih podataka pohranjenih na središnja računala i odlučio investirati u rješenja za osiguranje podataka na IT sustavima. U stvari, Shell je bio prvi komercijalni korisnik Iron Mountin kompanije za pohranu podataka na udaljenoj lokaciji što je začetak BC/DR tržišta kakvog danas poznajemo. Iako je tokom 1998-tih došlo do značajnijeg rasta komercijalnih lokacija za oporavak koje su nudile svoje usluge, naglasak je još uvijek bio na računalskim sustavima. Tek 1990-tih godina primjećuje se snažniji pomak od planova oporavka od katastrofe prvenstveno za računalske sustave prema planiranju neprekidnosti poslovanja i počeli su se razmatrati svi aspekti poslovanja. Danas je naglasak kod neprekidnosti poslovanja sa planiranja prešao na upravljanje čime postaje program, naglašavajući da je to neprekidan proces a ne zadatak ili projekt koji ima svoj početak i kraj.

Sve više organizacija pribjegava upravljanju neprekidnosti poslovanja i svjesne su ogromne količine rizika kojem su izložene ali istovremeno mnoge od njih ne ulažu napora koliko je potrebno. Nažalost, nije mnogo onih organizacija koje su svjesne važnosti neprekidnosti poslovanja. I pored događaja koji su pozivali na mobilizaciju kao što je 9/11 i mnogih drugih posljednjih godina još uvijek je u mnogim organizacijama prisutna apatija i nedostatak podrške najvišeg menadžmenta. Vrlo često su resursi i osoblje namijenjeni

upravljanju neprekidnosti poslovanja ograničeni, pogotovo u manjim organizacijama, i predmet su programa smanjenja troškova. Jedan od razloga je i taj što projekti planiranja neprekidnosti poslovanja nisu visoko profitabilni projekti pa samim tim nisu visoko pozicionirani u mnogim organizacijama sve dok ne dođe do katastrofe.

Ispravno je postaviti pitanje: Da li se mijenja mišljenje o važnosti BCM-a?

Suočeni sa valom terorističkih aktivnosti i učestalom pojavom katastrofalnih posljedica uzrokovanih vremenskim poremećajima, svakako se mijenja mišljenje uprava u organizacijama u cijelom svijetu. Podaci sa istraživanja provedenog na on-line na portalu ContinuityCentral.com, vezanim uz trendove i izazove uvođenja BCM-a bazirano na 2016 i 2017. godini idu u korist porasta broja organizacija koje će povećati ulaganja u cilju unaprjeđenja BCM-a.

- Demografski aspekt:

Primljen je 171 odgovor, pri čemu je većina (79,5 %) bila iz velikih organizacija (tvrtke s više od 250 zaposlenika). Najveći postotak ispitanika bio je iz Velike Britanije (36 %), a slijede ih Sjedinjene Države (32 %). Značajan broj odgovora također je primljen iz kontinentalne Europe (9 %), Kanade (6,5 %) i Australije (4 %).

- Očekivana razina promjena vezanih uz BCM:

Glavno pitanje: "Koliku razinu promjena očekujete u načinu na koji organizacija upravlja kontinuitetom poslovanja tijekom 2017. godine?"

- 19 % ispitanika očekuje da neće vidjeti promjene u načinu na koji njihova organizacija upravlja kontinuitetom poslovanja.

- 45 % očekuje male promjene, dok
- više od trećine (36 %) predviđa velike promjene.

Dio od 81 % ispitanika koji očekuju da će vidjeti promjene, trebalo je dati pojedinosti o jednom području koji će najvjerojatnije imati najveći utjecaj na praksu ili strategije kontinuiteta poslovanja unutar svoje organizacije. Iz odgovora na ovo pitanje vidljivi su različiti trendovi.

Zanimljivo je da pri izradi velikih revizija BCM strategija i / ili BCP-a, vrh popisa promjena koje menadžeri kontinuiteta poslovanja očekuju u 2017. godini, ovo područje je značajno smanjilo svoj udio od 9,5 % u odnosu na 13,3 % što je ostvareni rezultat tijekom 2016. godine. Implementacije softvera za kontinuitet poslovanja je visoko na popisu očekivanih promjena, a 9 % ispitanika navodi da će njihova organizacija raditi na tom području 2017. godine. 9 % ispitanika također očekuje da će se primijeniti nove tehnologije IT dostupnosti ili poslovanja u oblaku u 2017.

Najveći uspjeh na popisu očekivanih promjena u usporedbi s rezultatima za 2016. godinu, bio je u području normi kontinuiteta poslovanja. U 2016. godini samo 2,3 % ispitanika izjavilo je da očekuju veći fokus na certifikaciju ili usvajanje norme za kontinuitet poslovanja. Godine 2017. spomenuto se povećava na 8 %. [5]

Organizacije mogu poboljšati svoje izglede opstanka u poslovanju, ali samo ako poduzmu neophodne mjere prije i poslije nego što se katastrofa desi.“ [6]

Najčešći izgovori kao odgovor na potrebu uvođenja upravljanja neprekidnošću poslovanja od strane menadžmenta uglavnom su bili:

- To se neće nikad dogoditi nama,

- Nemoguće je planirati nepredviđeno,
- Ako nam se ne desi katastrofa, to je samo bacanje novca,
- Postoji toliko mnogo potencijalnih problema da je nemoguće imati efikasan plan za sve njih,
- Zar nam za takve slučajeve ne služi osiguranje,
- Nemamo vremena za takve stvari, postoje mnogo važnije stvari koje treba riješiti i slični.

Prije 11. rujna, potrebu za detaljnim planom neprekidnosti poslovanja bilo je uglavnom naglašavano od strane bilo vanjskih bilo unutrašnjih revizora, međutim nakon 11. rujna je dobilo mnogo više na važnosti. Kako su posebno teško u slučaju katastrofa pogađane osiguravajuće kuće, pored povećanja osiguravajućih premija počele su zahtijevati i dokaze ne samo o postojanju planova neprekidnosti poslovanja već i potvrdu da je uspostavljen proces s punom podrškom rukovodstva kompanije i da se planovi odgovarajuće testiraju. Kako je vrlo često prisutna predodžba da je implementacija planiranja neprekidnosti poslovanja izuzetno složena i skupa. Tako je pokrenuta gotovo čitava jedna nova industrija proizvođača IT rješenja i konzultantskih kompanija oko demistifikacije i olakšavanja implementacije planova neprekidnosti poslovanja ili oporavka od katastrofe. Pogotovo u posljednjem desetljeću došlo je do razvoja raznih tijela fokusiranih na ta područja kako na općoj razini tako i unutar pojedinih specifičnih grana industrije, regulativa i normi pa čak i uvođenja određenih zakonskih zahtijeva i implikacija u slučaju nepridržavanja. Većina organizacija koje su implementirala planove neprekidnosti poslovanja su upravo u visoko reguliranim granama industrije kao što su banke i ostali financijski sektori. Planiranje neprekidnosti poslovanja današnjih dana je vrlo ozbiljno poslovno područje kao što i treba biti.

3 OKVIR UPRAVLJANJA BCM-a

"U žarištu BCM-a jesu ključne poslovne funkcije i maksimalni vremenski period za koju poslovna funkcija ili proces mogu biti prekinute prije nego ugrozi opstanak poslovanja kompanije."

U svojoj naravi BCM je reaktivan jer se ne bavi toliko sprečavanjem određenog neželjenog događaja, već se više usredotočuje na posljedice i oporavak kritičnih funkcija kompanije u željenom vremenu nakon što se katastrofa dogodi. Plan neprekidnosti poslovanja razvija se kao odgovor za svaki neželjeni događaj visokog utjecaja bez obzira kako mala bila vjerojatnost njegove pojave i aktivira se tek nakon što se neželjeni događaj desi, tj. kad sve preventivne kontrole zakažu. [4]

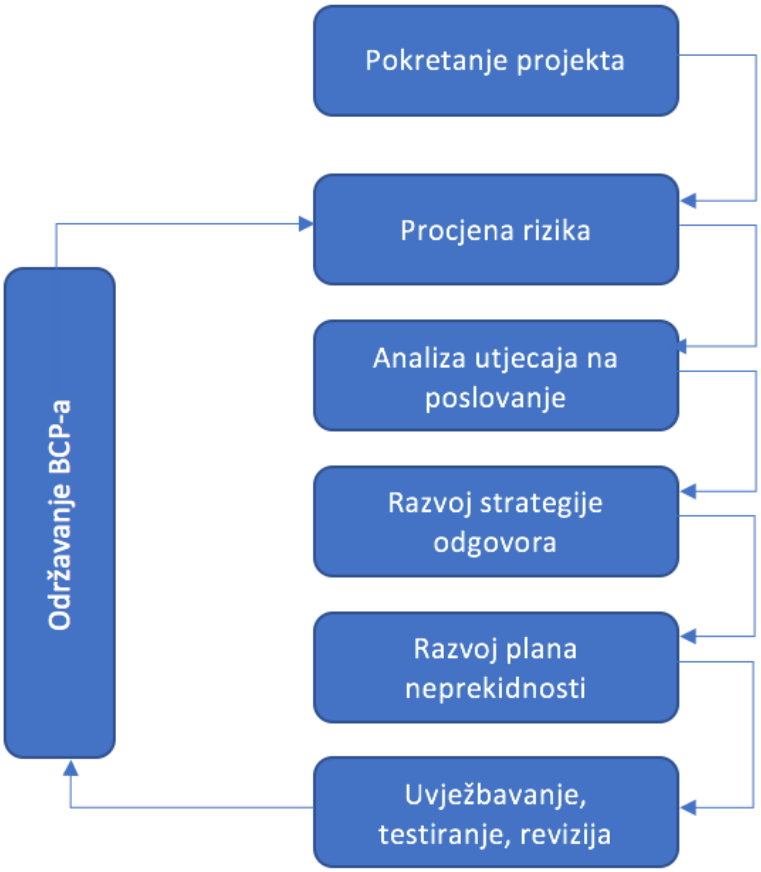
BCM je u osnovi proces planiranja čiji je cilj izraditi Plan i okolinu koja će osigurati neprekidnost i oporavak kritičnih poslovnih procesa/funkcija na ciljanu minimalnu razinu tj. u idealnom slučaju u obimu kao i prije ispada. Sam proces i konačni oblik plana neprekidnosti poslovanja ovise o potrebama i prirodi same organizacije i ova činjenica je ključna za planiranje neprekidnosti poslovanja. Da bi BCM ispravno funkcionirao važno je da je integriran u sve razine organizacije od najvišeg rukovodstva (podrške, postavljanja okvira i ciljeva, osiguranje resursa ...) do svakog pojedinog radnika kroz obuke i programe podizanja svijesti o njegovoj važnosti. [5]

3.1 Planiranje

Efikasno planiranje neprekidnosti poslovanja jest kritičan čimbenik u osiguranju da će se vitalne funkcije poslovanja nastaviti i u slučaju ostvarenja rizika s katastrofalnim posljedicama. Planiranje kontinuiteta poslovanja za cilj ima:

- osigurati održanje najviše moguće razine usluge,
- osigurati što je brže moguće oporavak poslovanja nakon prekida,
- svesti na najmanju moguću mjeru vjerojatnost pojave kao i negativan utjecaj prekida poslovanja

Planiranje kontinuiteta poslovanja jest upravljački sustav/proces koji omogućava organizaciji efikasan odgovor i oporavak ključnih poslovnih procesa u slučaju njihovog iznenadnog i neželjenog prekida.



Slika 2 - Proces planiranja kontinuiteta poslovanja (Izvor [vlastiti rad prema [9]])

Aktivnosti procesa planiranja kontinuiteta poslovanja, danas uglavnom prihvaćeni u svijetu, prikazani su na slici 2. Kako su u središtu planiranja kontinuiteta poslovanja ključni poslovni procesi tj. oni poslovni procesi čiji prekid potencijalno onemogućava normalno poslovanje i ugrožava opstanak tvrtke/organizacije, prva aktivnost jest utvrditi koji su to poslovni procesi. Aktivnost kojom se utvrđuje kritičnost pojedinih poslovnih procesa za poslovanje organizacije/tvrtke jest Analiza utjecaja na poslovanje (Business Impact Analysis). [9]

3.2 Norme za upravljanje kontinuitetom poslovanja

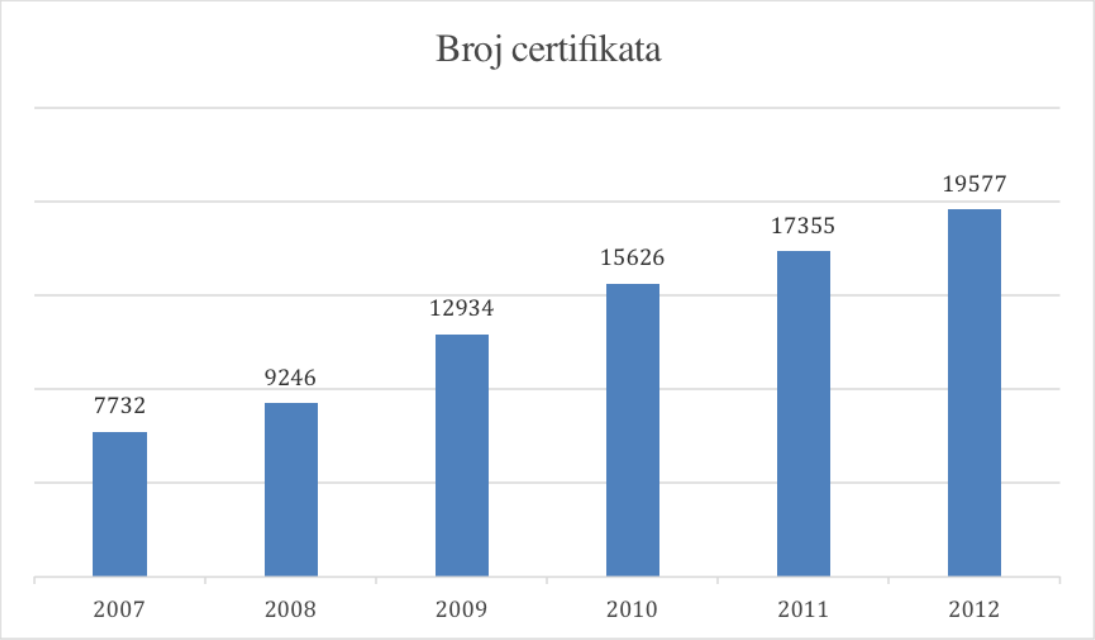
Unatoč evidentnoj potrebi i svim nabrojenim pogodnostima koje donosi BCM, primjena i efikasnost su često bili ometani nedostatkom jasnih smjernica za uspostavu procesa potrebnog za implementaciju učinkovite BCM strategije. Kao odgovor na potrebu za odgovarajućom metodologijom koja će osigurati okvir i strukturu kod uspostave BCM-a, razvijene su brojne smjernice i norme. Prvi zadatak im je definirati koncept BCM-a kao i značenje korištenih termina. Uloga norme je i u tome što omogućuju dosljedniji pristup implementaciji BCM-a, odgovore na regulatorne zahtjeve i zahtjeve tržišta kao i vrednovanje efikasnosti sposobnosti organizacije da svede na minimum utjecaj bilo kojeg većeg incidenta odnosno ispada. Neki od značajnijih raspoloživih smjernica i normi su:

- BSI (British Standard Institute): Objavio je 2003. godine „PAS 56:2003 Guide to business continuity management“ na čemu će se temeljiti BS 25999 norma.
- BCI (British Continuity Institute): Objavio je 2005. godine „Good Practice Guidelines – A Framework for Business Continuity Management“.
- DRII (Disaster Recovery Institute International): Objavio je 2012. godine „Professional Practices for Business Continuity Practitioners“
- 2004. godine u Australiji je objavljen od strane Standards Australia „HB 221:2004 Business Continuity Guidelines“ koji je 2006. godine nakon provedene rasprave i preispitivanja postao „HB 292 A Practitioners Guide to Business Continuity Management“
- „NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs“ u Sjedinjenim američkim državama postoji već duže vrijeme.

- BSI (British Standard Institute): BS 25999-1/2 (2007) – predstavlja osnovu za razumijevanje, razvoj i implementaciju neprekidnosti poslovanja.
- ISO (International Organization for Standardization): ISO/IEC 22301:2012 – nedavno objavljen, svibanj 2012., i zasnovan je na BS 25999-1/2. Zamijenio je BS 25999 normu. Prihvaćen u cijelom svijetu (u 163 zemlje).
- ISO (International Organization for Standardization): 27001 je međunarodni standard objavljen od strane Međunarodne Organizacije za Standardizacije (ISO) i opisuje kako upravljati informacijskom sigurnošću u tvrtkama. Najnovija inačica ove norme je objavljena 2013. godine, te je sadašnji puni naziv ISO/IEC 27001:2013. Prva revizija norme je objavljena 2005. godine a razvijena je na temelju britanske norme BS 7799-2.

Pored nabrojenih raspoložive su i mnoge druge norme i smjernice, bilo međunarodne, nacionalne ili granske.

ISO 27001 je postao najpopularnija norma informacijske sigurnosti u svijetu, te su mnoge kompanije certificirane prema njemu. Na slici 3. vidljiv je trend porasta broja organizacija koje su se odlučile za implementaciju sigurnosti prema ovoj normi.



Slika 3 - Udio ISO/IEC 27001 (Izvor: [12])

Danas je ISO/IEC 22301:2012 vrlo zastupljena i opće prihvaćena norma nastala kao odgovor na zahtjeve tržišta, kako javnog tako i privatnog sektora, za formalnom normom koji će omogućiti konzistentnost, jasno definirati što sačinjava BCM, uspostaviti terminologiju i definicije te omogućiti vrednovanje i usporedbu među organizacijama, industrijama i regijama. Objavljen je 2012 godine pod nazivom „ISO/IEC 22301:2012 - Societal security -- Business continuity management systems --- Requirements“ od strane International Organization for Standardization.

Norma ISO/IEC 22301:2012 određuje skup zahtjeva za planiranjem, uspostavom, implementacijom, nadzorom, održavanjem i neprekidnim unaprjeđivanjem dokumentiranog sustava upravljanja kako bi se zaštitili, umanjili mogućnost nastanka prekida poslovanja, bili pripremljeni za isti i spremni na reakciju i povrat na normalno poslovanje nakon rješavanja uzroka prekida. Zahtjevi pobrojani u spomenutoj normi su općeniti i namjera je

da budu primjenjivi na sve vrste organizacija, bez obzira na vrstu, veličinu ili prirodu organizacije. Prilagođavanje i primjena zahtjeva ovisi o poslovnoj okolini i samoj složenosti organizacije. *(Izvor* [13]*)*

3.3 Plan kontinuiteta poslovanja

Osnovna ideja kontinuiteta poslovanja jest sačiniti upravljački sustav koji omogućuje organizaciji efikasan odgovor i oporavak ključnih poslovnih procesa u slučaju njihovog iznenadnog i neželjenog prekida. [14]

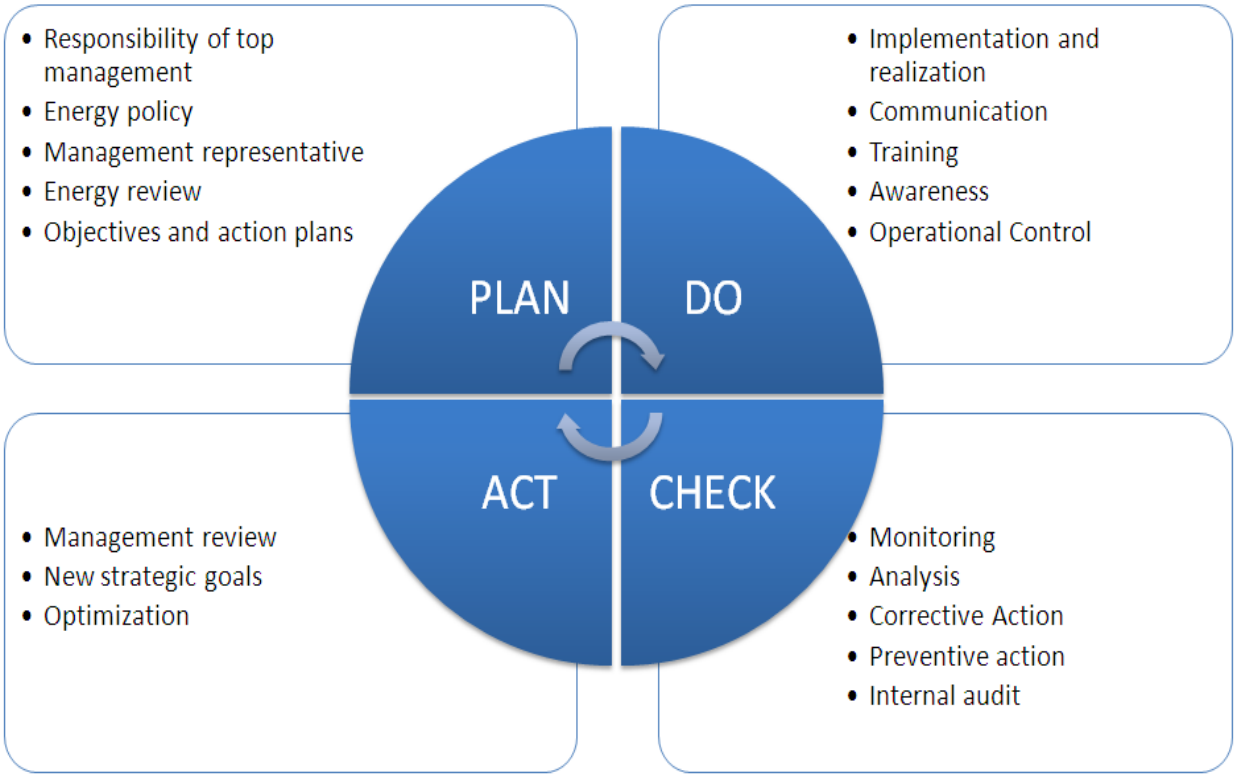
Svrha plana kontinuiteta poslovanja je uspostava sustava nadležnosti i odgovornosti te određivanje postupaka koji se izvršavaju u slučaju proglašenja katastrofe. Katastrofa se proglašava kada je situacija na terenu takva da je nemoguće obnoviti minimalnu funkcionalnost poslovnih procesa unutar utvrđenog RTO-a (engl. Recovery Time Objective) te je potrebno započeti obnovu na sekundarnoj lokaciji. Plan može biti primijenjen neovisno o vrsti i uzroku incidenta, stupnju oštećenja odnosno vremenu koje će biti potrebno za povratak primarne lokacije u normalno stanje i sličnim čimbenicima.

Cilj plana je osiguravanje kontinuiteta poslovanja odnosno opstanka tvrtke u slučaju incidenta koji je ozbiljnije ugrožava, a samim time i dugoročne dobrobiti njenih radnike. Navedeni se cilj postiže obnovom ključnih poslovnih procesa u što kraćem vremenu po proglašenju katastrofe.

Sve strane uključene u proces upravljanja kontinuitetom poslovanja moraju biti upoznate s odredbama ovog dokumenta te se isti mora ažurirati na redovnoj bazi. Plan kontinuiteta poslovanja ima za cilj organizirati održavanje osnovnih funkcija Agencije. Efikasnim upravljanjem kontinuitetom poslovanja Agencije definira aktivnosti potrebne za

nastavak odvijanja svojih poslovnih procesa te time smanjuje utjecaj katastrofalnog događaja na svoje poslovanje.

Osiguranje kontinuiteta poslovanja, predstavlja univerzalni standard koji se može primijeniti u svim vrstama organizacija bez obzira na veličinu ili područje poslovanja. Zahtjeva implementaciju u skladu s PDCA modelom (**P**lan-**D**o-**C**heck-**A**ct) koji se zasniva na ideji nesavršenosti i zbog toga slijedi neprekidni proces unapređivanja, kao što je prikazano na slici 4.



Slika 4 - Plan Do Check Act (Izvor [[15]])

Norme iz djelokruga BCM, određuju BCM kao:

„Potpun upravljački proces koji identificira potencijalne prijetnje organizaciji i utjecaje na poslovanje koje ove prijetnje, u slučaju ostvarenja, mogu uzrokovati i osigurava okvir za izgradnju otpornosti organizacije kroz sposobnost efektivnog odgovora koji štiti interese njenih ključnih interesnih skupina, ugled, prepoznatljivost i aktivnosti kreiranja vrijednosti.“

Stavlja ga se u kontekst strateških ciljeva organizacije na način da posljedice incidenata mogu biti dalekosežne i uzrokovati gubitke života, resursa i prihoda kao i nemogućnost isporuke proizvoda i usluga na čemu se u stvari zasniva strategija kao i opstanak organizacije. Zato BCM mora biti u stanju prepoznati strateške važnosti interesnih skupina organizacije i usredotočiti se na njih.

Kao što je vidljivo i iz same definicije BCM-a koja zahtijeva identifikaciju potencijalnih prijetnji i utjecaja, BCM je usko povezan sa procesom upravljanja rizikom. ISO/IEC 22301:2012 smatra BCM komplementarnim procesu upravljanja rizicima s tim da se BCM usredotočuje na posljedice prekida poslovanja i na taj način identificira proizvode i usluge o kojima ovisi opstanak organizacije.

Prekid poslovanja definiran je kao: „Događaj, bilo očekivan (npr. organizirani prekid rada ili oluja) ili ne (npr. teroristički napad ili zemljotres), koji uzrokuje neplanirano, negativno odstupanje isporuke proizvoda ili usluga od očekivanog prema ciljevima organizacije.

Osnovna postignuća BCM-a bi trebala biti:

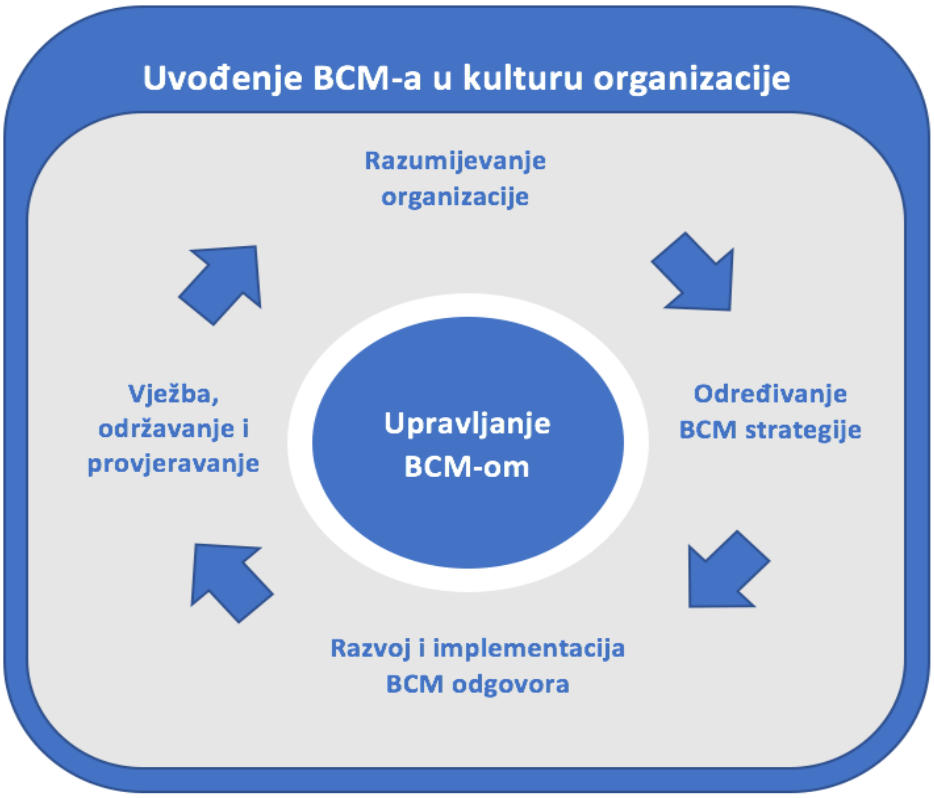
- **Povećanje otpornosti** – „proaktivno povećava otpornost organizacije na prekide i njene sposobnosti da postigne svoje ključne ciljeve“

- **Obnavljanje sposobnosti isporuke proizvoda i usluga** – „osigurava uvježbanu metodu obnove sposobnosti organizacije da isporučuje svoje ključne proizvode i usluge na ugovorenoj razini unutar ugovorenog vremena nakon prekida“
- **Upravljanje prekidima poslovanja** – „osigurava dokazanu sposobnost upravljanja prekidima i štiti ugled i prepoznatljivost organizacije“

3.3.1 Elementi životnog ciklusa BCM-a

BCM, sukladno svakoj normi iz BCM djelokruga, mora biti uspostavljen kao dio kulture organizacije. Važno je da ima snažnu podršku najviše razine upravljanja i da ciljevi i svijest o važnosti budu iskomunicirani na svim razinama organizacije. Stoga je inicijalni korak u uspostavi BCM-a razvoj Politike BCM-a. Politika ima za cilj osigurati odobrenje i opredijeljenost uprave, navesti ciljeve BCM-a i dokumentirati načela kojima je potrebno težiti i pomoću kojih će se sposobnost neprekidnosti poslovanja vrednovati kao i definirati okvir i sredstva. Mora biti donesena od strane visoke razine upravljanja kompanijom, redovno provjeravana i usklađivana s potrebama organizacije.

Životni ciklus BCM-a sastoji se od šest elemenata. Elementi životnog ciklusa BCM-a prikazani su na slici 5.



Slika 5 - Elementi životnog ciklusa BCM-a (Izvor vlastiti rad prema [3])

3.3.1.1 Program BCM-a

U središtu životnog ciklusa BCM-a jeste upravljanje programom BCM-a. Zadatak programa jeste osmisliti i provesti uspostavu i održavanje neprekidnosti poslovanja. Mora biti postavljen tako da omogući ostvarenje ciljeva definiranih Politikom, definira pristup organizacije neprekidnosti poslovanja i osigura ispravno uvođenje procesa BCM-a, odgovarajuću potporu i integraciju u kulturu organizacije. Uključuje tri osnovna koraka;

Dodjelu zaduženja – podrazumijeva uspostavu sustava ovlasti i odgovornosti za uspostavu i implementaciju BCM programa. Nužno ja da osoba ili tijelo, ovisno o veličini organizacije, zadužena za implementaciju ima odgovarajuće ovlasti i sveopću odgovornost za BCM i stalnu uspješnost ove sposobnosti. Uloge, ovlasti i odgovornosti moraju biti

sastavni dio opisa radnog mjesta i potrebnih znanja i vještina te ih je potrebno stalno revidirati kroz proces revizije organizacije.

Implementaciju neprekidnosti poslovanja u organizaciji – uključuje konstrukciju, izgradnju i implementaciju programa. U ovom dijelu potrebno je program predstaviti svim sudionicima, organizirati edukacije zaposlenih kao i uvježbavati sposobnost očuvanja neprekidnosti poslovanja.

Neprekidno upravljanje neprekidnošću poslovanja integriranog u kulturu organizacije – mora osigurati da je neprekidnost poslovanja sastavni dio aktivnosti poslovanja. Sposobnost očuvanja neprekidnosti poslovanja mora biti redovito provjeravana, uvježbavana i ažurirana naročito nakon značajnijih promjena radnih procesa, osoblja ili tehnologije a pogotovo nakon uočenih nedostataka.

3.3.1.2 Razumijevanje organizacije

Kako su u fokusu BCM-a upravo ključni proizvodi i usluge kao i ključne aktivnosti i resursi koji ih podupiru, ovaj element BCM-a jest prvi korak u uspostavi BCM sustava, a to je detaljno upoznati vlastiti poslovni sustav sa stajališta kritičnosti njegovih poslovnih procesa. Stoga je od presudnog značaja razumjeti potrebu poslovnih procesa neke organizacije za neprekidnošću, ispravno određivanje prioriteta, njihove kritičnosti i međuzavisnosti. Ukoliko se na krivi način procijene kritičnosti poslovnih procesa, daljnji razvoj BCM sustava činit će se na krivim pretpostavkama i u konačnici biti će neodgovarajući. Ovaj element osigurava da je BCM usklađen sa ciljevima i obavezama, kako poslovnim tako i zakonskim, same organizacije.

Za razumijevanje organizacije potrebno je identificirati ciljeve organizacije, obaveze sudionika, zakonske obaveze kao i okolinu u kojoj organizacija djeluje. Također je potrebno

identificirati kritične proizvode i usluge organizacije kao i aktivnosti i resursa koji ih podupiru. Potrebno je znati i međuzavisnosti ovih aktivnosti, kao i njihovu ovisnost o vanjskim organizacijama i ovisnost vanjskih organizacija o njima. Slijedeći korak jeste procjena utjecaja ukoliko ove aktivnosti i resursi zakažu te identifikacija prijetnji koje mogu uzrokovati ispade.

3.3.1.2.1 Analiza utjecaja na poslovanje (BIA)

Analizom utjecaja prekida ključnih poslovnih procesa na poslovanje (engl. Business Impact Analysis – BIA) Agencije utvrđeni su prioriteti obnove poslovnih procesa. Kroz BIA upitnike dokumentiraju su kritični resursi za pružanje ključnih poslovnih procesa:

- maksimalno prihvatljivo vrijeme obnove (RTO) i
- dopuštena starost podataka koji se koriste prilikom obnove (RPO).

3.3.1.2.2 Prepoznavanje kritičnih aktivnosti

Sukladno provedenoj BIA analizi, aktivnosti s najvećim utjecajem u najkraćem vremenu smatrat će se ***kritičnima***. Upravo su to one aktivnosti na koje se organizacija mora usredotočiti. Također je važno da se identificiraju kao kritične i one aktivnosti koje su preduvjet za izvršavanje identificiranih kritičnih aktivnosti.

3.3.1.2.3 Zahtjevi neprekidnosti

Za svaku aktivnost potrebno je odrediti resurse potrebne za njenu ponovnu obnovu od prostora za rad, ljudskih, tehnoloških, informacija i dokumentacija, vanjskih usluga i dobavljača itd.

3.3.1.2.4 Procjena rizika

Od organizacije se zahtjeva da bude svjesna rizika ispada kritičnih aktivnosti. Kako kritične aktivnosti zahtijevaju određene resurse za svoje odvijanje kao što su prostorije, ljudi, tehnologije i sl. potrebno je utvrditi i razumjeti prijetnje kojima su izloženi ovi resursi. Način procjene rizika nije propisan normom ISO/IEC 22301:2012, već se stavlja na volju organizaciji.

Na temelju provedene analize utjecaja na poslovanje i procjene rizika, potrebno je odrediti mjere koje će bilo smanjiti vjerojatnost ispada, skratiti vrijeme trajanja ispada ili ograničiti utjecaj ispada na ključne proizvode i usluge.

3.3.1.3 Određivanje strategije neprekidnosti poslovanja

Na osnovu analize provedene u prethodnom koraku, organizacija bi trebala biti u stanju odrediti strategiju neprekidnosti poslovanja koja bi zadovoljavala njene ciljeve. Osnovni kriteriji za određivanje strategije su maksimalno vrijeme ispada kritične aktivnosti koje se može tolerirati, cijena implementacije strategije i posljedice ukoliko se ništa ne poduzme. Strategiju je potrebno razviti za sve resurse koje podupiru odvijanje kritične aktivnosti. Primjer mogućih strategija npr. za neophodne ljudske resurse za odvijanje kritične aktivnosti mogu biti od održavanja detaljne operativne dokumentacije za provođenje aktivnosti, preko edukacije osoblja za obavljanje više poslovnih aktivnosti do korištenja vanjskih partnera ili kombinacija navedenog. Na sličan način potrebno je odrediti strategije i za ostale resurse. Pri određivanju strategija potrebno je voditi računa i o zaštiti interesa ključnih sudionika kao što su dobavljači roba i usluga i ugovorne strane, a također je potrebno uzeti u obzir i socijalna i kulturna obilježja.

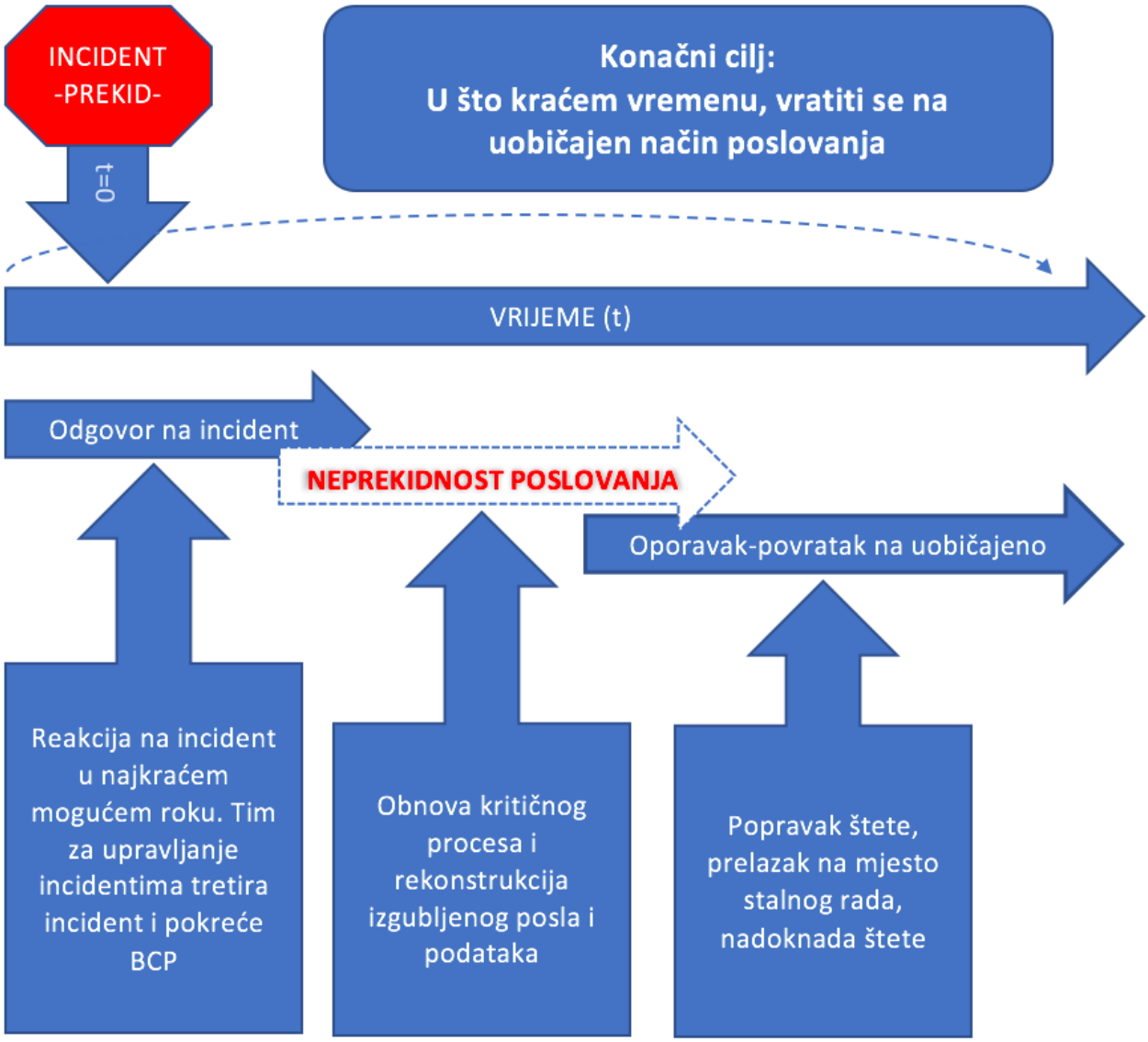
Na koncu, odabrane strategije moraju biti dokumentirane i potpisane od strane uprave organizacije i na taj način odobrene i prihvaćene.

3.3.1.4 Razvoj i implementacija BCM odgovora

U ovom dijelu potrebno je ustrojiti način odgovora na incidente, tj. za svaku incidentnu situaciju biti u stanju brzo i jednostavno uspostaviti strukturu koja će moći ocijeniti prirodu i razmjere incidenta, preuzeti kontrolu nad incidentom te inicirati odgovarajući odgovor u svrhu neprekidnosti poslovanja. Ova struktura se naziva tim za upravljanje incidentima (IMT) ili tim za upravljanje kriznim situacijama (CMT). Na slici 6 su prikazane faze odgovora na incidente tokom vremena i odnos između odgovora na incident i neprekidnosti poslovanja.

Organizacije mogu razviti konkretne planove da obnove aktivnosti ponovo na normalnu razinu. Bilo da se radi o planovima upravljanja incidentima , planovima neprekidnosti poslovanja ili planovima oporavka od katastrofe, planovi moraju biti jasni i lako dostupni. Tako razvijeni planovi moraju jasno definirati svrhu i obuhvat, kritične aktivnosti koje se obnavljaju i u kom vremenskom okviru, razinu aktivnosti koju je potrebno uspostaviti i za koje situacije se plan koristi. Uloge i odgovornosti kao i osobe i grupe obuhvaćeni planom moraju biti jasno definirane i dokumentirane.

Planovi upravljanja incidentima (IMP – Incident Management Plans) imaju zadatak dokumentirati postupanje u inicijalnoj fazi incidenta. Moraju sadržavati popis zadataka i aktivnosti, informacije o načinu



Slika 6 - Upravljanje incidentima i neprekidnost poslovanja (Izvor vlastiti rad prema [3])

komuniciranja u hitnim situacijama, načine i lokacije evakuacije, zaduženja i načine komuniciranja s javnošću, uspostavu prioriteta i komunikaciju s interesnim stranama. Dio

planova mogu biti i karte, skice, fotografije kao i sve ostale informacije koje mogu biti značajne za prirodu incidenta.

Planovi neprekidnosti poslovanja (BCP – Business Continuity Plan) imaju za cilj dokumentirati postupanje oporavka aktivnosti organizacije u slučaju prekida na normalnu razinu poslovanja. Također moraju sadržavati popis zadataka i aktivnosti, način i odgovornost za pokretanje plana neprekidnosti poslovanja, resurse potrebne za obnovu poslovanja, kako mobilizirati interne i eksterne resurse, upravljane i komunikaciju s interesnim stranama, zaduženja i odgovornosti.

Svi planovi moraju biti odobreni od strane Uprave organizacije i održavani ažurnima.

3.3.1.5 Uvježbavanje, održavanje i provjeravanje BCM-a

Ovaj element osigurava da je uspostavljeni BCM pouzdan i da ispunjava zahtjeve zbog kojih je uspostavljen. Zato mora biti stalno uvježbavan, provjeravan i samo-procjenjivan.

Uvježbavanje BCM-a je ključno za razvoj znanja i vještina nužnih u trenutku pojave incidenta. Mora biti pažljivo planirano i bez rizika uzrokovanja incidenta uslijed uvježbavanja te periodički izvršavano. Složenost uvježbavanja može varirati od provjere na papiru slijeda i aktivnosti, preko simulacija do izvođenja kompletnog plana neprekidnosti poslovanja. Rezultati provedenih vježbi trebaju se bilježiti u svrhu otklanjanja grešaka i poboljšanja samih planova.

Održavanje BCM-a ima za cilj identificirati sve promjene, bilo unutarnje ili vanjske, koje imaju utjecaja na BCM kao i nove proizvode i usluge koje bi trebale biti dio BCM-a i u skladu s tim ažurirati politike, strategije, procese i planove BCM-a.

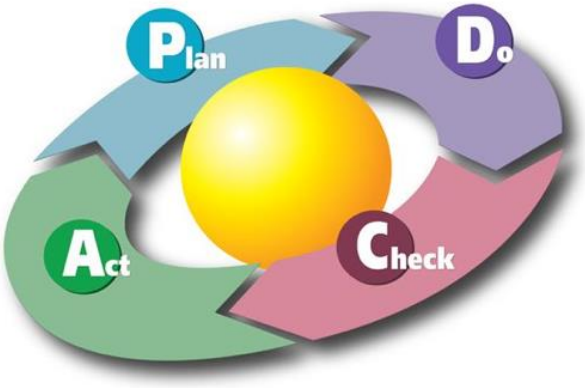
Svrha **provjeravanja** BCM-a jest preispitati sposobnost neprekidnosti poslovanja organizacije kao i usklađenost BCM-a sa zakonskim zahtjevima, primjenjivim normama, strateškim ciljevima i dobroj praksi. Provjeravanje se provodi kroz unutarnje ili vanjske revizije ili samo-procjenjivanjem.

3.3.1.6 Ugradnja BCM-a u svijest organizacije

Da bi bio uspješan, BCM mora postati dio načina upravljanja organizacijom. Razvoj BCM kulture unutar organizacije se najčešće postiže kroz rukovođenje na višim razinama, dodjeljivanjem zaduženja, podizanja svjesnosti, razvojem i uvježbavanjem potrebnih vještina te planiranjem i provođenjem uvježbavanja planova neprekidnosti poslovanja.

3.3.2 Neprekidan proces

Jednom uspostavljen BCM nije konačan. Jednom uspostavljen, BCM sustav implementira neprekidno provjeravanje i unapređivanje samog sebe sukladno PDCA modelu kao što je prikazano na slici 7. PDCA ciklus omogućava da se sa sposobnosti neprekidnosti poslovanja učinkovito upravlja i stalno unapređuje i primjenjuje se na sve elemente životnog ciklusa BCM-a. [14]



Slika 7 - Neprekidnost ciklusa BCM-a izvor [16])

Planiranje (***Plan***) – Uspostava politike neprekidnosti poslovanja, ciljeva, kontrola, procesa i procedura za upravljanje rizikom i unapređenje neprekidnosti poslovanja.

Izvršenje (***Do***) – Implementacija i izvršenje politike, kontrola, procesa i procedura.

Provjera (***Check***) – Nadziranje i provjeravanje učinkovitosti neprekidnosti poslovanja u odnosu na ciljeve i politiku i određivanje radnji za unapređenje.

Djelovanje (***Act***) – Primjena korektivnih radnji, održavanje i unapređenje BCM-a.

4 ANALIZA UTJECAJA NA POSLOVANJE

Razumijevanje same organizacije je temelj BCM-a. Da bi bili u stanju uspostaviti odgovarajući BCM nužno je najprije razumjeti naše poslovanje i utvrditi koji su aktivnosti i/ili procesi ključni za odvijanje kritičnih poslovnih aktivnosti barem na minimalnoj razini. Da bi se ispravno odredili osnovni čimbenici postojanja organizacije, potrebno je odgovoriti na sljedeća pitanja:

- Koje ciljeve organizacija mora ispuniti?
- Na koji način se ti ciljevi postižu?
- Koji su ključni proizvodi, odnosno usluge organizacije?
- Tko je uključen u proizvodni proces (kako unutar tako i izvan organizacije) u postizanju ciljeva organizacije?
- Koji su vremenski zahtjevi za isporuku proizvoda i usluga?

Razumijevanje se mora usredotočiti na aktivnosti koje najbrže ugrožavaju postizanje ciljeva organizacije. U razumijevanju organizacije glavna aktivnost jest analiza utjecaja na poslovanje (BIA – Business Impact Analyses). To je osnovni izvor za određivanje otpornosti organizacije i strategije neprekidnosti poslovanja. Osnovni zadatak BIA-e je razumijevanje koji poslovni procesi su vitalni za svakodnevno poslovanje i koji su utjecaji prekida takvih procesa. [5]

Sukladno svim normama u području BCM-a jest uloga analize utjecaja na poslovanje i može se svesti ukratko na „dokumentirati utjecaj prekida aktivnosti koje podržavaju ključne proizvode i usluge organizacije.“

Da bi se to postiglo analiza bi trebala za svaku aktivnost koja podržava isporuku ključnih proizvoda i usluga procijeniti;

- Utjecaj, u ovisnosti o vremenu trajanju prekida, koji bi bio prouzročen prekidom,
- Odrediti maksimalno vrijeme tolerancije ispade kroz određivanje,
    - Maksimalnog vremena nakon početka ispada unutar kojeg se aktivnost treba obnoviti (RTO),
    - Minimalnu razinu djelotvornosti aktivnosti nakon obnavljanja,
    - Vrijeme unutar kojeg se normalna razina djelotvornosti aktivnosti mora postići. (RPO)
- Utvrditi međuzavisne, podupiruće, aktivnosti i resurse koje se također trebaju uspostaviti unutar vremena oporavka.

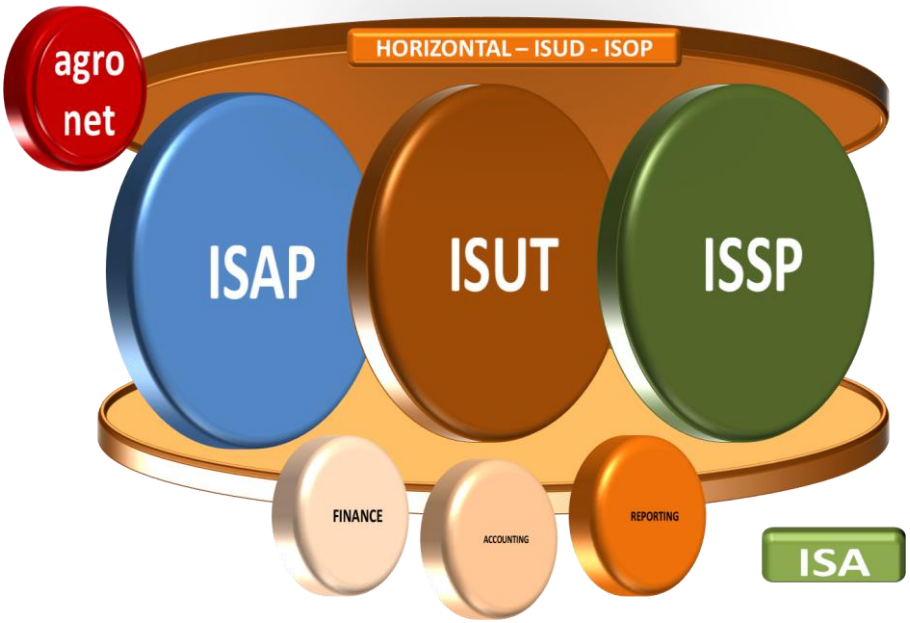
Konačni rezultat jest prioritet kojim bi se trebale obnoviti kritične aktivnosti nakon ispada i resursi potrebni za odvijanje tih kritičnih aktivnosti. Zbog toga je BIA u žarištu svakog dobro uspostavljenog BCM-a i aktivnost koja znatno utječe na konačne rezultate. Ukoliko se na krivi način procijene kritičnosti poslovnih procesa, daljnji razvoj BCM sustava činit će se na krivim pretpostavkama i u konačnici biti će neodgovarajući. Iz tog razloga je upravo BIA predmet ovog Završnog rada kao doprinos razumijevanju i provedbi ove aktivnosti.

U današnje vrijeme poslovanje gotovo svake organizacije snažno je ovisno o funkcioniranju ICT podrške. Gotovo nema poslovne aktivnosti i procesa koji nisu podržani ICT sustavom čime stavlja ICT u samo žarište upravljanja neprekidnošću poslovanja. Eventualni prekidi u pružanju ICT potpore, uvjetuju velike smetnje, pa i zastoje poslovnih procesa. Upravo zbog toga cilj istraživanja ovog završnog rada jest načiniti BIA analizu s primjenom na informatičke servise. Time se provedba BIA analize sužava na samo

određene podupiruće usluge, ICT servise, ali još uvijek i, s današnjeg stanovišta poslovanja, dovoljno kritične i značajne podupiruće servise i resurse bez kojih je nemoguće zamisliti odvijanje bilo kojeg poslovnog procesa. Praktični dio rada sastoji se o primjeni BIA postupka na informatičke servise Agencije.

4.1 Analiza utjecaja na poslovanje primijenjena na informatičke servise

Agenciju, koja je bila predmet promatranja, gledamo kao poslovni sustav čiji su poslovni procesi skoro u cijelosti podržani ICT-em. Slika broj 8, shematski prikazuje osnovne grupe i zastupljenost informatičkih servisa u odvijanju poslovnih procesa djelatnosti Agencije iz koje je vidljiv utjecaj informatičkih servisa na poslovanje a samim tim i na neprekidnost poslovanja.



Slika 8 - Informacijski sustav Agencije [izvor:vlastiti rad]

Obzirom da se analiza utjecaja na poslovanje primjenjuje isključivo na ICT servise, pristup rješavanju postavljenog problema sukladno normi ISO/IEC 22301:2012 je moguće postaviti na slijedeći način;

- Sukladno normi, prvi korak bi trebao biti, u sklopu razumijevanja organizacije, identificirati ciljeve i kritične usluge Agencije kao i poslovne procese i funkcije nužne za njihovo odvijanje. Ovdje je moguće krenuti od kataloga poslovnih informatičkih servisa i poslovnih funkcija i procesa koje podupiru, kao što je prikazano u tablici 2. Kroz korelaciju ICT servisa i poslovnih funkcija koje podupiru sužujemo opseg analize utjecaja na poslovanje prekida na samo one poslovne funkcije i aktivnosti koje su podržane bilo kojim od informatičkih servisa kako su poslovne aktivnosti koje nisu podržane informatičkim servisima izvan područja obuhvata ovog rada.

AGENCIJA ZA PLAĆANJA U POLJOPRIVREDI, RIBARSTVU I RURALNOM RAZVOJU

KATALOG IT SERVISA

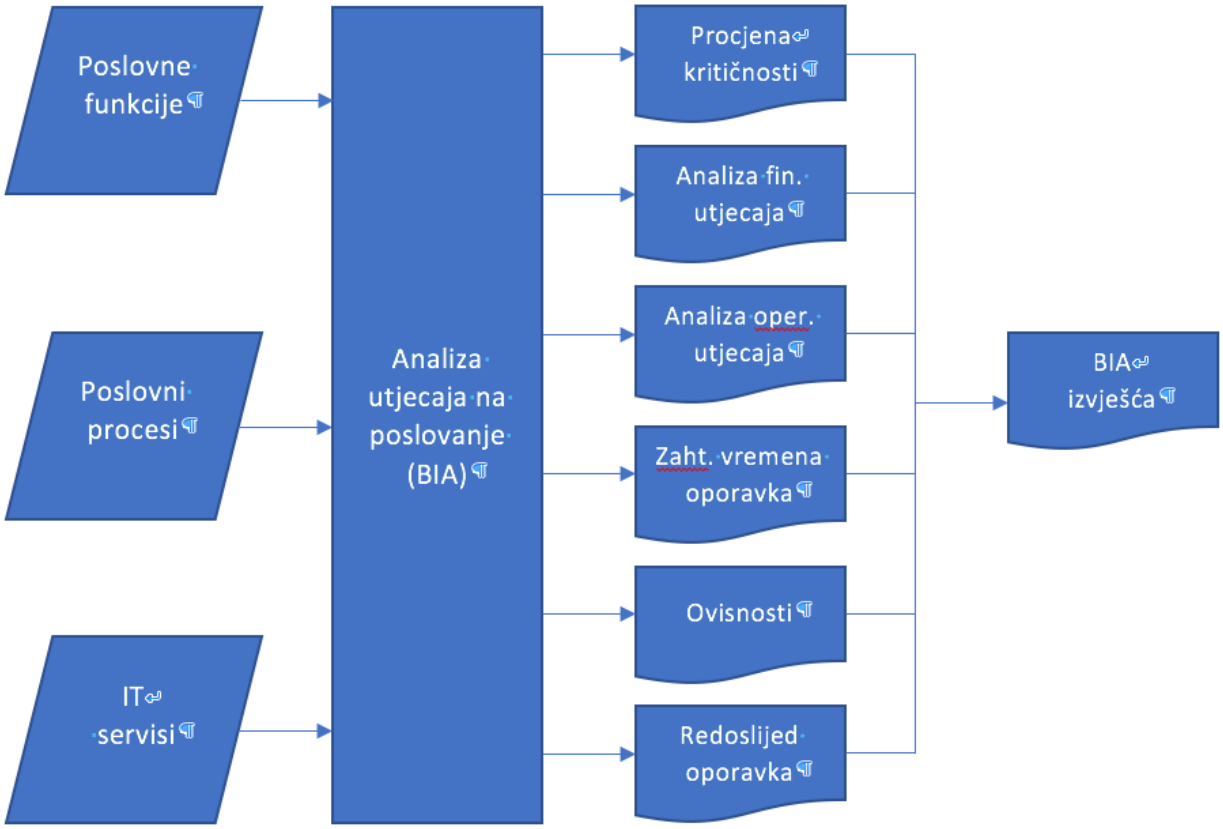
Veza na obrazac	Tip IT servisa	Naziv IT servisa	Dio IS-a	Modul	Informacije pružao	Status	Vlasnik aplikacije	Prva razina podrške	Druga razina podrške	Treća razina podrški	Ukupan broj korisnika	RTO,h	RPO, h	Povjerljivost	Cjelovitost	Raspoloživost
Pisarnica	Aplikativni - eksternalizirani	Pisarnica	Informacijski sustav upravljanja dokumentacijom (ISUD)	N/A	SM	U produkciji	RKJ	Help desk	SM	JP	53	24	24	Kritično	Visoka	Visoka
Plavo_Gorivo	Aplikativni - eksternalizirani	Plavo gorivo	0	0	0	U produkciji	SKM	0	0	0		4	4	Kritično	Vrlo visoka	Vrlo visoka
RS_EU	Aplikativni - eksternalizirani	Računovodstveni sustav pretpristupnih fondova	Računovodstveni sustav	N/A	BĐ	U produkciji	RM	Help desk	0	RK	10	4	4	Rezervirano	Srednja	Vrlo visoka
Riznica	Aplikativni - eksternalizirani	Rizinica	Informacijski sustav strukturne potpore (ISSP)	N/A	BĐ	U produkciji	SKS	0	0	0	2	8	24	Osjetljivo	Vrlo visoka	Visoka
WEB	Aplikativni – kupljeni	Javne web stranice	N/A	N/A	SM	U produkciji	LH	SM	JL	MK	50000	24	3	Javno	Vrlo visoka	Visoka
Kontrola_prolaza	Aplikativni – kupljeni	Kontrola prolaza	N/A	N/A	JV	U produkciji	GBO	Help desk	JL	0	210	24	24	Osjetljivo	Visoka	Visoka
SharePoint	Aplikativni – kupljeni	SharePoint	N/A	N/A	SM	U produkciji	AD	Help desk	JL	KK	220	3	0	Kritično	Visoka	Vrlo visoka
Revizija	Aplikativni – kupljeni	*Sustav za reviziju*	N/A	N/A	0	U planu	VM	0	0	0		48	24	Osjetljivo	Visoka	Srednja
agronet	Aplikativni – vanjski razvoj	agronet	N/A	N/A	RB	U produkciji	SKS	Help desk - agronet	Help desk	RB	10200	0	0	Kritično	Vrlo visoka	Vrlo visoka
AMKA	Aplikativni – vanjski razvoj	Aplikacija za mliječne kvote	Informacijski sustav upravljanja tržištem (ISUT)	0	0	U produkciji	SŠ	0	0	0		0	0	Osjetljivo	Visoka	Vrlo visoka
ARKOD	Aplikativni – vanjski razvoj	ARKOD	Informacijski sustav za administraciju izravnih plaćanja (ISAP)	Modul 2	SM	U produkciji	MŠ	Help desk - arkod	Help desk	RB	0	0	0	Kritično	Vrlo visoka	Vrlo visoka
Daljinsko	Aplikativni – vanjski razvoj	*Daljinsko istraživanje*	Informacijski sustav za administraciju izravnih plaćanja (ISAP)	0	RB	U razvoju	KB	0	0	0						
EU_mjere	Aplikativni – vanjski razvoj	*EU trgovinske mjere*	Informacijski sustav upravljanja tržištem (ISUT)	0	0	U planu	SŠ	0	0	0		0	0	Osjetljivo	Visoka	Vrlo visoka
FIS_garancije	Aplikativni – vanjski razvoj	Financijski sustav - garancije	Financijski sustav	N/A	RB	U produkciji	RM	Help desk	0	0	10	24	24	Osjetljivo	Visoka	Visoka
FIS_plaćanje	Aplikativni – vanjski razvoj	Financijski sustav - plaćanje	N/A	N/A	SM	U produkciji	RM	Help desk	0	MM	8	2	0	Kritično	Vrlo visoka	Vrlo visoka
FIS_voucheri	Aplikativni – vanjski razvoj	Financijski sustav - voucheri	Financijski sustav	N/A	RB	U produkciji	RM	Help desk	0	0	0	4	4	Osjetljivo	Vrlo visoka	Vrlo visoka
RS_APPRRR	Aplikativni – vanjski razvoj	Interni računovodstveni sustav Agencije	Računovodstveni sustav	N/A	SM	U produkciji	GI	Help desk	0	0	5	4	4	Rezervirano	Visoka	Vrlo visoka
Jedinstveni_zahtjev	Aplikativni – vanjski razvoj	Jedinstveni zahtjev	Informacijski sustav za administraciju izravnih plaćanja (ISAP)	0	0	U produkciji	SKM	0	0	0		3	3	Kritično	Vrlo visoka	Vrlo visoka
Kadrovska	Aplikativni – vanjski razvoj	*Kadrovska*	N/A	N/A	0	U razvoju	GBO	0	0	0		48	24	Rezervirano	Srednja	Srednja
Kontrola_na_terenu	Aplikativni – vanjski razvoj	*Kontrola na terenu*	Informacijski sustav za administraciju izravnih plaćanja (ISAP)	0	RB	U razvoju	KB	0	0	0		4	4	Osjetljivo	Visoka	Vrlo visoka
Nac_mjere	Aplikativni – vanjski razvoj	*Nacionalne ruralne mjere*	Informacijski sustav strukturne potpore (ISSP)	0	0	U planu	TMP	0	0	0		0	4	Kritično	Vrlo visoka	Vrlo visoka
Referetne_cijene	Aplikativni – vanjski razvoj	Referentne cijene	Informacijski sustav strukturne potpore (ISSP)	N/A	0	U produkciji	TMP	0	0	0		24	24	Rezervirano	Srednja	Visoka
Registar_prava	Aplikativni – vanjski razvoj	*Registar prava na plaćanje*	Informacijski sustav za administraciju izravnih plaćanja (ISAP)	0	0	U planu	MŠ	0	0	0						
Izvješćivanje	Aplikativni – vanjski razvoj	*Sustav za poslovno izvješćivanje*	Sustav za poslovno izvješćivanje	N/A	0	U razvoju	RM	0	0	0		72	24	Kritično	Visoka	Srednja
TIA	Aplikativni – vanjski razvoj	Trgovinska Internet aplikacija	Informacijski sustav upravljanja tržištem (ISUT)	0	0	U produkciji	SŠ	0	0	0		0	0	Osjetljivo	Visoka	Vrlo visoka
Upisnik	Aplikativni – vanjski razvoj	Upisnik poljoprivrednih gospodarstva	Informacijski sustav za administraciju izravnih plaćanja (ISAP)	0	RB	U produkciji	MŠ	Help desk - arkod	Help desk	RB	0	0	0	Kritično	Vrlo visoka	Vrlo visoka
Help_desk	Aplikativni - vlastiti razvoj	Help desk sustav	N/A	N/A	SM	U produkciji	ZD	ZD	0	0	1	120	120	Rezervirano	Visoka	Vrlo visoka
anti_malver	Infrastrukturni	Anti-malver sustav	N/A	N/A	JV	U produkciji	DM	Help desk	JL	JV	600	24	24	Osjetljivo	Visoka	Visoka
email	Infrastrukturni	Elektronička pošta	N/A	N/A	JV	U produkciji	DM	Help desk	JL	JV	501	6	3	Kritično	Visoka	Vrlo visoka
File_servis	Infrastrukturni	File servis	N/A	N/A	JV	U produkciji	DM	Help desk	JL	JV	200	3	3	Kritično	Vrlo visoka	Vrlo visoka
FTP	Infrastrukturni	*FTP servis*	N/A	N/A	JV	Ne koristi se	DM	Help desk	JL	JV		120	120	Rezervirano	Niska	Niska
AD	Infrastrukturni	Imenički servis	N/A	N/A	JV	U produkciji	DM	Help desk	JL	JV	500	0	24	Kritično	Vrlo visoka	Vrlo visoka
LAN	Infrastrukturni	Interna računalna mreža	N/A	N/A	JV	U produkciji	DM	Help desk	JL	0	200	0	0	Kritično	Vrlo visoka	Vrlo visoka
PBX	Infrastrukturni	Interna telefonija	N/A	N/A	JV	U produkciji	DM	ČR	AA	0	185	0	8	Osjetljivo	Srednja	Vrlo visoka
PKI	Infrastrukturni	PKI sustav	N/A	N/A	JV	U produkciji	DM	ČR	JV	KK	0	120	120	Osjetljivo	Srednja	Niska
Internet	Infrastrukturni	Pristup Internetu	N/A	N/A	JV	U produkciji	DM	Help desk	0	0	729	0	0	Kritično	Vrlo visoka	Vrlo visoka
SSO	Infrastrukturni	*Sustav jedinstvene autentikacije*	N/A	N/A	0	U razvoju	DM	0	0	0		0	0	Kritično	Vrlo visoka	Vrlo visoka
Veza_MPRRR	Infrastrukturni	Veza prema MPRRR	N/A	N/A	JV	U produkciji	DM	Help desk	DK	0	41	3	4	Rezervirano	Srednja	Vrlo visoka
Virtualnizacija	Infrastrukturni	Virtualizacijski servis	N/A	N/A	JL	U produkciji	DM	Help desk	JL	JV	#N/A	0	0	Kritično	Vrlo visoka	Vrlo visoka
VPN	Infrastrukturni	VPN	N/A	N/A	JL	U produkciji	DM	Help desk	JL	MP	300	0	0	Kritično	Vrlo visoka	Vrlo visoka
Mrežni_nadzor	Uslužni IT servisi	Mrežni nadzor	N/A	N/A	JV	U produkciji	DM	JL	JL	JV	0	4	24	Osjetljivo	Visoka	Visoka
Back_up	Uslužni IT servisi	Sigurnosna pohrana	N/A	N/A	JL	U produkciji	DM	JL	ŽČ	0	0	6	24	Kritično	Vrlo visoka	Visoka
Update	Uslužni IT servisi	Update servis	N/A	N/A	JL	U produkciji	DM	JL	JV	0	500	120	120	Rezervirano	Srednja	Niska
Video_nadzor	Uslužni IT servisi	Video nadzor	N/A	N/A	JV	U produkciji	DM	JL	JV	KP	0	168	24	Rezervirano	Srednja	Niska

Tablica 1 - Tablični prikaz veza IT servisa i poslovnih procesa Agencije (Izvor: vlastiti rad)

- Slijedeći korak jeste provedba analize utjecaja na poslovanje prekida poslovnih aktivnosti Agencije koji su podržane ICT servisima kroz;
  - Određivanje utjecaja prekida pojedine aktivnosti na poslovanje Agencije kroz procjenu operativnog i financijskog utjecaja tokom vremena,
  - Određivanja zahtijevanih vremena oporavka i sukladno tome kritičnih aktivnosti i kritičnih ICT servisa na koje će se preslikati najzahtjevnija vremena oporavka poslovnih aktivnosti koje podržavaju,
  - U dijelu ovisnosti odvijanja kritičnih aktivnosti razmotrit će se samo ovisnost o ICT servisima tj. podupiruće aktivnosti i resursi potrebni za odvijanje ICT servisa. Za svaki ICT servis/aplikaciju koja podržava odvijanje kritične aktivnosti odredit će se podupirući servisi i resursi neophodni za njihovo odvijanje,

Konačni rezultat jest redoslijed obnove ICT servisa, njihovih podupirućih servisa i resursa i vremenski okvir oporavka svakog od njih predočen kroz predloženi oblik izvještaja.

Provedba analize utjecaja na poslovanje primijenjena na ICT servise, kako je predložena u ovom radu, može se prikazati blok dijagramom kako je prikazano na slici 9.



Slika 9 - Ulazi i izlazi postupka analize utjecaja na poslovanje (Izvor: vlastiti rad)

4.1.1 O Agenciji

Svaka država članica Europske unije mora imati agenciju za plaćanja u poljoprivredi. Osnivanje takve agencije u Hrvatskoj bio je uvjet za zatvaranje pristupnih pregovora s Europskom unijom, pa je tako Agencija za plaćanja u poljoprivredi, ribarstvu i ruralnom razvoju jedina institucija čije je osnivanje, odnosno postojanje, izrijekom navedeno u Ugovoru o pristupanju Hrvatske u EU kao uvjet za punopravno članstvo.

Da bi mogla koristiti oko 5 milijardi kuna godišnje iz EU proračuna namijenjenih poljoprivredi i ruralnom razvoju RH, Agencija za plaćanja akreditirana je po točno

određenim kriterijima (Uredba EK 885/2006, zamijenjena novom Uredbom 907/2014) te svoj rad temelji na akreditiranim procesima i procedurama. Agencija za plaćanja nadležna je za operativnu provedbu mjera poljoprivredne politike u skladu sa Zakonom o poljoprivredi i Zakonom o osnivanju Agencije za plaćanja u poljoprivredi, ribarstvu i ruralnom razvoju, a posluje putem središnjeg ureda u Zagrebu i podružnica u jedinicama regionalne (područne) samouprave. Osnovana je 21 podružnica u županijskim centrima te 3 ispostave (Senj, Metković, Korčula), a od svibnja 2017. i četvrta - u Đakovu.

Zadaća Agencije za plaćanja je operativna provedba mjera izravne potpore, mjera ruralnog razvoja i mjera zajedničke organizacije tržišta, kao i vođenje upisnika i registara te održavanje i korištenje Integriranog administrativnog i kontrolnog sustava (IAKS-a) preko kojeg se zaprimaju, obrađuju i kontroliraju izravna plaćanja poljoprivrednicima.

Od ostalih neophodnih sustava, Agencija ima Upisnik poljoprivrednika s 167.047 registriranih poljoprivrednika (podaci od svibnja 2017.), zatim ARKOD–sustav za digitalnu identifikaciju zemljišnih parcela; te prateće registre (vinogradarski registar, registar primarnih proizvođača hrane, registar subjekata u ekološkoj proizvodnji), ISAP–centraliziranu elektronsku bazu podataka (za istovremeni unos podataka sa svih 26 lokacija APPRRR u RH) i AGRONET–zaštićenu internetsku aplikaciju putem koje poljoprivrednici pregledavaju podatke o svom gospodarstvu te u kojoj elektronski popunjavaju zahtjeve za potpore.

Operativna provedba potpora podrazumijeva zaprimanje zahtjeva poljoprivrednika, administrativne kontrole zahtjeva, kontrole na terenu, odobravanje i isplatu potpora. Agencija za plaćanja također provodi delegirane funkcije ekonomskih i tehničkih analiza zahtjeva za potpore u ribarstvu te njihovu isplatu.

Navedene mjere poljoprivredne politike financiraju se iz državnog proračuna Republike Hrvatske i proračuna Europske unije. Iz Europskog fonda za jamstva u poljoprivredi (EFJP) financiraju se izdaci za mjere izravne potpore i mjere zajedničke organizacije tržišta dok se iz Europskoga poljoprivrednog fonda za ruralni razvoj (EPFRR) financiraju izdaci za mjere ruralnog razvoja.

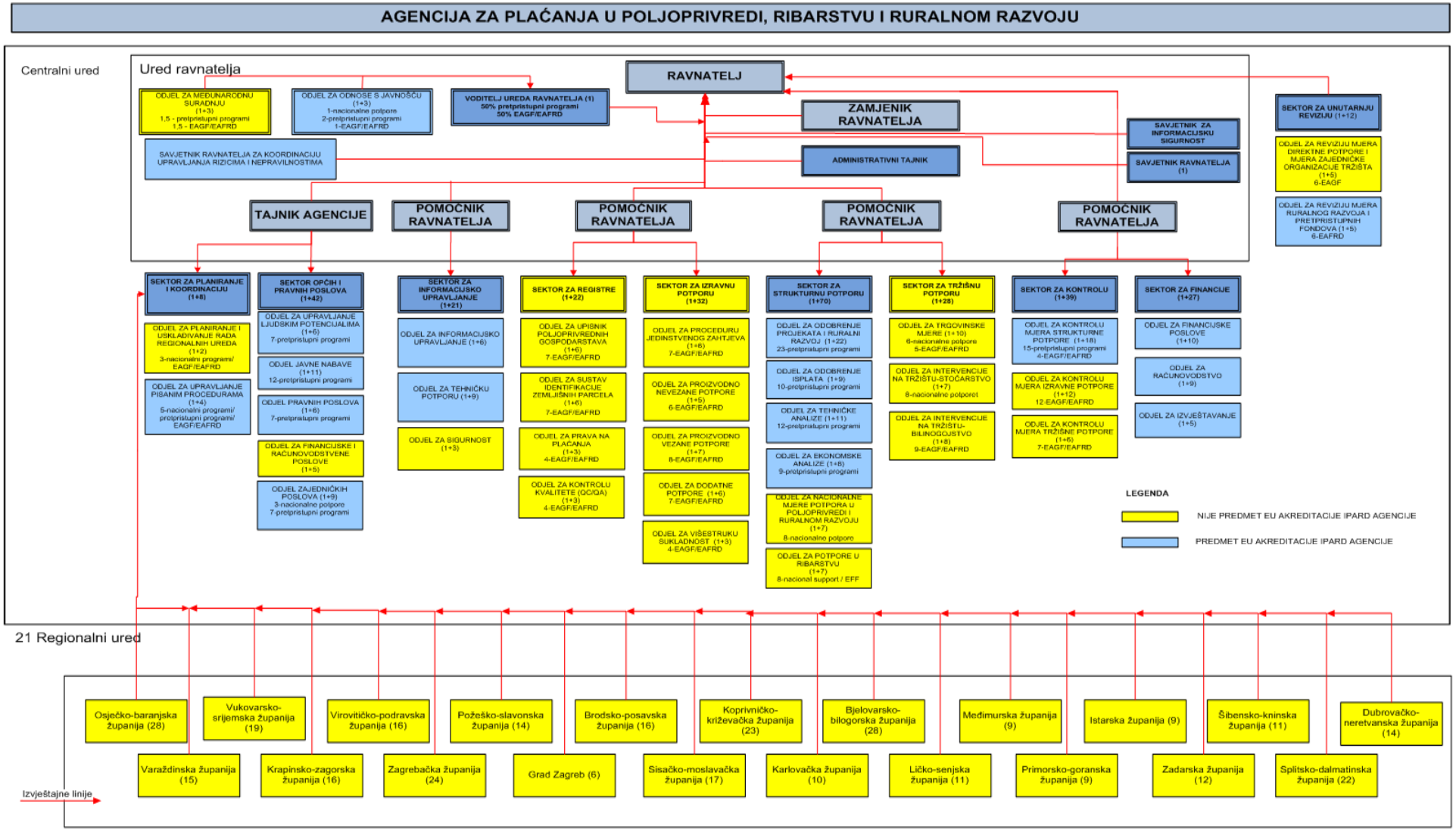
Tijekom 2016. godine Agencija za plaćanja je isplatila ukupno 4,3 mlrd. kn potpore poljoprivrednim proizvođačima, ribarima i ostalim korisnicima. Od tog iznosa iz proračuna Europske unije refundirano je 2,8 mlrd. kn i to iz EFJP-a 1,5 mlrd. kn, EPFRR-a 995,3 mil. kn, Europskog fonda za ribarstvo/Europskog fonda za pomorstvo i ribarstvo (EFR/EFPR) 74 mil. kn i iz pretpristupnog IPARD programa 228,2 mil. kn.

Misija Agencije:

Misija Agencije za plaćanja je povezivanje hrvatskih poljoprivrednika, ribara i subjekata u ruralnom prostoru s institucijama na nacionalnoj i europskoj razini koje kroz svoje programe i fondove financiraju razvoj poljoprivrede, ribarstva i ruralnog prostora.

Vizija Agencije:

Primjereniji životni standard poljoprivrednika i ribara te očuvanje ruralnih prostora i njihov uravnotežen razvoj. (Izvor Internet)



Slika 10 - Organigram Agencije (Izvor: vlastiti rad)

4.1.2 Procjena rizika, te korelacija informatičkih servisa i poslovnih funkcija Agencije

U ovom dijelu izvršit će se procjena rizika, te korelacija poslovnih funkcija i informatičkih servisa Agencije. Procjena rizika proizvest će nalaze karakteristične za informacijsku sigurnost, te dodatno razraditi problematiku raspoloživosti kroz svojevrsnu analizu utjecaja na poslovanje, karakterističnom za upravljanje kontinuitetom poslovanja. Na temelju analize određuju se kritičnosti informacijskih sustava i IT servisa, ciljana vremena oporavka i maksimalna tolerancija gubitaka podataka te se odabiru preventivne sigurnosne mjere, kojima se nastoji umanjiti ukupni rizik po informacije u Agenciji.

U postupku je bila razmatrana sva imovina koja je uključena u proces obrade informacija u Agenciji. Svrha je identificirati poslovne funkcije i aktivnosti koje su podržane informatičkim servisima Agencije i na taj način odrediti opseg provedbe analize utjecaja na poslovanje. Kao polazište za ovu aktivnost idealna izbor jeste Katalog informatičkih servisa Agencije. Kako je u Agenciji održavanje ažurnog kataloga informatičkih servisa redovan operativni posao Sektora za informacijsko upravljanje, tako je ovaj posao već obavljen i bit će korišten kao polazište. Stoga neće biti izložen detaljan postupak izrade kataloga informatičkih servisa, već samo struktura Kataloga i elementi od interesa za daljnju provedbu analize utjecaja na poslovanje.

Temeljni proces svakog sustava upravljanja informacijskom sigurnošću je periodička provedba procjene rizika informacijske sigurnosti. Ovaj proces je pokretač promjena i unaprjeđenja sigurnosnih mjera u organizaciji. Sukladno postupku iz dokumenta Priručnik za procjenu i upravljanje rizicima informacijske sigurnosti, procjena razmatra indirektne gubitke koje Agencija trpi u slučaju razotkrivanja

povjerljivih informacija, narušavanja integriteta informacija te nemogućnosti odvijanja poslovnih aktivnosti zbog neraspoloživosti informacija koje poslovni korisnici koriste u svom svakodnevnom radu. Analiza također definira i zahtjeve poslovanja prema informacijskoj imovini tj. određuje granice unutar koje povjerljivost, integritet ili raspoloživost može biti narušena a da pritom ne nastanu neprihvatljivi gubici za Agenciju.

Ovom analizom se procjenjuje vjerojatnost ostvarivanja raznih vrsti rizika iz okoline ili unutar same Agencije te utjecaj koji ti rizici imaju ukoliko se ostvare. Rezultati analize daju uvid u moguće probleme na koje Agencija može naići te kao takva predstavlja dobar izvor informacija za korake koje je potrebno poduzeti da se vjerojatnost pojave ili negativni utjecaj smanje na najmanju moguću mjeru.

4.1.2.1 Način provedbe prikupljanja informacija

Tijekom perioda od 60 dana, provedeni su intervjui i radionica s ciljem prikupljanja informacija radi provođenja snimke stanja, identifikacije informacijske imovine i rizika informacijske sigurnosti.

Informacije potrebne za analizu IT servisa su se prikupljale od djelatnika Sektora za informacijskom upravljanje, dok su se informacije potrebne za analizu poslovnih aktivnosti prikupljale na radionici sa vlasnicima procesa. Tijekom ovih aktivnosti popunjavani su pripremljeni obrasci, koji su izrađeni prema najboljim praksama i zbog jednostavnosti popunjavanja i publike podijeljeni u dva dijela. Prvi dio se odnosi na informacije vezane uz poslovni aspekt korištenja IT servisa i sastavni dio je kataloga poslovnih aktivnosti, dok je drugi dio orijentiran prema tehničkim karakteristikama pojedinog IT servisa i sastavni je dio kataloga IT servisa. S obzirom na različite

namjene i tipove IT servisa nisu svi obrasci IT servisa uniformno ispunjeni, tj. određeni parametri se nisu mogli definirati za pojedine IT servise.

4.1.2.2 Struktura Kataloga informatičkih servisa Agencije

Katalog informatičkih servisa Agencije (u Prilogu A) temelji se na detaljnom opisu informatičkog servisa nakon njegove uspostave. Obrazac definicije uspostavljenog informatičkog servisa nalazi se u Prilogu B. Strukturiran je na način da su grupirani zasebno infrastrukturni servisi i zasebno poslovni aplikativni servisi. Aplikativni poslovni servisi dalje su grupirani prema segmentu djelatnosti koju podržavaju u Agencija

IT servisi ili usluge su prvenstveno orijentirane prema korisniku i načinu na koji on percipira logičke cjeline korištenja informacijske tehnologije, a ne prema arhitekturnim ili tehnološkim aspektima korištene tehnologije. S obzirom da postoje sustavi koji pružaju IT uslugu drugim sustavima tj. predstavljaju neku vrstu zajedničke IT infrastrukture ostalim IT servisima te postoje IT servisi koji pružaju određenu vrijednost samoj IT organizacijskoj funkciji korištena je slijedeća podjela IT servisa:

4.1.2.3 Identificirani IT servisi

IT servisi ili usluge su prvenstveno orijentirane prema korisniku i načinu na koji on percipira logičke cjeline korištenja informacijske tehnologije, a ne prema arhitekturnim ili tehnološkim aspektima korištene tehnologije. S obzirom da postoje sustavi koji pružaju IT uslugu drugim sustavima tj. predstavljaju neku vrstu zajedničke IT infrastrukture ostalim IT servisima te postoje IT servisi koji pružaju određenu vrijednost samoj IT organizacijskoj funkciji korištena je slijedeća podjela IT servisa:

- **Aplikativni – eksternalizirani IT servisi** čiji su softver u potpunosti implementirali te održavaju vanjski partneri, tj. svi IT servisi koje nije moguće restaurirati i administrirati bez vanjske pomoći
- **Aplikativni - vlastiti razvoj,** tj. interno razvijene i održavane aplikacije te aplikacije koje su vanjski razvoj, ali su održavanje i nadogradnja preuzete te se odvijaju od strane Agencije
- **Aplikativni – kupljeni**, tj. gotove (*engl. „off-the-shelf")* aplikacije s mali brojem zahvata i prilagodbi
- **Aplikativni – vanjski razvoj**, tj. aplikacije razvijene po narudžbi od strane vanjskih dobavljača ali Agencija posjeduje mogućnost administracije
- **Infrastrukturni IT servisi** T servisi koje korisnici ne koriste direktno već im je primarna namjena podloga radu drugim servisima (primjerice anti-malver sustav, imenički servis, virtualizacija,…) ili IT servisi koji spadaju u osnovni preduvjet za rad (primjerice elektronička pošta, pristup Internetu, interna telefonija i slično).
- **Lokalne aplikacije** tj. kritične poslovne aplikacije koje za nominalni rad nemaju potrebu za računalnom mrežom i drugim IT servisima već rade u potpunosti autonomno (primjerice aplikacije za rad na terenu ili udaljenim lokacijama bez pristupa mreži). U ovu kategoriju se najčešće ne ubrajaju tipične uredske aplikacije.
- **Uslužni IT servisi IT** tj. servisi koji se koriste od strane djelatnika IT i namijenjeni su podršci rada ostalim IT servisima (primjerice nadzorni alati, alati za udaljenu administraciju i slično).

Prilikom definiranja IT servisa određeni su slijedeći poslovni i tehnički parametri:

- Kontakti podrške tj razine podrške i eskalacije u slučaju problema sa IT servisom,
- Poslovno odgovorna osoba

- Krajnje vrijeme unutar kojega je potrebno osposobiti IT servis u slučaju ispada ili više slike
- Primjerena učestalost i metoda izrade sigurnosne kopije podataka
- Vršna opterećenja IT servisa i broj korisnika
- Poslovni značaj IT servisa i utjecaj u slučaju ispada istog
- Međuovisnosti i preduvjeti za rad

Poslovne parametre procijenili su predstavnici poslovanja, a tehnološke djelatnici Sektora za informacijskom upravljanje. Tijekom snimke identificirano je 44 IT servisa, od kojih:

- **18** pripada kategoriji **Aplikativni – vanjski razvoj**, od kojih 5 je još u razvoju, 5 u planu, jedan u testnoj fazi i preostalih 7 u produkciji,
- **13** u kategoriji **Infrastrukturnih servisa**, od kojih jedan je u razvoju a jedan se više ne koristi,
- **4** u kategoriji **uslužnih IT servisa**, kojih su svi u produkciji,
- **4** u kategoriji **Aplikativnih – kupljenih**, od kojih jedan je tek u planu,
- **4** u kategoriji **Aplikativnih - eksternaliziranih servisa**, od kojih je jedan u testnoj fazi te
- **1** u kategoriji **Aplikativni – vlastiti razvoj,** koji je u produkciji.

Tablica 2 prikazuje odgovornosti prema informacijskim servisima - predstavlja dio kataloga IT servisa koji definira odgovornosti za identificirane IT servise. Odgovornosti uključuju: poslovnog vlasnika aplikacije/sustava i tri razine podrške u slučaju ispada ili kvara dotičnog. Neki IT servisi nemaju definirane sve tri razine podrške s obzirom na vrlo ograničene ljudske resurse te veliku razinu eksternalizacije IT usluga.

Tip IT servisa	Naziv IT servisa	Dio IS-a	Vlasnik aplikacije	Prva razina podrške	Druga razina podrške	Treća razina podrške
Aplikativni - eksternalizirani	***Pisarnica***	Informacijski sustav upravljanja dokumentacijom (ISUD)	RKJ	Help desk	SM	JP
Aplikativni - eksternalizirani	***Računovodstveni sustav pretpristupnih fondova***	Računovodstveni sustav	RM	Help desk		RK
Aplikativni - eksternalizirani	***Rizinica***	Informacijski sustav strukturne potpore (ISSP)	SKS			
Aplikativni – kupljeni	***Javne web stranice***	N/A	LH	SM	JL	MK
Aplikativni – kupljeni	***Kontrola prolaza***	N/A	GBO	Help desk	JL	
Aplikativni – kupljeni	***SharePoint***	N/A	AD	Help desk	JL	KK
Aplikativni – vanjski razvoj	***agronet***	N/A	SKM	Help desk - agronet	Help desk	RB
Aplikativni – vanjski razvoj	***ARKOD***	Informacijski sustav za administraciju izravnih plaćanja (ISAP)	MŠ	Help desk - arkod	Help desk	RB
Aplikativni – vanjski razvoj	***Financijski sustav - garancije***	Financijski sustav	RM	Help desk		
Aplikativni – vanjski razvoj	***Financijski sustav - plaćanje***	N/A	RM	Help desk		MM
Aplikativni – vanjski razvoj	***Financijski sustav - voucheri***	Financijski sustav	RM	Help desk		
Aplikativni – vanjski razvoj	***Interni računovodstveni sustav Agencije***	Računovodstveni sustav	GI	Help desk		
Aplikativni – vanjski razvoj	***Upisnik poljoprivrednih gospodarstva***	Informacijski sustav za administraciju izravnih plaćanja (ISAP)	MŠ	Help desk - arkod	Help desk	RB
Aplikativni - vlastiti razvoj	***Help desk sustav***	N/A	ZD	ZD		
Infrastrukturni	***Anti-malver sustav***	N/A	DM	Help desk	JL	JV
Infrastrukturni	***Elektronička pošta***	N/A	DM	Help desk	JL	JV
Infrastrukturni	***File servis***	N/A	DM	Help desk	JL	JV

Tip IT servisa	Naziv IT servisa	Dio IS-a	Vlasnik aplikacije	Prva razina podrške	Druga razina podrške	Treća razina podrške
Infrastrukturni	***Imenički servis***	N/A	DM	Help desk	JL	JV
Infrastrukturni	***Interna računalna mreža***	N/A	DM	Help desk	JL	
Infrastrukturni	***Interna telefonija***	N/A	DM	ČR	AA	
Infrastrukturni	***PKI sustav***	N/A	DM	Help desk	JV	KK
Infrastrukturni	***Pristup Internetu***	N/A	DM	Help desk		
Infrastrukturni	***Veza prema MPRRR***	N/A	DM	Help desk	DK	
Infrastrukturni	***Virtualizacijski servis***	N/A	DM	Help desk	JL	JV
Infrastrukturni	***VPN***	N/A	DM	Help desk	JL	MP
Uslužni IT servisi	***Mrežni nadzor***	N/A	DM	JL	JL	JV
Uslužni IT servisi	***Sigurnosna pohrana***	N/A	DM	JL	ŽČ	
Uslužni IT servisi	***Update servis***	N/A	DM	JL	JV	
Uslužni IT servisi	***Video nadzor***	N/A	DM	JL	JV	KP

Tablica 2 - Odgovornost za IT servise Agencije (Izvor: vlastiti rad)

Osnovni elementi Kataloga informatičkih servisa prikazani su na slici 10. jesu:

- **Tip IT servisa –** Pripadnost tipu informatičkog servisa,
- **Naziv IT servisa -** Naziv IT servisa,
- **Dio IS-a –** Pripadnost informacijskom sustavu (procesu), organizacijske jedinica ili više njih u kojima se koristi navedeni informatički servis u obavljanju redovnih poslovnih aktivnosti. Ovaj podatak nam kazuje koje poslovne funkcije su podržane ovim informatičkim servisom
- **Vlasnik aplikacije/podataka/procesa** – Odnosno odgovorna osoba. Organizacijska jedinica odgovorna za isporuku, tj. redovan rad informatičkog servisa. Ravnatelj Agencije, direktori poslovnih funkcija i voditelji Službi u pojedinim Sektorima Agencije koji imaju upravljačku odgovornost za nadzor nad produkcijom, razvojem, održavanjem, upotrebom i sigurnošću podataka/informacija.

Ostali podaci o informatičkim servisima koji se prikupljaju vidljivi su iz obrasca detaljnog opisa informatičkog servisa koji se nalazi u Privitku B.

4.1.2.4 Procjena kritičnosti IT servisa

Tablica 3 predstavlja dio kataloga IT servisa koji definira parametre procjene kritičnosti identificiranih IT servisa. Ovi parametri uključuju: procijenjeni ukupan broj korisnika, ciljano vrijeme oporavka IT servisa u slučaju kvara ili više sile, mogućnost restauracije izgubljenih podataka uslijed destruktivnog kvara te procijenjena razina povjerljivost i integriteta podataka koji IT servis izrađuje, pohranjuje i prosljeđuje.

Aplikativni - eksternalizirani	***Pisarnica***	Informacijski sustav upravljanja dokumentacijom (ISUD)	53	24		Kritično	Visoka	Visoka
Aplikativni - eksternalizirani	***Računovodstveni sustav pretpristupnih fondova***	Računovodstveni sustav	10	4	4	Rezervirano	Srednja	Vrlo visoka
Aplikativni - eksternalizirani	***Rizinica***	Informacijski sustav strukturne potpore (ISSP)	2	8	24	Osjetljivo	Vrlo visoka	Visoka
Aplikativni – kupljeni	***Javne web stranice***	N/A	50000	24	3	Javno	Vrlo visoka	Visoka
Aplikativni – kupljeni	***Kontrola prolaza***	N/A	210	24	24	Osjetljivo	Visoka	Visoka
Aplikativni – kupljeni	***SharePoint***	N/A	220	3	0	Kritično	Visoka	Vrlo visoka
Aplikativni – vanjski razvoj	***agronet***	N/A	10200	0	0	Kritično	Vrlo visoka	Vrlo visoka
Aplikativni – vanjski razvoj	***ARKOD***	Informacijski sustav za administraciju izravnih plaćanja (ISAP)	0	0	0	Kritično	Vrlo visoka	Vrlo visoka
Aplikativni – vanjski razvoj	***Financijski sustav - garancije***	Financijski sustav	10	24	24	Osjetljivo	Visoka	Visoka
Aplikativni – vanjski razvoj	***Financijski sustav - plaćanje***	N/A	8	2	0	Kritično	Vrlo visoka	Vrlo visoka
Aplikativni – vanjski razvoj	***Financijski sustav - voucheri***	Financijski sustav	0	4	4	Osjetljivo	Vrlo visoka	Vrlo visoka
Aplikativni – vanjski razvoj	***Interni računovodstveni sustav Agencije***	Računovodstveni sustav	5	4	4	Rezervirano	Visoka	Vrlo visoka
Aplikativni – vanjski razvoj	***Upisnik poljoprivrednih gospodarstva***	Informacijski sustav za administraciju izravnih plaćanja (ISAP)	0	0	0	Kritično	Vrlo visoka	Vrlo visoka
Aplikativni - vlastiti razvoj	***Help desk sustav***	N/A	1	120	120	Rezervirano	Visoka	Vrlo visoka
Infrastrukturni	***Anti-malver sustav***	N/A	600	24	24	Osjetljivo	Visoka	Visoka

Infrastrukturni	***Elektronička pošta***	N/A	501	6	3	Kritično	Visoka	Vrlo visoka
Infrastrukturni	***File servis***	N/A	200	3	3	Kritično	Vrlo visoka	Vrlo visoka
Infrastrukturni	***Imenički servis***	N/A	500	0	24	Kritično	Vrlo visoka	Vrlo visoka
Infrastrukturni	***Interna računalna mreža***	N/A	200	0	0	Kritično	Vrlo visoka	Vrlo visoka
Infrastrukturni	***Interna telefonija***	N/A	185	0	8	Osjetljivo	Srednja	Vrlo visoka
Infrastrukturni	***PKI sustav***	N/A	0	120	120	Osjetljivo	Srednja	Niska
Infrastrukturni	***Pristup Internetu***	N/A	729	0	0	Kritično	Vrlo visoka	Vrlo visoka
Infrastrukturni	***Veza prema MPRRR***	N/A	41	3	4	Rezervirano	Srednja	Vrlo visoka
Infrastrukturni	***Virtualizacijski servis***	N/A		0	0	Kritično	Vrlo visoka	Vrlo visoka
Infrastrukturni	***VPN***	N/A	300	0	0	Kritično	Vrlo visoka	Vrlo visoka
Uslužni IT servisi	***Mrežni nadzor***	N/A	0	4	24	Osjetljivo	Visoka	Visoka
Uslužni IT servisi	***Sigurnosna pohrana***	N/A	0	6	24	Kritično	Vrlo visoka	Visoka
Uslužni IT servisi	***Update servis***	N/A	500	120	120	Rezervirano	Srednja	Niska
Uslužni IT servisi	***Video nadzor***	N/A	0	168	24	Rezervirano	Srednja	Niska

Tablica 3 - Procjena kritičnosti IT servisa (Izvor: vlastiti rad)

Navedeni parametri su sistematično navedeni u kataloga IT servisa li su prikupljeni tijekom radionice sa predstavnicima poslovanja. Tijekom provedbe analize intervjuirano je i anketirano ukupno 30 zaposlenika, kao što je prikazano u tablici 4.

Vrsta aktivnosti	Naziv	Informacije pružao
Ključne	**Odjel za financijske poslove**	Voditelj odjela
Ključne	**Odjel za izvještavanje**	Voditelj odjela
Ključne	**Odjel za kontrolu mjera izravne potpore**	Voditelj odjela
Ključne	**Odjel za kontrolu mjera strukturne potpore**	Voditelj odjela
Ključne	**Odjel za kontrolu mjera tržišne potpore**	Voditelj odjela
Ključne	**Odjel za odobrenje isplata**	Voditelj odjela
Ključne	**Odjel za odobrenje projekata i ruralni razvoj**	Voditelj odjela
Ključne	**Odjel za potpore u ribarstvu**	Voditelj odjela
Ključne	**Odjel za proceduru jedinstvenog zahtjeva**	Voditelj odjela
Ključne	**Odjel za računovoodstvo**	Voditelj odjela
Ključne	**Odjel za tehničke analize**	Voditelj odjela
Ključne	**Regionalni ured**	JF
Ključne	**Sektor za izravnu potporu**	Voditelj sektora
Ključne	**Sektor za registre**	Voditelj sektora
Ključne	**Sektor za tržišnu potporu**	Voditelj sektora
Potporne	**Hrvatska poljoprivredna agencija - Služba za ICT**	DL
Potporne	**Hrvatski zavod za poljoprivrednu savjetodavnu službu (HZPSS)**	VČ
Potporne	**Odjel javne nabave**	AŠ
Potporne	**Odjel pravnih poslova**	SŽ
Potporne	**Odjel za financijske i računovodstvene poslove**	GI
Potporne	**Odjel za informacijsko upravljanje**	SM
Potporne	**Odjel za nacionalne mjere potpora u poljoprovredi i ruralnom razvoju**	RM
Potporne	**Odjel za sigurnost**	Voditelj odjela
Potporne	**Odjel za tehničku potporu**	Voditelj odjela
Potporne	**Odjel za upravljanje ljudskim potencijalima**	Voditelj odjela
Potporne	**Odjel zajedničkih poslova**	Voditelj odjela
Potporne	**Sektor za planiranje i koordinaciju**	Voditelj sektora
Potporne	**Sektor za unutarnju reviziju**	Voditelj sektora
Upravljačke	**Odjel za međunarodnu suradnju**	Voditelj odjela
Upravljačke	**Odjel za odnose s javnošću**	Voditelj odjela

Tablica 4 - Popis predstavnika poslovanja koju su dali poslovno relevantne podatke (Izvor: vlastiti rad)

4.1.2.5 Tablica korelacije informatičkih servisa i poslovnih funkcija

Korištenjem podataka iz kataloga informatičkih servisa moguće je napraviti početnu tablicu korelacije informatičkih servisa, poslovnih funkcija i aktivnosti. Konačna tablica korelacije dobit će se kroz prikupljanje podataka o utjecaju prekida poslovnih funkcija i aktivnosti i zavisnosti o podupirućim uslugama i resursima.

Za izradu početne tablice korelacije koristit će se naziv informatičkog servisa, naziv poslovnog procesa, odnosno referenca na konkretan informacijski sustav (Dio IS-a) i vlasnika podataka/informacija u kontekstu odgovorne organizacijske jedinice. Izgled inicijalna Tablica korelacije prikazana je na slici 5.

Tip IT servisa	Naziv IT servisa	Dio IS-a	Modul	Informacije pružao	Vlasnik podataka (OJ)
Aplikativni - eksternalizirani	Pisarnica	Informacijski sustav upravljanja dokumentacijom (ISUD)	N/A	SM	Odjel pravnih poslova
Aplikativni - eksternalizirani	Plavo gorivo	0	0	0	Odjel za odobrenje isplata
Aplikativni - eksternalizirani	Računovodstveni sustav pretpristupnih fondova	Računovodstveni sustav	N/A	BĐ	Odjel za računovoodstvo
Aplikativni - eksternalizirani	Rizinica	Informacijski sustav strukturne potpore (ISSP)	N/A	BĐ	Sektor za strukturnu potporu
Aplikativni – kupljeni	*Javne web stranice*	N/A	N/A	SM	Odjel za izvještavanje
Aplikativni – kupljeni	*Kontrola prolaza*	N/A	N/A	JV	Sektor za informacijsko upravljanje
Aplikativni – kupljeni	*SharePoint*	N/A	N/A	SM	Sektor za informacijsko upravljanje
Aplikativni – kupljeni	*Sustav za reviziju*	N/A	N/A	0	Sektor za unutarnju reviziju
Aplikativni – vanjski razvoj	*agronet*	N/A	N/A	RB	Sektor za izravnu potporu
Aplikativni – vanjski razvoj	*Aplikacija za mliječne kvote*	Informacijski sustav upravljanja tržištem (ISUT)	0	0	Sektor za tržišnu potporu
Aplikativni – vanjski razvoj	*ARKOD*	Informacijski sustav za administraciju izravnih plaćanja (ISAP)	Modul 2	SM	Sektor za registre
Aplikativni – vanjski razvoj	*Daljinsko istraživanje*	Informacijski sustav za administraciju izravnih plaćanja (ISAP)	0	RB	Sektor za kontrolu
Aplikativni – vanjski razvoj	*EU trgovinske mjere*	Informacijski sustav upravljanja tržištem (ISUT)	0	0	Sektor za tržišnu potporu
Aplikativni – vanjski razvoj	*Financijski sustav - garancije*	Financijski sustav	N/A	RB	Sektor za financije
Aplikativni – vanjski razvoj	*Financijski sustav - plaćanje*	N/A	N/A	SM	Sektor za financije
Aplikativni – vanjski razvoj	*Financijski sustav - voucheri*	Financijski sustav	N/A	RB	Sektor za financije
Aplikativni – vanjski razvoj	*Interni računovodstveni sustav Agencije*	Računovodstveni sustav	N/A	SM	Sektor za financije
Aplikativni – vanjski razvoj	*Jedinstveni zahtjev*	Informacijski sustav za administraciju izravnih plaćanja (ISAP)	0	0	Sektor za izravnu potporu
Aplikativni – vanjski razvoj	*Kadrovska*	N/A	N/A	0	Sektor općih i pravnih poslova
Aplikativni – vanjski razvoj	*Kontrola na terenu*	Informacijski sustav za administraciju izravnih plaćanja (ISAP)	0	RB	Sektor za kontrolu
Aplikativni – vanjski razvoj	*Nacionalne ruralne mjere*	Informacijski sustav strukturne potpore (ISSP)	0	0	Sektor za strukturnu potporu
Aplikativni – vanjski razvoj	*Referentne cijene*	Informacijski sustav strukturne potpore (ISSP)	N/A	0	Sektor za strukturnu potporu
Aplikativni – vanjski razvoj	*Registar prava na plaćanje*	Informacijski sustav za administraciju izravnih plaćanja (ISAP)	0	0	Sektor za izravnu potporu
Aplikativni – vanjski razvoj	*Sustav za poslovno izvješćivanje*	Sustav za poslovno izvješćivanje	N/A	0	Odjel za izvještavanje
Aplikativni – vanjski razvoj	*Trgovinska Internet aplikacija*	Informacijski sustav upravljanja tržištem (ISUT)	0	0	Sektor za tržišnu potporu
Aplikativni – vanjski razvoj	*Upisnik poljoprivrednih gospodarstva*	Informacijski sustav za administraciju izravnih plaćanja (ISAP)	0	RB	Sektor za registre
Aplikativni - vlastiti razvoj	*Help desk sustav*	N/A	N/A	SM	Sektor za informacijsko upravljanje
Infrastrukturni	*Anti-malver sustav*	N/A	N/A	JV	Sektor za informacijsko upravljanje
Infrastrukturni	*Elektronička pošta*	N/A	N/A	JV	Sektor za informacijsko upravljanje
Infrastrukturni	*File servis*	N/A	N/A	JV	Sektor za informacijsko upravljanje
Infrastrukturni	*FTP servis*	N/A	N/A	JV	Sektor za informacijsko upravljanje
Infrastrukturni	*Imenički servis*	N/A	N/A	JV	Sektor za informacijsko upravljanje
Infrastrukturni	*Interna računalna mreža*	N/A	N/A	JV	Sektor za informacijsko upravljanje
Infrastrukturni	*Interna telefonija*	N/A	N/A	JV	Sektor za informacijsko upravljanje
Infrastrukturni	*PKI sustav*	N/A	N/A	JV	Sektor za informacijsko upravljanje
Infrastrukturni	*Pristup Internetu*	N/A	N/A	JV	Sektor za informacijsko upravljanje
Infrastrukturni	*Sustav jedinstvene autentikacije*	N/A	N/A	0	Sektor za informacijsko upravljanje
Infrastrukturni	*Veza prema MPRRR*	N/A	N/A	JV	Sektor za informacijsko upravljanje
Infrastrukturni	*Virtualizacijski servis*	N/A	N/A	JL	Sektor za informacijsko upravljanje
Infrastrukturni	*VPN*	N/A	N/A	JL	Sektor za informacijsko upravljanje
Uslužni IT servisi	*Mrežni nadzor*	N/A	N/A	JV	Sektor za informacijsko upravljanje
Uslužni IT servisi	*Sigurnosna pohrana*	N/A	N/A	JL	Sektor za informacijsko upravljanje
Uslužni IT servisi	*Update servis*	N/A	N/A	JL	Sektor za informacijsko upravljanje
Uslužni IT servisi	*Video nadzor*	N/A	N/A	JV	Sektor za informacijsko upravljanje

Tablica 5 - Inicijalna Tablica korelacije IT servisa i poslovnih funkcija Agencije (Izvor: vlastiti rad)

Za ovu tablicu je karakteristično da je poredana po tipovima informatičkih servisa a da je za svaki informatički servis dodijeljen atribut poslovne funkcije i vlasništvo nad podacima u kontekstu organizacijske jedinice. Time smo odredili poslovne funkcije i aktivnosti od interesa za analizu utjecaja na poslovanje primijenjene na informatičke servise.

Tablica korelacije Informatičkih servisa, poslovnih funkcija i aktivnosti Agencije u obliku matrice, nalazi se u Prilogu C.

4.1.3 Određivanje utjecaja prekida poslovnih aktivnosti na poslovanje Agencije

Određivanje utjecaj prekida pojedine aktivnosti na poslovanje Agencija provest će se kroz procjenu operativnog i financijskog utjecaja tokom vremena kao i određivanja zahtijevanih vremena oporavka. Na osnovu procijenjenih parametara bit će moguće definirati kritične poslovne aktivnosti a samim tim i kritične informatičke servise na koje će se preslikati najzahtjevnija vremena oporavka poslovnih aktivnosti koje podržavaju.

4.1.3.1 Razine kritičnosti

Da bismo odredili prioritete i značaj oporavka poslovnih funkcija i aktivnosti kompanije za osiguranje neprekinutosti poslovanja, potrebno je najprije definirati razine kritičnosti koje ćemo dodijeliti poslovnim funkcijama i aktivnostima tvrtke. Moguće je definirati bilo koje razine kritičnosti koje smatramo primjerenim imajući pri tome na umu da su one jasno definirane i da nema preklapanja područja koja definiraju. Jedna od mogućih i relativno široko prihvaćena kategorizacija kritičnosti je slijedeća:

- Razina 1: Kritične funkcije - Kritično
- Razina 2: Suštinske funkcije - Vitalno
- Razina 3: Neophodne funkcije - Važno
- Razina 4: Poželjne funkcije - Nebitno

Kritične funkcije su oni procesi i funkcije koje imaju najveći utjecaj na poslovanje tvrtke i najveću razinu prioriteta kod oporavka. Gotovo svaki pojedini zaposlenik kompanije ima svoj vlastiti sud o kritičnosti funkcija za odvijanje poslovanja. Svrha je prikupiti sve te podatke i procijeniti kritičnost funkcija kompanije iz organizacijske perspektive. Oni procesi i funkcije koji se moraju odvijati da bi tvrtka odnosno organizacija poslovala predstavljaju Kritične funkcije. Odgovori na pitanje zaposlenicima (bilo kroz ankete, intervjue ili radionice); "Koje tri od pet stvari bi najprije trebalo napraviti u njihovom odjelu nakon prekida?", omogućuju najbolji način identifikacije kritičnih funkcija. Iz IT perspektive, ispad računalske mreže, sustava ili aplikacije koji su kritični uzrokovali bi ozbiljne zastoje u poslovanju. Takvi zastoji obično imaju značajne zakonske i financijske posljedice. Tolerancija takvih ispada je vrlo niska i iskazuje se uglavnom u satima.

Suštinske funkcije je kategorija koja pokriva područje između Kritičnih i Neophodnih funkcija. Možemo zaključiti da su neke funkcije kritične a neke izuzetno važne i moraju biti uspostavljene odmah iza kritičnih. U takve funkcije možemo ubrojiti npr. obradu plaća. Ta funkcija zasigurno nije kritična za oporavak poslovanja ali je od vitalne važnosti za funkcioniranje kompanije nakon oporavka. Iz IT perspektive to su sustavi i komponente koji sučeljavaju s kritičnim funkcijama. Zahtjevi za oporavak se mjere u satima ili najviše dan do dva.

Neophodne funkcije neće utjecati na poslovanje u kraćem periodu ali će na duži period imati značajan utjecaj na poslovanje. Iz IT perspektive, ovakvi sustavi mogu uključivati elektroničku poštu, pristup Internetu i ostali poslovni alati koji se koriste kao podrška funkciji ili procesu. Zahtjevi za oporavak se mjere u danima ili tjednima.

Poželjne funkcije su one razvijene tokom vremena da podrže male i povremene funkcije. Nisu neophodne u bližoj budućnosti kao ni za oporavak poslovanja. Vrlo često su ovakve funkcije razvijene usputno i potrebno ih je revidirati i uspostaviti na efikasniji način. U nekim slučajevima prekid poslovanja jest dobra prilika da se ovo i učini. Zahtjevi za oporavak se izražavaju u tjednima pa čak i u mjesecima.

4.1.3.2 Zahtjevi za vremenom oporavka

Kako norma ISO/IEC 22301:2012 propisuje, potrebno je procijeniti dva najvažnija parametra:

- **Ciljano vrijeme oporavka** (***engl. Recovery Time Objective - RTO***) – krajnje vrijeme unutar kojega je potrebno osposobiti minimalni skup funkcionalnosti poslovnih procesa kako ne bi nastali neprihvatljivi gubici i kompromitirala održivost poslovanja
- **Maksimalna tolerancija gubitka podataka** (***engl. Recovery Point Objective – RPO***) – točka u vremenu prije koje svi pohranjeni podaci moraju biti sigurno očuvani tj. ciljana frekvencija izrade pričuvne pohrane podataka kako bi u slučaju gubitka podataka, gubici sveli na prihvatljivu razinu

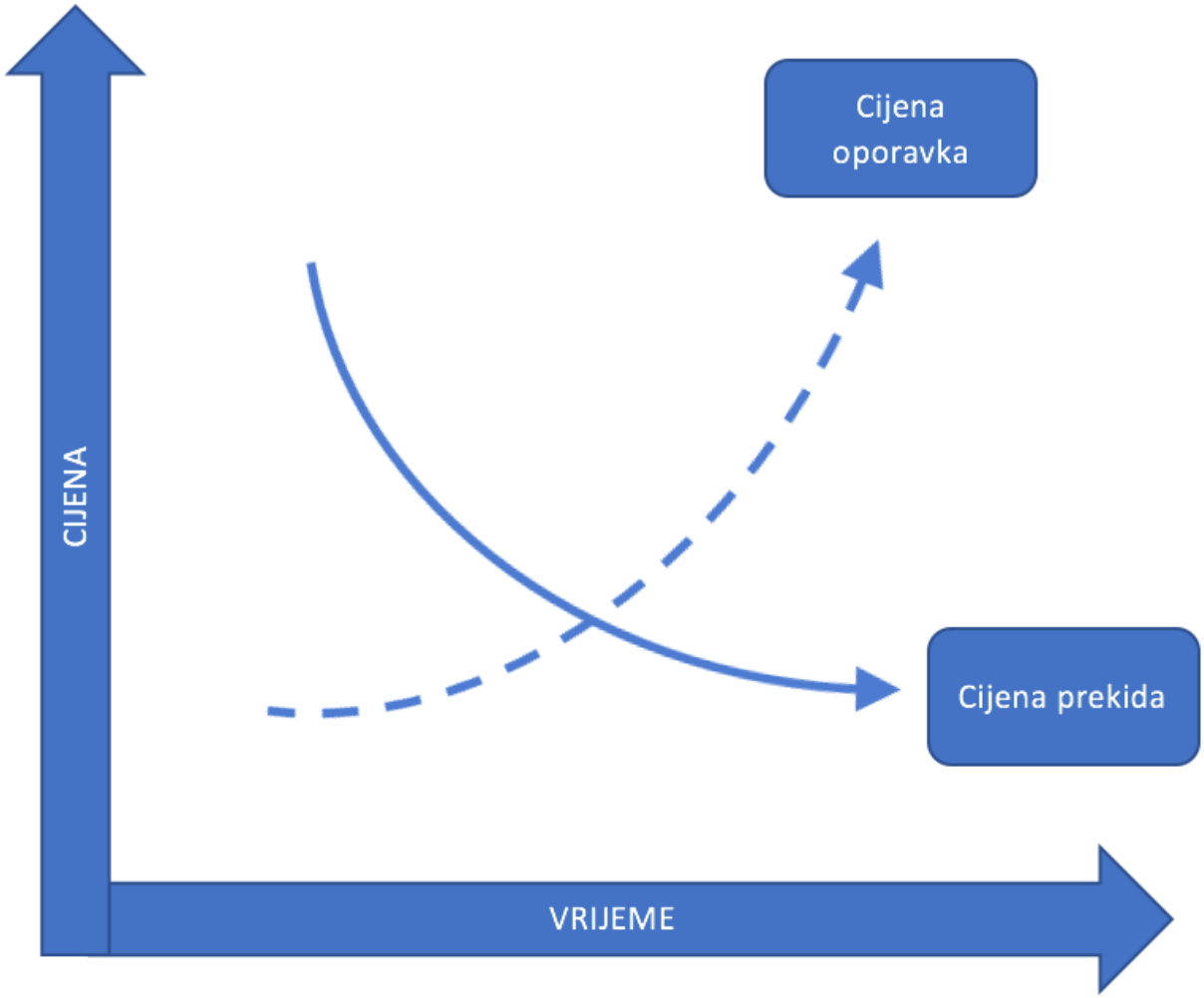
Zadovoljenje RPO parametara se može promatrati iz dva aspekta, prvi dostupnost podataka u slučaju ispada i drugi očuvanje integriteta prilikom njenog narušavanja.

Dostupnost podataka se postiže redundantnim kopijama, bilo na trake, disk ili bilo koji drugi medij.

Zadovoljenje RTO parametara govori o razlici u vremenu koje je trenutno potrebno za uspostavu poslovnih procesa nakon ispada. Smanjenje vremena oporavka poslovnih procesa i približavanje ciljanom vremenu oporavka (RTO) se postiže na razne načine od kojih su najčešći sljedeći:

- uspostava redundancije,
- priprema i osigurava potrebnih preduvjeta za brži oporavak,
- priprema rezervne opreme,
- edukacija djelatnika,
- izrada IT arhitekture koja može automatski ili poluautomatski iskoristiti uspostavljanu redundanciju.

Cijena oporavka i troškovi uzrokovani prekidom su u obrnuto proporcionalnom odnosu. Vrlo lako ćemo primijetiti da što duže prekid poslovanja traje da su troškovi uzrokovani prekidom veći. Isto tako što je zahtijevano vrijeme oporavka duže, to je cijena oporavka manja kao što je prikazano na slici 11. Potrebno je težiti optimalnom odnosu ovih dviju veličina.



Slika 11 - Odnos zahtijevanog vremena oporavka i cijene prekida. Sjecište krivulja predstavlja optimalni odnos troškova prekida i troškova oporavka (Izvor: vlastiti rad prema [17])

Minimalne razine na kojoj se aktivnost mora odvijati nakon obnove kao i količina podataka čiji gubitak se može tolerirati u nekim zahtjevima upravljanja neprekidnošću poslovanja poznato je kao RPO – *Recovery Point Objective* parametar i važan je za određivanje strategije odgovora na prekide poslovanja tj. određivanje zahtijeva na neprekidnost poslovanja i izvan su opsega analize utjecaja na poslovanje.

4.1.3.3 Određivanje utjecaja

Treba imati na umu da prekid poslovanja može biti uzrokovan čitavom paletom mogućih neželjenih događaja pa se tako i potencijalni utjecaj na poslovanje može manifestirati u raznim područjima. Ovdje ćemo pokušati utvrditi područja utjecaja, za čije određivanje ćemo trebati prikupiti i analizirati različite podatke i uzeti ih u obzir u postupku procjene utjecaja prekida poslovne aktivnosti. Norme iz ovog područja nalažu da je potrebno procijeniti različite utjecaje i to u slijedećim područjima;

- Utjecaj na zaposlenike i javnu dobrobit,
- Utjecaj od kršenja zakonskih i regulatornih zahtjeva,
- Utjecaj na reputaciju,
- Utjecaj na financijsku održivost,
- Utjecaj od degradacije kvalitete proizvoda ili usluga,
- Utjecaj na okoliš itd…

Tako nalaže da je potrebno dokumentirati pristup procjeni utjecaja prekida kao i nalaza i zaključaka.

Da bi dovoljno precizno odredili utjecaj prekida pojedinih poslovnih funkcija i aktivnosti, a također i udovoljili zahtjevu norme, potrebno je posvetiti dužnu pažnju definiciji koje podatke je potrebno prikupljati i s kojom svrhom te kako vrednovati utjecaj iz prikupljenih podataka. Podaci koji mogu biti značajni za analizu utjecaja na poslovanje s kratkim opisom svrhe prikupljanja nabrojeni su u slijedećoj tablici. Odmah su navedene i podaci nužni za primjenu na informatičke servise. Nabrojeni podaci od značaja nisu konačni i popis može biti modificiran sukladno potrebama kompanije. Tablica 6 predstavlja područja od interesa za procjenu kritičnosti poslovnih funkcija i aktivnosti.

Podaci od značaja	Opis	Ovisnost o IT-u
Poslovna funkcija ili aktivnost	Kratak opis poslovne funkcije ili aktivnosti.	Navesti osnovne IT servise koji je podržavaju.
Ovisnosti	Opisati ovisnosti o ovoj funkciji/aktivnosti. Što su ulazi i izlazi? Što se mora desiti ili biti raspoloživo da se ova funkcija odvija? Koji ulazi su zahtijevani za odvijanje ove funkcije iz internog ili eksternog izvora? Kako bi prekid ove funkcije utjecao na ostale poslovne funkcije? Kako i kad bi se ovaj prekid odrazio na ostale funkcije?	Opisati IT sustave koji utječu ili na koje utječe ova poslovna funkcija. Da li postoje bilo kakve interne ili eksterne ovisnosti?
Ovisnosti o resursima	Da li je ova poslovna funkcija ovisna o nekoj ključnoj poslovnoj funkciji. Ako jest o kojoj i do kog razmjera? Da li je ovisna o nekim posebnim resursima? Ako jest, o kojima i do kog razmjera (ugovori, specijalna oprema itd)	Opisati IT sustave o kojima je ova funkcija posredno ovisna.
Ovisnost o osoblju	Da li je funkcija ovisna o specijalnim vještinama, znanjima ili pozicijama. Koje su ključne pozicije i uloge pridružene ovoj funkciji? Što bi se dogodilo kad bi bili neraspoloživi?	Opisati ključne uloge znanja, iskustva, uvjerenja potrebna za rad s IT sustavom.
Profil utjecaja	Kad se ova funkcija odvija? Sezonski, dnevno, kvartalno, svaki sat? Da li je ova funkcija posebno rizična u specifično vrijeme dana ili tjedna?	Opisati kritično vrijeme za ovu funkciju za ovisne IT sustave.

	Da li je poslovanje posebno ugroženo ako se ova funkcija ne odvija u neko posebno vrijeme (prijava poreza,..)?	
Financije	Ako se ova funkcija ne odvija, kakav bi bio financijski utjecaj na poslovanje? Kad bi se financijski utjecaj osjetio ili primijetio? Da li bi bio jednokratan ili trajan?	
Oporavak	Koji resursi su neophodni za potporu ove funkcije? Koliko resursa je potrebno i u kom vremenu (telefoni, stolovi, računala, štampači ..)?	Koji resursi, znanje i vještine bi bile potre- potrebne za oporavak IT sustava koji su potrebni za uvu funkciju?
Vrijeme oporavka	Koje je minimalno vrijeme potrebno za oporaviti ovu funkciju ako je u prekidu. Koje je maksimalno vrijeme koje ova funkcija može biti neraspoloživa?	Koliko je potrebno za oporavak, zamjenu ili rekonfig uraciju IT sustava?
SLA	Da li postoje SLA povezani s ovom funkcijom? Koji su zahtjevi i metrika tih SLA. Kako će prekid ove funkcije utjecati na SLA.	Kako će prekid funkcije utjecati na IT SLA? Kako eksterni SLA utječe na IT sustava?
Tehnologija	Koji HW, SW, aplikacije, ili druge tehnološke komponente su potrebne za podršku i održavanje ove funkcije? Kakav bi bio utjecaj?	Koji IT resursi su potrebni za podršku ove funkcije?
Zaobilazne procedure	Da li su uspostavljene određene ručne procedure? Da li bi one omogućile odvijanje funkcije u slučaju ispada IT sustava? Koliko dugo se funkcija može odvijati ručnim procedurama? Ukoliko nisu uspostavljene, da li je razumno uspostaviti ih?	Da li postoje neke IT zaobilazne procedure? Ako da, kako se mogu uspostaviti?

Udaljeni rad	Može li se ova funkcija obavljati udaljeno, bilo sa druge lokacije ili od doma?	Može li se ova funkcija raditi daljeno s IT perspektive?
Prebacivanje posla	Da li je moguće prebaciti poslove u neku drugu poslovnu jedinicu koja nije u prekidu?	Da li postoje drugi IT sustavi ili komponente koje se mogu koristiti?
Zapisi poslovnih podataka	Gdje su poslovni podaci pohranjeni? Da li su u ovom trenutku izrađene sigurnosne kopije? Ako jesu, kako, gdje i kojom frekvencijom?	Gdje i kako se spremaju sigurnosne kopije? Da li je trenutni postupak optimalan u odnosu na procjenu rizika?
Prijašnja iskustva prekida	Da li je ova funkcija bila ikad ranije u prekidu? Ako jeste, kakav je bio prekid i koje su bile posljedice. Koja su iskustva izvučena?	Da li je IT iskusio prekid u prošlosti? Koje prirode i trajanja. Što je poduzeto i koja su iskustva?
Ostali podaci od interesa	Koji ostali podaci mogu biti relevantni za ovu funkciju?	Da li postoje neke druge teme IT relevantne?

Tablica 6 - Područja od interesa za procjenu kritičnosti poslovnih funkcija i aktivnosti (Izvor: [5])

Prikupljanje ovih podataka za sve poslovne funkcije i aktivnosti omogućava temeljito razumijevanje poslovanja, ključnih funkcija i posljedica u slučaju prekida ovih funkcija. Kritičnost poslovnih funkcija definirana u ovoj fazi procjene i potencijalni rizici kojima je naše poslovanje izloženo predstavljaju osnovu za određivanje strategije umanjenja rizika.

Poteškoća s analizom utjecaja na poslovanje jest u tome što može proizvesti ogromnu količinu podataka koje je potrebno povezati, sortirati, procijeniti i analizirati. Za ovo ne postoji jednostavan recept niti prečac, ali je vrlo važno imati na umu krajnji rezultat koji

želimo dobiti a to je identifikacija ključnih funkcija i aktivnosti u našoj kompaniji za obavljanje poslovanja. Za sada je potrebno shvatiti što je apsolutno nužno za održanje našeg poslovanja. Nakon toga se možemo posvetiti ostalim, manje kritičnim funkcijama i procesima.

4.1.3.4 Načini prikupljanja podataka za analizu utjecaja na poslovanje

Najprikladniji načini prikupljanja podataka jesu kroz intervjue, upitnike ili radionice sa vlasnicima procesa tvrtke. Bilo koji od ovih načina jest određeni oblik grupnog intervjua. Slijedeći mogući način može biti istraživanjem i pregledom dokumentacije kompanije, ali takav način se preporučuje samo kao nadopuna podacima prikupljena direktnim kontaktom s ekspertima.

4.1.3.4.1 Upitnici

Upitnici mogu biti vrlo prikladan način za prikupljanje podataka od eksperata tvrtke. Najteži dio jest izrada upitnika koji će biti osmišljeni, jasni, lako razumljivi i koji će se lako popunjavati. Prednosti ove metode su konzistentni, fokusirani i koncizni odgovori. Stručnjaci mogu popunjavati upitnike tj. odgovarati na pitanja o njihovim poslovnim funkcijama, jedinicama i procesima u vrijeme koje im odgovara čime se povećava odziv i sudjelovanje većeg broja stručnjaka. Također je važno objasniti sudionicima svrhu upitnika, pogotovo na način da sudjelovanje donosi i neke pogodnosti i njima samima, kao i sam proces popunjavanja.

4.1.3.4.2 Intervjui

Ukoliko se prikupljanje provodi putem intervjua, također je potrebno pripremiti pitanja koja će biti okosnica za vođenje intervjua. Svaki intervju mora slijediti predefinirani tok i pitanja postavljena svakom sudioniku moraju biti ista.

4.1.3.4.3 Radionice

I kod ove metode možemo se opredijeliti za izradu predefiniranih pitanja kako bi se osigurali da su sve skupine podataka od interesa obuhvaćene. Potrebno je dogovoriti vrijeme i prostor, sudionike odgovarajuće razine kao i njihov pristanak za sudjelovanje na radionicama. Poželjno je izraditi jasan sadržaj radionice i unaprijed ga distribuirati sudionicima, ciljeve radionice i zahtijevane izlaze. Rezultati radionice moraju biti dobro dokumentirani a sudionici moraju imati prigodu provjeriti ih zbog eventualnih grešaka ili propusta.

4.1.3.5 Prikupljanje podataka i način procjena utjecaja u Agencija

Uzimajući u obzir da je cilj provesti analizu utjecaja na poslovanje u Agenciji s primjenom na informatičke servise, potrebno je prilagoditi prikupljane podataka tom cilju. Kako smo već korelacijom informatičkih servisa i poslovnih funkcija i aktivnosti odredili poslovne funkcije i aktivnosti koje su u fokusu naše analize potrebno je prikupljanje podataka usmjeriti na one preko kojih ćemo moći procijeniti utjecaj na poslovanje uslijed prekida informatičkog servisa koji tu poslovnu funkciju ili aktivnost podržava i samim tim odrediti razinu kritičnosti neprekidnosti samog informatičkog servisa. Podaci koje ćemo prikupljati, osim razine kritičnosti moraju dati odgovor i o zahtijevanim vremenima oporavka poslovne funkcije ili aktivnosti odnosno u konačnici informatičkog servisa a također moramo prikupiti podatke koje će eventualno korigirati inicijalnu Tablicu korelacije informatičkih servisa i poslovnih funkcija.

4.2 Maksimalna tolerancija gubitka podataka – RPO

Zadovoljnost RPO parametara se može promatrati iz dva aspekta, prvi dostupnost podataka u slučaju ispada i drugi očuvanje integriteta prilikom njenog narušavanja. Dostupnost podataka se postiže redundantnim kopijama, bilo na trake, disk ili bilo koji drugi medij. Ono što je bitno napomenuti je da sinkrona replikacija podataka i podatkovni grozdovi osigurava RPO od 0 ali samo po pitanju dostupnosti ne i integriteta podataka. Integritet se štiti redundantnim kopijama koje se ne rade sinkrono već sa vremenskim pomakom.

Sukladno tome napravljena je usporedba trenutno korištenih mehanizama zaštite integriteta i dostupnosti podataka sa definiranim za sve IT servise.

Provedena analiza (tablica 7) ukazuje da većina IT servisa ne zadovoljava zahtjeve za dostupnost podataka. Zadovoljavanje integriteta predstavlja problem za kritične IT servise, jer učestalost sigurnosne pohrane podataka je manja od zahtijevanog RPO parametara, dodati sigurnosni mehanizmi kao npr. journaling ne postoje. Ukoliko se odluči da ovo predstavlja neprihvatljivi rizik potrebno je strategijom kontinuiteta poslovanja odrediti najprimjereniji način adresiranja ovog problema.

Dio specifičnih rizika je adresiran kroz pojedine sigurnosne mjera opisane niže do većina smjernica za zadovoljavanje RPO parametara je definirano u dokumentu Strategija kontinuiteta poslovanja.

Tip IT servisa	Naziv IT servisa	RPO,h	Zadovoljeno
Aplikativni – vanjski razvoj	**agronet**	0	DA (transakcijski zapisi), al ne u slučaju korupcije eksternog diskovnog sustava, pouzdano 24h
Aplikativni – vanjski razvoj	**ARKOD**	0	Generalno NE, pouzdano samo 24h. U slučaju manje havarije atributni podaci iz Upisnika se mogu vratiti pomoću transakcijskih zapisa
Aplikativni – vanjski razvoj	**Financijski sustav - plaćanje**	0	NE, trenutno 24h
Infrastrukturni	**Interna računalna mreža**	0	NE, trenutno se radi ručni backup nakon većih promjena i pohranjen je u KING-u
Infrastrukturni	**Pristup Internetu**	0	NE, trenutno se radi ručni backup nakon većih promjena i pohranjen je u KING-u
Aplikativni – kupljeni	**SharePoint**	0	Trenutno nema backup-a
Aplikativni – vanjski razvoj	**Upisnik poljoprivrednih gospodarstva**	0	DA (transakcijski zapisi), al ne u slučaju korupcije eksternog diskovnog sustava, pouzdano 24h
Infrastrukturni	**Virtualizacijski servis**	0	NE, trenutno se radi ručni backup nakon većih promjena
Infrastrukturni	**VPN**	0	NE, trenutno se radi ručni backup nakon većih promjena i pohranjen je u KING-u
Infrastrukturni	**Elektronička pošta**	3	NE, trenutno 24h
Infrastrukturni	**File servis**	3	NE, trenutno 24h
Aplikativni – kupljeni	**Javne web stranice**	3	NE, trenutno 24h
Aplikativni – vanjski razvoj	**Financijski sustav - voucheri**	4	DA (transakcijski zapisi), al ne u slučaju korupcije eksternog diskovnog sustava, pouzdano 24h
Aplikativni – vanjski razvoj	**Interni računovodstveni sustav Agencije**	4	NE, trenutno 24h
Aplikativni - eksternalizirani	**Računovodstveni sustav pretpristupnih fondova**	4	NE, trenutno 24h
Infrastrukturni	**Veza prema MPRRR**	4	NE, trenutno se radi ručni backup nakon većih promjena i pohranjen je u KING-u
Infrastrukturni	**Interna telefonija**	8	DA, konstantno na SD karticu
Infrastrukturni	**Anti-malver sustav**	24	Trenutno nema backup-a
Aplikativni – vanjski razvoj	**Financijski sustav - garancije**	24	DA, dnevni backup + replikacija
Infrastrukturni	**Imenički servis**	24	DA, dnevni backup + replikacija na drugi DC

Aplikativni – kupljeni	**Kontrola prolaza**	24	Trenutno nema backup-a
Uslužni IT servisi	**Mrežni nadzor**	24	Trenutno nema backup-a
Aplikativni - eksternalizirani	**Pisarnica**	24	DA, dnevni backup
Aplikativni - eksternalizirani	**Riznica**	24	Trenutni računalno nema backup
Uslužni IT servisi	**Sigurnosna pohrana**	24	DA, dnevni backup
Uslužni IT servisi	**Video nadzor**	24	Trenutno nema backup-a
Aplikativni - vlastiti razvoj	**Help desk sustav**	120	Trenutno nema backup-a
Infrastrukturni	**PKI sustav**	120	Radi se kopija Root CA mašine nakon promjene, Issuing CA nema backup
Uslužni IT servisi	**Update servis**	120	Trenutno nema backup-a

Tablica 7 - Maksimalna tolerancija gubitka podataka - RPO (Izvor: vlastiti rad)

4.3 Ciljano vrijeme oporavka - RTO

Zadovoljnost RTO parametara govori o razlici u vremenu koje je trenutno potrebno za uspostavu IT servisa nakon ispada i onog definiranog.

Smanjenje vremena oporavka IT servisa i približavanje ciljanom vremenu oporavka (RTO) se postiže na razne načine od kojih najčešći su:

- uspostava redundancije,
- priprema i osigurava potrebnih preduvjeta za brži oporavak,
- priprema rezervne opreme,
- edukacija djelatnika,
- izrada IT arhitekture koja može automatski ili poluautomatski iskoristiti uspostavljanu redundanciju.

Sukladno tome napravljena je usporedba trenutno korištenih mehanizama zaštite sa traženim za sve IT servise. Generalno govoreći svi IT servisi se mogu restaurirati iz sigurnosne pohrane podataka i originalnih instalacijskih medija na zamjenske poslužitelje. Ovaj postupak uz preduvjet da je raspoloživ adekvatni zamjenski poslužitelj i da je izrađena sigurnosna pohrana traje minimalno 4h, ali potencijalno znatno dulje ukoliko je potrebno oporaviti više IT servisa na taj način zbog uskog grla koji predstavlja sustav za magnetske trake. U koliko se koriste virtualne mašine i unaprijed pripremljene slike tvrdih diskova ovaj postupak može biti provedenu unutar 2h. Fizička instalacija i konfiguracija poslužitelja dodaje dodatnih 2h na postupak.

Najveće usko grlo predstavljaju ljudski resursni potrebni za fizičku instalaciju te uređaj za trake koji ne može obavljati opravak više od nekoliko IT servisa istovremeno. Za sve IT servise koji bi se oporavljali na navedeni način u tablici niže navedeno je da bi oporavak trajao 4-8 sati. Izuzetak su virtualizirani IT servisi za koje se navodi vrijeme od 2h. U slučaju da oporavak zahtjeva nabavu novih poslužitelja vrijeme oporavka prelazi jedan dan. Izrada snapshot-ova virtualnih poslužitelja omogućavala bi oporavak ispod 2h.

Tip IT servisa	Naziv IT servisa	RTO,h	Zadovoljeno
Aplikativni – vanjski razvoj	**agronet**	0	Da, postoji redundancija aplikacijskog i podatkovnog poslužitelja
Aplikativni – vanjski razvoj	**ARKOD**	0	NE, približno 2h za dizanje virtualnih mašina
Infrastrukturni	**Imenički servis**	0	DA, decentralizirana arhitektura
Infrastrukturni	**Interna računalna mreža**	0	DA za središnje mrežne uređaje, ostali + regionalni uredi – dan ili više
Infrastrukturni	**Interna telefonija**	0	Više dana

Infrastrukturni	**Pristup Internetu**	0	NE, ISA 4h, ASA 4h uz rekonfiguraciju preostalog, link do jednog dana prema SLA
Aplikativni – vanjski razvoj	**Upisnik poljoprivrednih gospodarstva**	0	Da u slučaju ispada jednog podatkovnog poslužitelja, inače dan ili više
Infrastrukturni	**Virtualizacijski servis**	0	NE, prebacivanje IT servisa na sekundarni ESX barem 4h
Infrastrukturni	**VPN**	0	NE, min 4h za rekonfiguraciju preostalog Cisco ASA uređaja
Aplikativni – vanjski razvoj	**Financijski sustav - plaćanje**	2	DA, približno 2h za dizanje virtualnih mašina i restauraciju podatka
Infrastrukturni	**File servis**	3	DA, približno 2h za dizanje virtualnih mašina i restauraciju podatka
Aplikativni – kupljeni	**SharePoint**	3	DA, približno 2h za dizanje virtualnih mašina i restauraciju podatka
Infrastrukturni	**Veza prema MPRRR**	3	Moguće, min 4h za rekonfiguraciju preostalog Cisco ASA uređaja
Aplikativni – vanjski razvoj	**Financijski sustav - voucheri**	4	Da u slučaju ispada jednog podatkovnog poslužitelja, inače dan ili više
Aplikativni – vanjski razvoj	**Interni računovodstveni sustav Agencije**	4	DA, približno 2h za dizanje virtualnih mašina i restauraciju podatka
Uslužni IT servisi	**Mrežni nadzor**	4	DA, približno 2h za dizanje virtualnih mašina i restauraciju podatka
Aplikativni - eksternalizirani	**Računovodstveni sustav pretpristupnih fondova**	4	Vjerojatno, prebacivanjem funkcionalnosti na razvojni sustav
Infrastrukturni	**Elektronička pošta**	6	DA, približno 2h za dizanje virtualnih mašina i restauraciju podatka
Uslužni IT servisi	**Sigurnosna pohrana**	6	Više dana za nabavu opreme
Aplikativni - eksternalizirani	**Riznica**	8	Više dana za nabavu opreme
Infrastrukturni	**Anti-malver sustav**	24	DA, približno 4h za dizanje virtualnih mašina i ažuriranje definicija
Aplikativni – vanjski razvoj	**Financijski sustav - garancije**	24	Da u slučaju ispada jednog podatkovnog poslužitelja, inače dan ili više
Aplikativni – kupljeni	**Javne web stranice**	24	DA, približno 4h za dizanje virtualnih mašina i ažuriranje definicija

Aplikativni – kupljeni	**Kontrola prolaza**	24	DA za poslužitelj - približno jedan dan za realokaciju novog računala i instalaciju, NE za kontrolne module
Aplikativni - eksternalizirani	**Pisarnica**	24	DA, približno jedan dan za dizanje svih virtualnih mašina i ažuriranje definicija
Aplikativni - vlastiti razvoj	**Help desk sustav**	120	DA, 2h za presnimavanje aplikacije sa pohranjene lokacije
Infrastrukturni	**PKI sustav**	120	DA, približno jedan dan za dizanje svih virtualnih mašina i ažuriranje definicija
Uslužni IT servisi	**Update servis**	120	DA, približno 4h za dizanje virtualnih mašina i ažuriranje definicija
Uslužni IT servisi	**Video nadzor**	168	DA za poslužitelj - približno jedan dan za realokaciju novog računala i instalaciju

Tablica 8 - Ciljano vrijeme oporavka - RTO (Izvor: vlastiti rad)

Provedena analiza ukazuje da velika većina IT servisa sa RTO parametrom 24 ili više sati zadovoljavaju zahtjeve za brzinu oporavka, dok kritičniji IT servisi ne zadovoljavanju brzinom oporavka kao što je prikazano u tablici 8. Najveće razlike su vidljive u IT servisima koji zahtijevaju kontinuiranu raspoloživosti.

Dodatno je potrebno razmotriti načine oporavka kritičnih mrežnih infrastrukturnih komponenti u slučaju većih fizičkih kvarova. Ovo može uključivati i vlastiti zalihu kritičnih dijelova.

Dio specifičnih rizika je adresiran kroz pojedine sigurnosne mjera opisane niže do većina smjernica za zadovoljavanje RTO parametara je definirano u dokumentu Strategija kontinuiteta poslovanja.

4.4 Identifikacija, vrednovanje i klasifikacija informacijske imovine

Tijekom ranije navedenih intervjua i radionice paralelno sa određivanjem karakteristika IT servisa, koji predstavljaju primarni oblik informacijskih sustava, identificirana i vrednovanja je informacijska imovina. Predstavnici poslovanja su direktno identificirali i vrednovali svu, za njih, bitnu informacijsku imovinu. Dok su djelatnici sektora za informacijsko upravljanje identificirali informaciju imovinu a vrijednosti su preslikane iz poslovne kritičnosti IT servisa koji su procijenili predstavnici poslovanja.

Procjena se provela prema sva tri aspekta informacijske sigurnosti: povjerljivost, integritet i raspoloživost.

Slijedeće tri tablice prikazuju korišteni kriterij za procjenu povjerljivosti, integriteta i raspoloživosti.

Numerička vrijednost	Povjerljivost	
0	**Javno**	Informacije koje su predviđene za javno objavljivanje, odnosno koje se nedvojbeno mogu javno objaviti bez ograničenja.
1	**Interno**	Podaci koji su namijenjeni internoj upotrebi i to bez ograničenja za sve zaposlenike. Ovi podaci se mogu karakterizirati kao osjetljivi ako bi dospjeli u javnost. Podacima mogu pristupiti i osobe koje nisu zaposlenici tvrtke, ali tek uz odobrenje vlasnika informacija. Mjere zaštite sukladne informacijama stupnja tajnosti: „**Ograničeno**“,
2	**Rezervirano**	Podaci koji su namijenjeni internoj upotrebi, ali uz ograničenje pristupa sukladno opisu radnog mjesta. Ovi podaci se mogu karakterizirati kao osjetljivi ako bi dospjeli u javnost. Podacima mogu pristupiti i osobe koje nisu zaposlenici tvrtke, ali tek uz odobrenje vlasnika informacija. Mjere zaštite sukladne informacijama stupnja tajnosti: „**Povjerljivo**“,
3	**Osjetljivo**	Podaci čiji značaj je osjetljiv za Agenciju. Pristup podacima mora biti prethodno eksplicitno odobren od vlasnika za svaki uvid te prilikom pristupa mora biti nedvojbeno ustanovljen identitet zaposlenika. Mjere zaštite sukladne informacijama stupnja tajnosti: „**Tajno**“
4	**Kritično**	Podaci najvišeg značenja za Agenciju. Pristup do ovih podataka imaju samo osobe koje dobiju odobrenje od Ureda ravnatelja uz sigurnosnu provjeru. Mjere zaštite sukladne informacijama stupnja tajnosti: „**Vrlo Tajno**“

Tablica 9 - Kriterij vrednovanja povjerljivosti informacijske imovine (Izvor: vlastiti rad)

Numerička vrijednost	Vrijednost	Integritet
0	**Beznačajna**	Oštećenje, slučajna ili namjerna izmjena **ne utječe na poslovni proces**
1	**Niska**	Oštećenje, slučajna ili namjerna izmjena ne utječe na rezultata poslovnog procesa, nego **uzrokuje manji dodatni interni posao i manje zaostatke u radu**.
2	**Srednja**	Oštećenje, slučajna ili namjerna izmjena uzrokuje probleme u radu, **poslovni proces ne daje željeni rezultat**, mogući financijski problem
3	**Visoka**	Oštećenje, slučajna ili namjerna izmjena uzrokuje veće probleme u radu, **sigurni financijski problem, prekršajnu i kaznenu odgovornost bez reputacijske štete**
4	**Vrlo visoka**	Oštećenje, slučajna ili namjerna izmjena uzrokuje vrlo značajne probleme u radu, **sigurni financijski problem, prekršajnu i kaznenu odgovornost uz znatnu reputacijsku štetu**

Tablica 10 - Kriterij vrednovanja integriteta informacijske imovine (Izvor: vlastiti rad)

Numerička vrijednost	Vrijednost	Raspoloživost
0	**Beznačajna**	Nedostupnost **ne utječe** na poslovni proces
1	**Niska**	Nedostupnost veća **od tjedan dana** uzrokuje značajne probleme u radu
2	**Srednja**	Nedostupnost veća od **3 dana** uzrokuje značajne probleme u radu
3	**Visoka**	Nedostupnost veća od **jednog radnog dana** uzrokuje značajne probleme u radu
4	**Vrlo visoka**	Nedostupnost veća od **4h** uzrokuje značajne probleme u radu

Tablica 11 - Kriterij vrednovanja raspoloživosti informacijske imovine (Izvor: vlastiti rad)

Nakon vrednovanja informacijske imovine izrađen je katalog informacijske imovine u kojem je za svu informacijsku imovinu definirana potrebna razina povjerljivosti, integriteta i raspoloživosti. Dodatno imovina je klasificirana tj. grupirana u obilježja prema osnovnim značajkama i primjenjivosti prijetnji i ranjivosti. Osnovna podjela je na:

- informacije u elektronskom obliku (EDATA),
- informacije u ne-elektronskom obliku (PDATA),
- ljudski resursi (HR),
- hardver (HW),
- okolina i infrastrukturna (IS),
- softver (SW),
- fizička imovina koja ne sadrži informacije (PH),
- vanjski i interne usluge (S).
- Dodatno imovina je podijeljena u 38 podkategorije:

- EDATA - Podaci baze
- EDATA - Tehnička dokumentacija
- HW - Eksterni diskovni sustav
- HW - Elektronski mediji
- HW - Mobilni telefon/Smartphone
- HW - Mrežna oprema
- HW - Mrežna oprema - kritična
- HW - Poslužitelji
- HW - Prijenosna/ručna računala - kritična
- HW - Stolna računala - kritična
- HW - Telefonska centrala / PBX
- IS - Arhiva
- IS - HVAC na kritičnim lokacijama
- IS - Server sala / Data centar
- PDATA - Dokumentacija interna
- PDATA - Dokumentacija klijenata
- PDATA - Dosjei

- PDATA - Interni akti društva
- PDATA - Javno dostupni dokumenti
- PDATA - Operativni dokumenti
- PDATA - Računi / otpremnice / zapisnici
- PDATA - Ugovori
- PH - Alat i oprema
- PH - Kontroleri
- PH - Nadzorne kamere
- PH - Oprema za unos/ispis podataka
- PH - Specijalna oprema
- PH - Vozila
- S - Interni servisi / procesi
- S - Nadležni organi
- S - Treće strane
- S - Ugovorene usluge - vanjske
- SW - DBMS/SUBP
- SW - ERP aplikacije
- SW - Operacijski sustavi
- SW - Sistemsko-upravljački softver
- SW - Virtualni poslužitelji
- SW - Web aplikacije

Ukupno je identificirano 372 komada informacijske imovine, od čega manji dio nije jedinstven već predstavlja različiti pogled i procjenu iste informacijske imovine. Sukladno Pravilniku o uspostavi upravljanja informacijskom sigurnošću, samo informacijska imovina koje je barem po jednom od tri kriterija procijenjena kao visoka ili vrlo visoko se dalje razmatra u procjeni rizika.

4.5 Identifikacija i vrednovanje rizika informacijske sigurnosti

Rizici su identificirani na obilježjima informacijske imovine i IT servisima te je na osnovu toga izrađen katalog sa ukupno 229 rizika, od čega 148 je jedinstveno.

Nakon identifikacije provedeno je vrednovanje parametara rizika sukladno postupku definiranom u Pravilniku o uspostavi upravljanja informacijskom sigurnošću. Korišteni parametri su :

- ocjena mogućnosti pojavljivanja specifičnog rizika- vjerojatnost da će se rizik dogoditi (tablica 12)
- ocjena učinka/utjecaja rizika odnosno posljedice koje ponavljanje rizika može izazvati (tablica 13)
- Vrednovanje vjerojatnosti i utjecaja je napravljeno provedeno prema slijedeće dvije tablice. (tablica 14)

Numerička vrijednost	Vjerojatnost	Opis
1	Niska	Rizik je manje vjerojatan zbog implementiranih sigurnosnih mjera (manje od 1x godišnje)
2	Srednja	Manjak sigurnosnih mjera čini ovaj rizik vrlo vjerojatnim (1x u pola godine)
3	Visoka	Manjak sigurnosnih mjera rezultira učestalom manifestacijom ovog rizika (1x tjedno)

Tablica 12 - Razine vjerojatnosti rizika (Izvor: vlastiti rad))

Numerička vrijednost	Utjecaj	Opis
1	Nizak	Minimalni utjecaj na rad i upravljanje ljudima Minimalan utjecaj na neke usluge/programe; do jednog dana kašnjenje u pružanju usluga. Utjecaj na 2% proračuna Privremena šteta na imovinu Kratkotrajan negativan utjecaj na zajednicu ili okoliš

Numerička vrijednost	Utjecaj	Opis
2	Srednji	Lokalizirana ograničenja u radu ljudi i kršenju kodeksa etike. Kašnjenje u pružanju usluga do jednog tjedna. Utjecaj na 5% proračuna Šteta na imovini koja nije trajna Negativan utjecaj na zajednicu ili okoliš
3	Visok	Veliko ograničenje u radu ključnih procesa Veliki prekršaj u kršenju standarda financijskog upravljanja ili kazneno djelo Prestanak pružanja usluga ili programa na razini države, mjesec dana odgode operativnog djelovanja Utjecaj na 10% i više proračuna. Glavni poslovni ciljevi nisu ostvarivi Gubitak kritičnih usluga, programa ili podataka ili podataka Dugoročan ili totalni gubitak imovine Ogroman utjecaj na zajednicu ili okoliš.

Tablica 13 - Razine utjecaja rizika (Izvor: vlastiti rad)

Uporabom matrice za izračun rizika (vidi tablicu niže), izračunat je ukupni rizik.

RIZIK		**Vjerojatnost**		
Utjecaj		1	2	3
		Niska	Srednja	Visoka
1	Visok	**Srednji**	**Visok**	**Kritičan**
2	Srednji	**Mali**	**Srednji**	**Visok**
3	Mali	**Mali**	**Mali**	**Srednji**

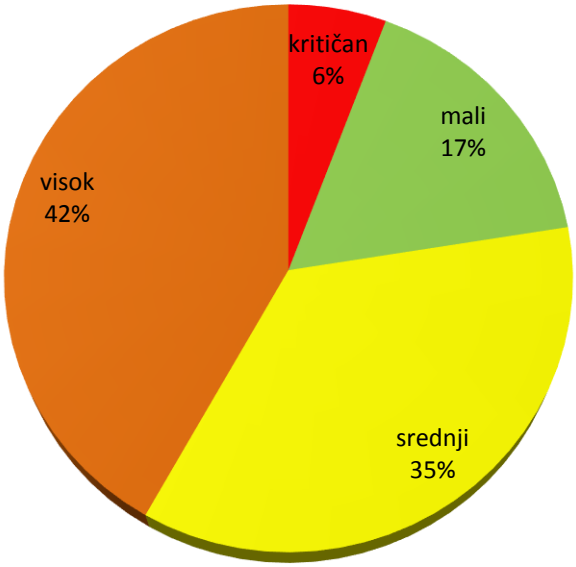
Tablica 14 - Matrica za analizu rizika (Izvor: vlastiti rad)

Procjenjivanje rizika provedeno na temelju podataka prikupljenih tijekom intervjua snimke IT servisa i poznavanje problematike i naravi rizika u Agenciji. Voditelj odjela za informacijsku sigurnosti je provodio ovu aktivnost uz konzultacije sa relevantnim djelatnicima prema potrebi.

4.6 Rezultati analize utjecaja na poslovanje

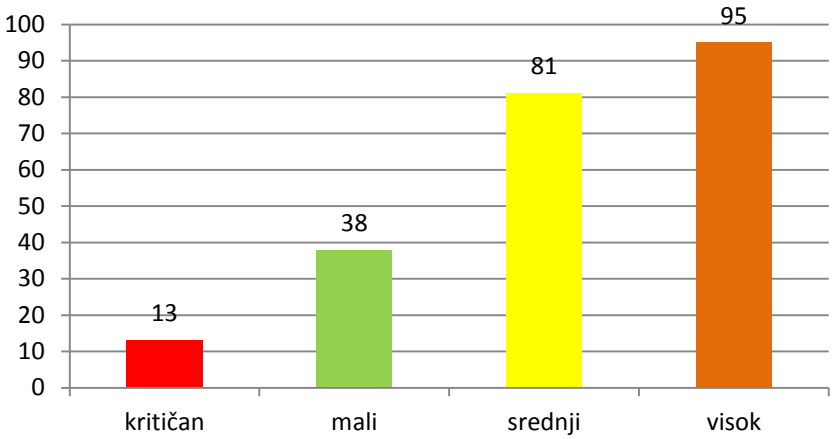
4.6.1 Generalni pregled identificiranih rizika

Sukladno navedenoj metodologiji prema Priručniku za procjenu i upravljanje rizicima informacijske sigurnosti i prikupljenim procijenjenim vrijednostima, izračunati su iznosi rizika. prikazuje broj neprihvatljivih, tj. visokih i vrlo visokih rizika, nasuprot broju prihvatljivih, tj. srednjih i niskih. Slika 12 prikazuje ukupnu raspodjelu identificiranih rizika u njihovom relativnom omjeru. [18]



Slika 12 - Ukupna raspodjela rizika sa relativnim omjerima (Izvor: [18])

Slika 12, prikazuje ukupnu raspodjelu rizika sa apsolutnim brojevima identificiranih rizika.

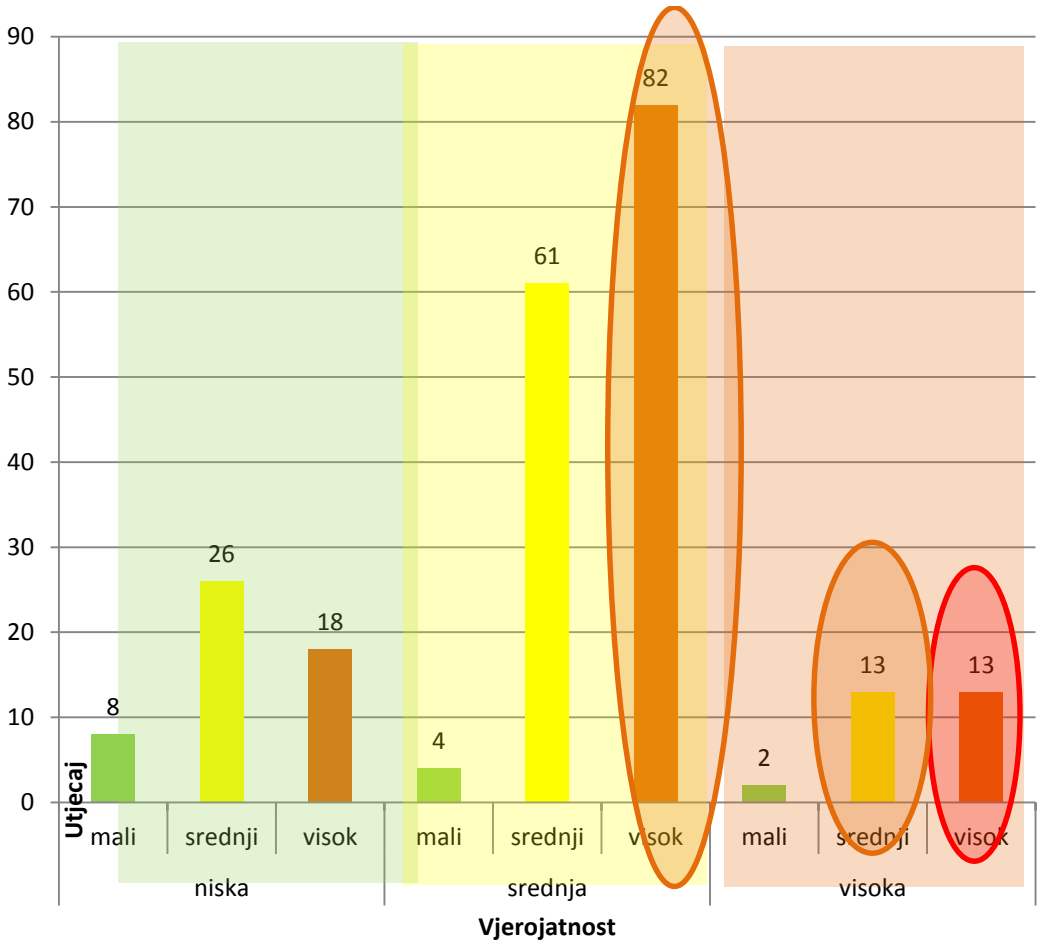


Slika 13 - Ukupna raspodjela rizika sa apsolutnim iznosima

Raspodjela podsjeća na normalnu (Gaussovu razdiobu) sa više izraženim brojem malih vrijednosti rizika. Razlog za ovakvu razdiobu taj što su u katalog rizika stavljani samo direktno identificirani rizici uz sumjerljivi broj vjerojatno primjenjivih rizika. Ovim postupkom se znatno ubrzao postupak vrednovanja uz minimalni rizik ispuštanja relevantnih rizika. Razlog je što se prilikom izrade kataloga rizika radilo filtriranje generalno prihvaćenih rizika za primjenjivost u Agenciji. Dodatno ovim se osiguralo koncentriranje na bitne rizike. Alternativno da je u katalogu korišten vrlo velik broj generalnih rizika znatno veći broj bi bio neprimjenjiv ili već adresiran kontrolama. U tom slučaju raspodjela bi znatno naginjala na stranu malih i srednjih rizika. S obzirom da je nadležnim Priručnikom definirano obavezo adresiranje samo visokih i vrlo visokih rizika, tj. neprihvatljivih rizika, daljnja analiza se prvenstveno odnosni na njih.

Slika 14, prikazuje sumarnu raspodjelu rizika zajedno sa ulaznim vrijednostima procijenjene vjerojatnosti nastupanja te utjecaja. Na osi apscise prikazane su vrijednosti utjecaja te vjerojatnost, dok je na osi ordinate prikazan broj rizika određenih vrijednosti.

Smeđim elipsama označene su vrijednosti koje rezultiraju visokim rizikom, a crvenim one koji rezultiraju kritičnim rizikom.

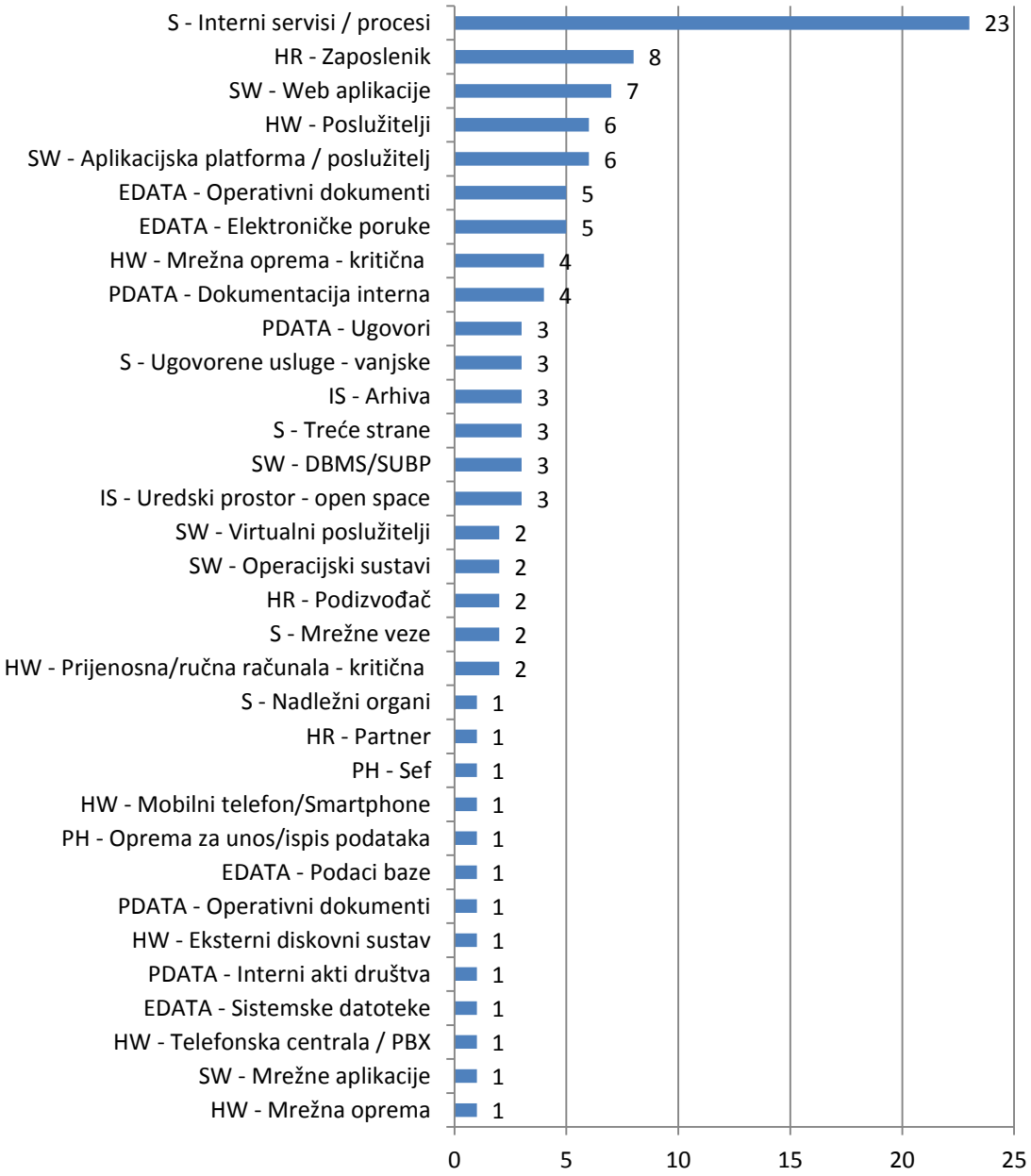


Slika 14 - Ukupna raspodjela rizika prema procijenjenim vjerojatnostima i utjecaju

S obzirom na navedeno, kritični rizici predstavljaju situacije koje je nužno potrebno obuhvatiti definiranjem i primjenom sigurnosnih mjera. Visoki rizici također predstavljaju neprihvatljive rizike, ali s obzirom da su u najvećoj mjeri proizašli iz situacija sa srednjom vjerojatnošću nastupanja, zapravo predstavljaju stvari koje ukazuju na prostor za

dugoročno poboljšanje. Određivanje prioriteta je potrebno napraviti sukladno potencijalnom utjecaju odnosno kritičnosti informacija, IT servisa i infrastrukture.

Slika 15, prikazuje apsolutni broj identificiranih rizika prema obilježju na kojima su identificirani.

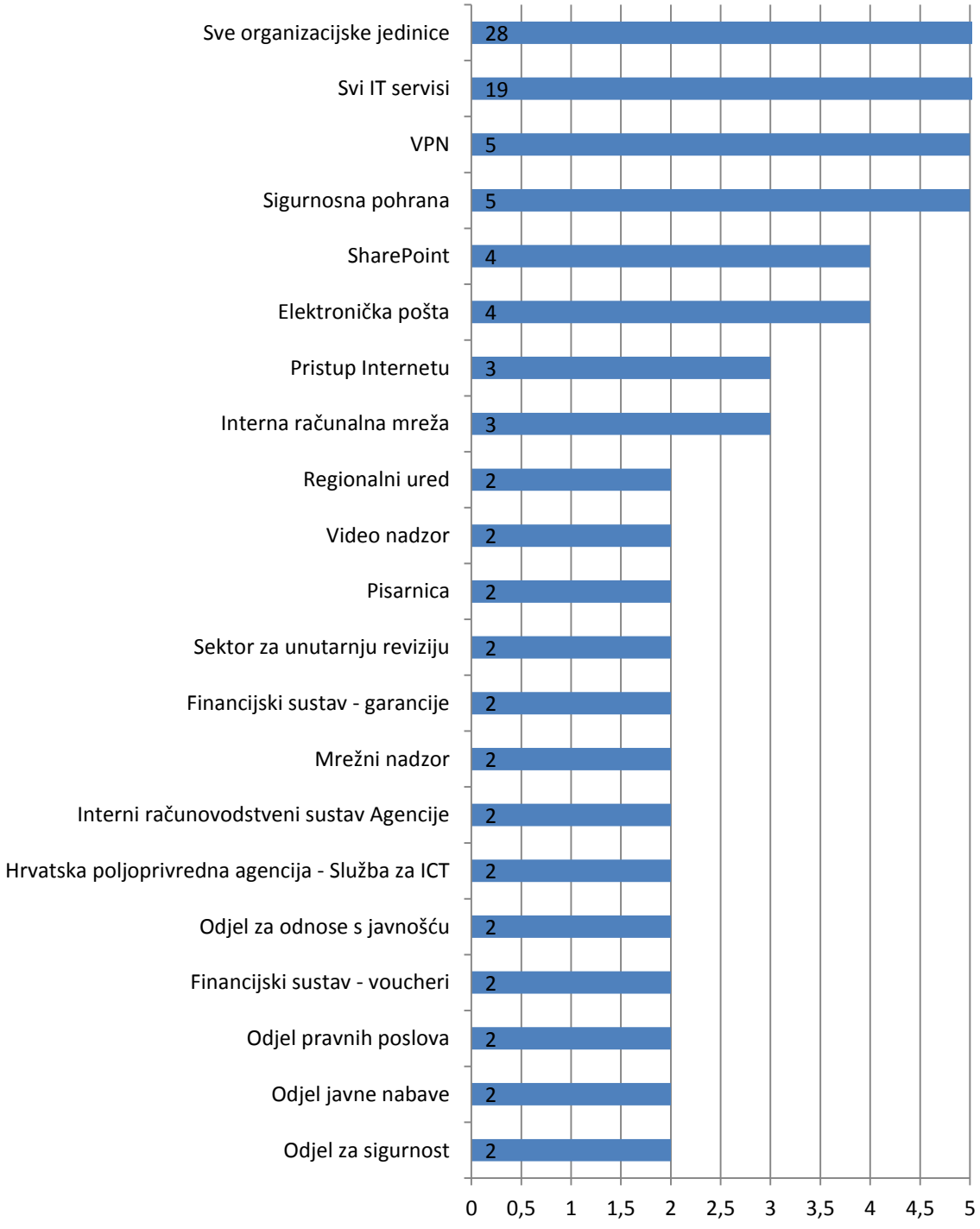


Slika 15 - Raspodjela neprihvatljivih rizika prema obilježjima

Prikazana razdioba ukazuje na činjenicu da je najviše neprihvatljivih rizika (23) identificirano i dodijeljeno internim procesima i servisima što je proizlazi iz činjenice da ta kategorija adresira opće prisutne rizike u svim IT servisima i poslovnim aktivnostima. Razdvajanjem tih rizika na sve IT servise i organizacijske jedinice nepotrebno je, jer bi se multiplicirao broj rizika, što bi vodilo do krivog zaključka. Preostale visoko kritične kategorije su:

- zaposlenici,
- web bazirane aplikacije,
- računalni poslužitelji,
- aplikativni softver i platforme,
- elektronički dokumenti i poruke,
- mrežna oprema te
- fizička dokumentacija.

Slika 16, prikazuje raspodjelu neprihvatljivih rizika prema mjestu identifikacije.



Slika 16 - Raspodjela neprihvatljivih rizika prema mjestu identifikacije

Prikazana razdioba ukazuje na činjenicu da se najviše neprihvatljivih rizika (47) na sve IT servise i poslovne aktivnosti tj da su to zajednički rizici cijelom poslovanju. Ovo je vrlo tipično za sustave za upravljanje informacijskom sigurnošću koji su povojima i upućuje da je prvo potrebno uspostavi generalne okviri ponašanje i upravljanja i time adresirati ove rizike. Jedno kad sustav sazrije očekuje se više specifičnih rizika. Izuzev navedenog najčešće mjesto identificiranih neprihvatljivih rizika su IT servisi „VPN“, „sigurnosna pohrane“„elektronička pošta“, „SharePoint“, „interna računalna mreža“, „pristup Internetu“ te potom neke poslovne aktivnosti u određenim organizacijskim jedinicama te IT servisi sa 2 ili manje neprihvatljiva rizika. Analiza visokih rizika je u Prilogu D.

Tip IT servisa	Naziv IT servisa	Dio IS-a	Vlasnik podataka (OJ)	Vlasnik aplikacije	Ukupan broj korisnika	RTO,h	RPO, h	Povjerljivost	Cjelovitost	Raspoloživost
Infrastrukturni	*Imenički servis*	N/A	Sektor za informacijsko upravljanje	DM	800	0	24	Kritično	Vrlo visoka	Vrlo visoka
Infrastrukturni	*Interna računalna mreža*	N/A	Sektor za informacijsko upravljanje	DM	400	0	0	Kritično	Vrlo visoka	Vrlo visoka
Infrastrukturni	*Interna telefonija*	N/A	Sektor za informacijsko upravljanje	DM	400	0	8	Osjetljivo	Srednja	Vrlo visoka
Infrastrukturni	*Pristup Internetu*	N/A	Sektor za informacijsko upravljanje	DM	800	0	0	Kritično	Vrlo visoka	Vrlo visoka
Infrastrukturni	*Sustav jedinstvene autentikacije*	N/A	Sektor za informacijsko upravljanje	DM	800	0	0	Kritično	Vrlo visoka	Vrlo visoka
Infrastrukturni	*Virtualizacijski servis*	N/A	Sektor za informacijsko upravljanje	DM	0	0	0	Kritično	Vrlo visoka	Vrlo visoka
Infrastrukturni	*VPN*	N/A	Sektor za informacijsko upravljanje	DM	300	0	0	Kritično	Vrlo visoka	Vrlo visoka
Aplikativni – vanjski razvoj	*agronet*	N/A	Sektor za izravnu potporu	SKS	10200	0	0	Kritično	Vrlo visoka	Vrlo visoka
Aplikativni – vanjski razvoj	*Aplikacija za mliječne kvote*	Informacijski sustav upravljanja tržištem (ISUT)	Sektor za tržišnu potporu	SŠ		0	0	Osjetljivo	Visoka	Vrlo visoka
Aplikativni – vanjski razvoj	*ARKOD*	Informacijski sustav za administraciju izravnih plaćanja (ISAP)	Sektor za registre	MŠ	0	0	0	Kritično	Vrlo visoka	Vrlo visoka
Aplikativni – vanjski razvoj	*EU trgovinske mjere*	Informacijski sustav upravljanja tržištem (ISUT)	Sektor za tržišnu potporu	SŠ		0	0	Osjetljivo	Visoka	Vrlo visoka
Aplikativni – vanjski razvoj	*Nacionalne ruralne mjere*	Informacijski sustav strukturne potpore (ISSP)	Sektor za strukturnu potporu	TMP		0	4	Kritično	Vrlo visoka	Vrlo visoka

Aplikativni – vanjski razvoj	*Trgovinska Internet aplikacija*	Informacijski sustav upravljanja tržištem (ISUT)	Sektor za tržišnu potporu	SŠ		0	0	Osjetljivo	Visoka	Vrlo visoka
Aplikativni – vanjski razvoj	*Upisnik poljoprivrednih gospodarstva*	Informacijski sustav za administraciju izravnih plaćanja (ISAP)	Sektor za registre	MŠ	0	0	0	Kritično	Vrlo visoka	Vrlo visoka
Aplikativni – vanjski razvoj	*Financijski sustav - plaćanje*	N/A	Sektor za financije	RM	8	2	0	Kritično	Vrlo visoka	Vrlo visoka
Aplikativni – kupljeni	*SharePoint*	N/A	Sektor za informacijsko upravljanje	AD	220	3	0	Kritično	Visoka	Vrlo visoka
Aplikativni – vanjski razvoj	*Jedinstveni zahtjev*	Informacijski sustav za administraciju izravnih plaćanja (ISAP)	Sektor za izravnu potporu	SKM		3	3	Kritično	Vrlo visoka	Vrlo visoka
Infrastrukturni	*File servis*	N/A	Sektor za informacijsko upravljanje	DM	200	3	3	Kritično	Vrlo visoka	Vrlo visoka
Infrastrukturni	*Veza prema MPRRR*	N/A	Sektor za informacijsko upravljanje	DM	41	3	4	Rezervirano	Srednja	Vrlo visoka
Aplikativni - eksternalizirani	*Plavo gorivo*	0	Odjel za odobrenje isplata	SKM		4	4	Kritično	Vrlo visoka	Vrlo visoka
Aplikativni - eksternalizirani	*Računovodstveni sustav pretpristupnih fondova*	Računovodstveni sustav	Odjel za računovoodstvo	RM	10	4	4	Rezervirano	Srednja	Vrlo visoka
Aplikativni – vanjski razvoj	*Financijski sustav - voucheri*	Financijski sustav	Sektor za financije	RM	0	4	4	Osjetljivo	Vrlo visoka	Vrlo visoka
Aplikativni – vanjski razvoj	*Interni računovodstveni sustav Agencije*	Računovodstveni sustav	Sektor za financije	GI	5	4	4	Rezervirano	Visoka	Vrlo visoka
Aplikativni – vanjski razvoj	*Kontrola na terenu*	Informacijski sustav za administraciju izravnih plaćanja (ISAP)	Sektor za kontrolu	KB		4	4	Osjetljivo	Visoka	Vrlo visoka

Uslužni IT servisi	*Mrežni nadzor*	N/A	Sektor za informacijsko upravljanje	DM	0	4	24	Osjetljivo	Visoka	Visoka
Infrastrukturni	*Elektronička pošta*	N/A	Sektor za informacijsko upravljanje	DM	501	6	3	Kritično	Visoka	Vrlo visoka
Uslužni IT servisi	*Sigurnosna pohrana*	N/A	Sektor za informacijsko upravljanje	DM	0	6	24	Kritično	Vrlo visoka	Visoka
Aplikativni - eksternalizirani	*Rizinica*	Informacijski sustav strukturne potpore (ISSP)	Sektor za strukturnu potporu	SKS	2	8	24	Osjetljivo	Vrlo visoka	Visoka
Aplikativni - eksternalizirani	*Pisarnica*	Informacijski sustav upravljanja dokumentacijom (ISUD)	Odjel pravnih poslova	RKJ	53	24	24	Kritično	Visoka	Visoka
Aplikativni – kupljeni	*Javne web stranice*	N/A	Odjel za izvještavanje	LH	50000	24	3	Javno	Vrlo visoka	Visoka
Aplikativni – kupljeni	*Kontrola prolaza*	N/A	Sektor za informacijsko upravljanje	GBO	210	24	24	Osjetljivo	Visoka	Visoka
Aplikativni – vanjski razvoj	*Financijski sustav - garancije*	Financijski sustav	Sektor za financije	RM	10	24	24	Osjetljivo	Visoka	Visoka
Aplikativni – vanjski razvoj	*Referentne cijene*	Informacijski sustav strukturne potpore (ISSP)	Sektor za strukturnu potporu	TMP		24	24	Rezervirano	Srednja	Visoka
Infrastrukturni	*Anti-malver sustav*	N/A	Sektor za informacijsko upravljanje	DM	600	24	24	Osjetljivo	Visoka	Visoka
Aplikativni – kupljeni	*Sustav za reviziju*	N/A	Sektor za unutarnju reviziju	VM		48	24	Osjetljivo	Visoka	Srednja
Aplikativni – vanjski razvoj	*Kadrovska*	N/A	Sektor općih i pravnih poslova	GBO		48	24	Rezervirano	Srednja	Srednja
Aplikativni – vanjski razvoj	*Sustav za poslovno izvješćivanje*	Sustav za poslovno izvješćivanje	Odjel za izvještavanje	RM		72	24	Kritično	Visoka	Srednja
Aplikativni - vlastiti razvoj	*Help desk sustav*	N/A	Sektor za informacijsko upravljanje	ZD	1	120	120	Rezervirano	Visoka	Vrlo visoka

Infrastrukturni	*FTP servis*	N/A	Sektor za informacijsko upravljanje	DM		120	120	Rezervirano	Niska	Niska
Infrastrukturni	*PKI sustav*	N/A	Sektor za informacijsko upravljanje	DM	0	120	120	Osjetljivo	Srednja	Niska
Uslužni IT servisi	*Update servis*	N/A	Sektor za informacijsko upravljanje	DM	500	120	120	Rezervirano	Srednja	Niska
Uslužni IT servisi	*Video nadzor*	N/A	Sektor za informacijsko upravljanje	DM	0	168	24	Rezervirano	Srednja	Niska
Aplikativni – vanjski razvoj	*Daljinsko istraživanje*	Informacijski sustav za administraciju izravnih plaćanja (ISAP)	Sektor za kontrolu	KB						
Aplikativni – vanjski razvoj	*Registar prava na plaćanje*	Informacijski sustav za administraciju izravnih plaćanja (ISAP)	Sektor za izravnu potporu	MŠ						

Tablica 15 - Rezultati provedene analize utjecaja na poslovanje primijenjena na informatičke servise u Agencija (Izvor: vlastiti rad)

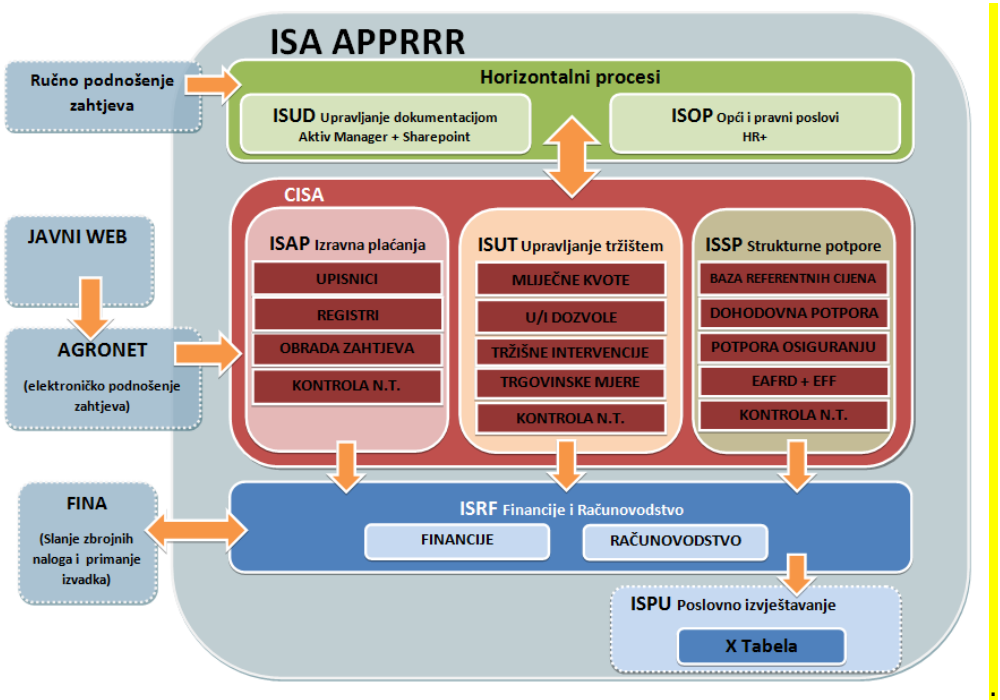
)

Za obnovu ključnih poslovnih procesa osim infrastrukturnih servisa potrebni su sljedeći IT servisi/aplikacije (prikazano na slici 17):

- ISAP (Informacijski sustav za administraciju izravnih plaćanja),
- ISSP (Informacijski sustav strukturne potpore),
- ISUT (Informacijski sustav upravljanja tržištem) i
- ISRF (Informacijski sustav za financije i računovodstvo).

Osim spomenutih IT servisa/aplikacija informacijski sustav Agencije (ISA) čine još:

- ISUD (Informacijski sustav upravljanja dokumentacijom),
- ISOP (Informacijski sustav za opće poslove),
- ISPU (Informacijski sustav za poslovno izvješćivanje),
- Agronet (sustav namijenjen za pomoć poljoprivrednim gospodarstvima i ostalim korisnicima u ostvarivanju prava na potpore u poljoprivredi),
- Javni web



Slika 17 - Informacijski sustav Agencije (Izvor: vlastiti rad)

4.7 Strategija odgovora sukladno provedenoj analizi

Kako se radi o analizi utjecaja na poslovanje primijenjene na informatičke servise, u ovom radu nisu razmotrene sve ovisnosti odvijanja poslovnih funkcija ili aktivnosti već samo ovisnost o informatičkim servisima i strategija odgovora bi trebala imati u konačnici za cilj oporavak informatičkog servisa u zadanim zahtijevanim vremenima oporavka. To znači da nam je u određivanju strategije odgovora polazište tablica 15., tj redoslijed oporavka informatičkih servisa obzirom na RTO i RPO parametre.

Pošto resursi nužni za obnovu poslovnih procesa u suštini sačinjavaju tipični podatkovni centar (engl. data centre), u kombinaciji s nekolicinom manje tipičnih usluga, razmatrat će se uobičajene strategije za obnovu podatkovnog centra u slučaju incidenta koji onemogućava rad primarnog podatkovnog centra.

Resursi za obnovu funkcionalnosti pojedinih procesa dati su tablici u PRILOGU "D".

4.7.1 Predložene strategije

4.7.1.1 Cold Site (hladna lokacija)

Cold site je financijski najpristupačniji oblik back-up lokacije. Takva lokacija osigurava minimalne uvjete i resurse potrebne za obnavljanje poslovnih procesa, kao što su struja, voda, hlađenje, komunikacijske linije (koje najčešće nisu aktivne) i sl. Lokacija također obuhvaća minimalne uvjete potrebne za prihvat broja radnika potrebnog za obnavljanje procesa (spomenuti uvjeti uključuju uredski namještaj, sanitarne čvorove i sl.).

Lokacija ne uključuje back-up kopije podataka i informacija s originalne (primarne) lokacije, niti na njoj postoji oprema (engl. hardware) koja se koristi u poslovanju. Nedostatak opreme glavni je nedostatak hladne lokacije.

U slučaju incidenta, proces oporavka započinje nabavkom opreme i njenom isporukom na lokaciju. Ukoliko telekomunikacijske linije nisu bile aktivne, poželjno je što ranije uputiti pružateljima usluga zahtjev za njihovo aktiviranje. Nakon isporuke, radnici mogu pristupiti instalaciji opreme i potrebnog software-a, te konfiguraciji istih. Konačno, po instalaciji i konfiguraciji opreme, pristupa se restauraciji podataka iz back-up kopija koje su prethodno dopremljene na lokaciju.

U slučaju prekida, hladna lokacija može postati operativna kroz 10 ili češće i više dana. U slučaju poslovnih procesa Agencije, ovakav tip lokacije nije zadovoljavajući – osim ukoliko je moguće sklopiti ugovore s dobavljačima kojima se garantira isporuka potrebne opreme na lokaciju u roku koji ostavlja dovoljno vremena za njenu instalaciju i konfiguraciju (dakle, unutar 2-3 dana) čime se smanjuje vrijeme potrebno za obnovu servisa.

4.7.1.2 Warm Site (topla lokacija)

Ovakav tip back-up lokacije uključuje svu potrebnu infrastrukturu (struja, voda, hlađenje, sanitarije i sl.) i opremu, ali se na njoj ne čuvaju back-up kopije podataka. Oprema koja se nalazi na lokaciji najčešće nije instalirana i konfigurirana, a često je i slabijeg kapaciteta obrade od one na primarnoj lokaciji. Lokacija također ima osigurane telekomunikacijske veze koje su aktivne ili mogu biti aktivirane u vrlo kratkom razdoblju (što se osigurava, primjerice, posebnim ugovorom s pružateljem usluga). Dobar izbor za ovakvu lokaciju su veze koje se naplaćuju po prometu (dakle, ako lokacija nije u upotrebi trošak održavanja je vrlo nizak). Kapacitet veza također ne mora odgovarati onima na primarnoj lokaciji.

Financijski gledano, ovakav je tip back-up lokacije nešto zahtjevniji – ponajprije zbog troška nabave opreme. Organizacije često niti ne razmatraju ovakav tip lokacije zato što

podrazumijeva određenu količinu potencijalno skupe opreme (poslužitelja, osobnih računala, mrežne opreme i sl.) koja se uopće ne koristi – štoviše, ukoliko se tijekom životnog vijeka lokacije ne dogodi incident, oprema ne mora nikada biti korištena.

Po incidentu, na pričuvnoj je lokaciji potrebno izvršiti instalaciju i konfiguraciju opreme, te zatim restauraciju podataka iz back-up kopija. Kao i u prethodnom slučaju, back-up kopije se često ne čuvaju na lokaciji (bar ne posljednja verzija), nego ih je potrebno dopremiti.

U slučaju prekida pričuvna lokacija može postati operativna unutar 48 sati do tjedan dana. Ovakav tip lokacije prikladan je za poslovne procese Agencije, jer pruža mogućnost obnove servisa u dovoljno kratkom roku, uz prihvatljiv financijski trošak, ali samo ukoliko se katastrofalan događaj dogodi izvan perioda kampanje.

4.7.1.3 Hot Site (vruća lokacija)

Na lokaciji su osigurani svi resursi potrebni za odvijanje procesa – struja, hlađenje, komunikacijski kanali, mrežna povezanost i sl. Na lokaciji se nalazi i popuno instalirana konfigurirana oprema, te operativno spremne i funkcionalne aplikacije. Također, na lokaciji se održavaju potpune ili gotovo potpune back-up kopije podataka (ovisno, prije svega, o RPO-u podataka).

U slučaju incidenta, potrebno je restaurirati posljednju kopiju podataka i zatim preusmjeriti korisnike na pričuvnu lokaciju.

Lokacija postaje potpuno operativna za tipično nekoliko minuta, do najviše nekoliko sati. Kod ovakvog tipa lokacije često je osoblju potrebno više vremena za prelazak, nego pričuvnoj lokaciji da postane aktivna po pitanjima raspoloživosti opreme i obnove podataka.

Ovakav tip lokacije financijski je zahtjevniji od prethodnih (cold site i warm site), jer je na lokaciji potrebno održavati opremu. Također, održavanje zahtjeva da dio radnika povremeno ili stalno radi na pričuvnoj lokaciji.

4.8 Odabir rješenja

Analizom utjecaja na poslovanje i procjenom rizika ustanovljeno je da je poslovno opravdano razmatrati investiranje u pričuvni podatkovni centar u stalnoj pripravnosti (eng. hot site) koji će preuzeti na sebe posluživanje ključnih informatičkih servisa koji podupiru ključne poslovne procese u slučaju ispada glavnog podatkovnog centra u Zagrebu. S obzirom na vremensku kritičnost u periodu provođenja kampanje tj. svi IT servisi koji podržavaju ključne poslovne procese podložni su probijanju zadanih rokova u slučaju bilo kakvih infrastrukturnih problema (primjerice kvar na sustavu napajanja, ispad eksternog diskovnog sustava ispad središnje mrežne opreme i sl.). Kako vrlo često nije moguće otkloniti i jednostavnije kvarove tijekom jednog radnog dana ti poslovni procesi i IT servisi koji podržavaju te procese primarni su kandidati za pokretanje na sekundarnoj lokaciji. Naravno, sekundarna lokacija bi trebala imati višak računalnih kapaciteta i fizičkog prostora, tako da je u slučaju većih destruktivnih ispada moguće ad hoc osposobiti dodatne IT servise koji omogućuju nastavak odvijanja nekritičnih poslovnih procesa prema padajućem redoslijedu poslovne kritičnosti.

Prilikom razmatanja i procjene prihvatljivosti sekundarnog podatkovnog centra potrebno je uzeti u obzir sljedeće parametre:

- osiguravanje potrebnih ljudskih resursa na dotičnoj lokaciji,
- mrežna povezanost sa primarnom lokacijom,
- lokaciju i smještaj

- osiguravanje neovisne elektroenergetske infrastrukture
- dovoljnu udaljenost za slučaj požara ili poplave na primarnoj lokaciji
- prometnu povezanost,
- učestalost potresa na lokaciji,
- tip lokacije (vruća, topla, hladna, replicirana u pripravnosti, on-line),
- mogućnosti testiranja,
- cijena.

Preporuke vezane uz udaljenost sekundarnog podatkovnog centra u pogledu rizika od potresa, uzimajući u obzir potresna područja i trusnost, impliciraju smještaj dotičnog na obalu. Trenutno ova opcija predstavlja preveliku investiciju, te je realno razmatranje lokacije u Zagrebu ili blizu Zagreba čime se osigurava manja cijena mrežne povezanosti za brze veze i jednostavniji prijevoz ljudi, a ipak omogućuje odabir lokacije sa odvojenom elektroenergetskom infrastrukturom i dovoljnu udaljenost za slučaj požara ili poplave.

S obzirom na financijsku neisplativost izgradnje vlastitog sekundarnog podatkovnog centra razumno je bilo razmotriti najam prostora u podatkovnom centru vanjske tvrtke. U ovom slučaju radi se o sistemskom prostoru nadležnog Ministarstva u gdje je Agencija uzela u zakup adekvatan prostor i smjestila svoje poslužitelje.

4.8.1 Uspostave veze prema sekundarnoj lokaciji

Osnovni preduvjet za korištenje sekundarne lokacije je dobra infrastrukturna povezanost.

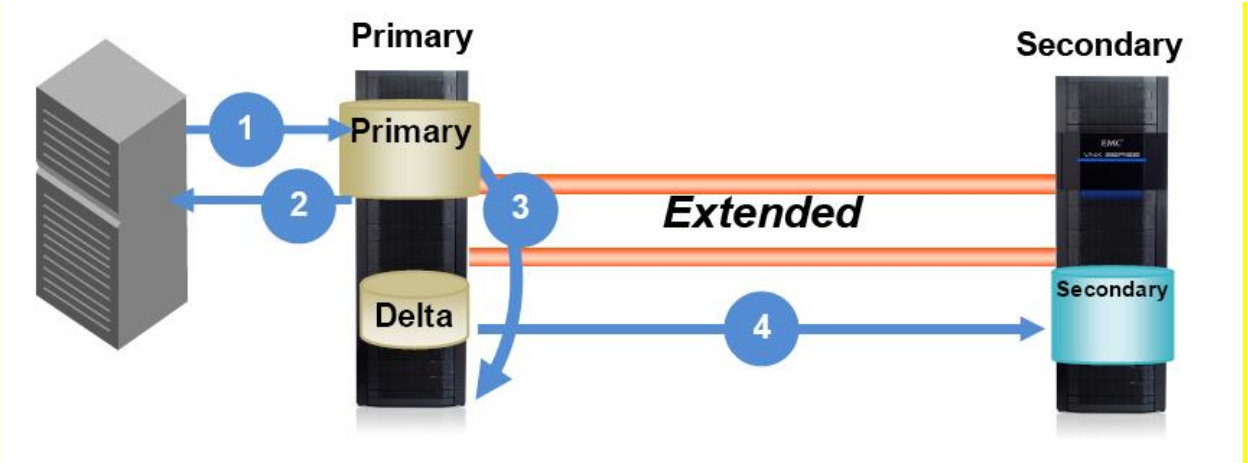
Replikacija je bazirana na EMC MirrorView/A sustavu koji radi na asinkronom principu nudeći mogućnost veće udaljenosti između primarne i sekundarne lokacije te upotrebu komunikacijskih veza manjih kapaciteta i brzina.

MirrorView/A je princip koji periodično inkrementalno ažurira sekundarne volumene sa svim promjenama koje su se dogodile na produkcijskim volumenima od posljednjeg ažuriranja.

MirrorView također nudi princip Consistency Group koji omogućuje sinkronizaciju grupe volumena koji su u međusobnoj ovisnosti o konzistentnosti podataka.

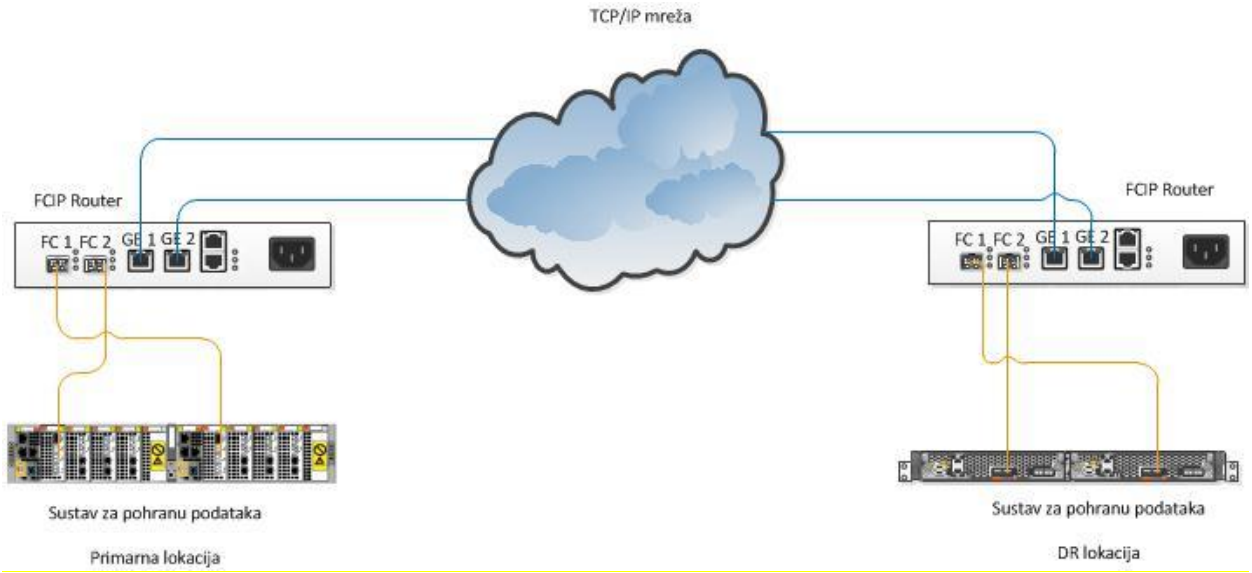
Dvije bitne veličine koje određuju cilj oporavka kod upotrebe asinkrone replikacije su dakako RPO i RTO.

U klasičnim primjenama asinkrone replikacije upisi na primarni volumen šalju se na sekundarni volumen kako su zaprimljeni od poslužitelja. Potvrda upisa poslužitelju ne dolazi od sekundarnog sustava nego od primarnog, međutim ako je količina upisa primarne strane veća nego što mogućnosti veze prema sekundarnoj lokaciji mogu iste proslijediti, većina I/O će biti na čekanju za slanje na primarnom sustavu.



Slika 18 - Asinkroni (periodično ažuriranje) slijed toka podataka

Komponente sustava su EMC diskovni sustavi, na produkcijskoj lokaciji EMC VNX5300 a na udaljenoj lokaciji EMC CX3-40 diskovni sustav te licence za MirrorView/A programsku podršku na oba sustava za pohranu podataka.



Slika 19 - Komponente replikacijskog sustava

Uz navedene komponente koristi se i FCIP Router za konverziju FC protokola u IP protokol.

FCIP (Fibre Channel over IP) omogućuje enkapsuliranje FC protokola unutar IP okvira omogućujući komunikaciju FC komponenti.

FCIP router služi za povezivanje obaju sustava za pohranu podataka te time omogućuje replikaciju podataka upotrebom postojeće IP infrastrukture.

5 ZAKLJUČAK

Analiza utjecaja na poslovanje primijenjena na informatičke servise prikazana u ovom radu daje odgovarajući okvir za provedbu iste. Na taj način, slijedeći određene korake i njihov redoslijed moguće je zaključiti koje odluke je potrebno donijeti. Iako je postupak vrlo određen, ipak ne rješava suštinski problem provedbe analize utjecaja na poslovanja. Najteža zadaća jeste što bolje odrediti kritičnost poslovnih funkcija i aktivnosti a samim time i zahtjeve na neprekidnost poslovanja.

Nedostatak egzaktne metode u određivanju razine utjecaja prekida i vrlo često nevjerica u točnost rezultata. Također i subjektivnost u poimanju kritičnosti pojedine poslovne funkcije ili aktivnosti za poslovanje kompanije i sklonost vrednovanja značaja vlastitog posla većine zaposlenih. Posebno je upitan način i procjena operativnog utjecaja koji je po svojoj prirodi neopipljiv i teško ga je kvantificirati. Jedino što može pomoći točnijem određivanju utjecaja jest vlastito poznavanje poslovanja organizacije onog tko provodi analizu, što objektivnije i ujednačenije prikupljanje i vrednovanje podataka, te pažljiv odabir od koga će se podaci prikupljati.

Međutim, jedno je sigurno a to je da uspjeh i vjerodostojnost rezultata provedene analize utjecaja na poslovanje definitivno ovisi o razini poznavanja poslovanja same organizacije. Kao što sve norme iz ovog područja, tako i norma ISO/IEC 22301:2012 navodi:

- upravljanje neprekidnošću poslovanja je svojstveno prirodi svake organizacije i složenosti poslovnih procesa iste i ne mogu postojati jedinstveni, široko primjenjivi, strogo određeni parametri. Ako je ovo točno, tada su poslovne organizacije na višoj razini

uređenosti u prednosti nad onima koje to nisu. Kao što je izloženo u ovom radu, za provedbu analize utjecaja na poslovanje korišteni su već pripremljeni podaci iz svakodnevnog poslovanja Agencije kao što je „Katalog informatičkih servisa Agencija“. Također kao vrijedan izvor informacija za provedbu analize su i vlasnici poslovnih procesa zajedno sa poslovnim analitičarima koji sudjeluju u razvoju aplikativnih rješenja koje koristi Agencija. Ove funkcije su izuzetno značajne upravo kod primjene analize utjecaja na poslovanje primijenjene na informatičke servise. Upravo uređenost poslovanja određene kompanije i vlastito poznavanje poslovanja predstavlja osnovu za provedbu učinkovite analize utjecaja na poslovanje i ne može biti nadomješteno vanjskim ekspertnim i konzultantskim znanjima.

Ipak metoda provedbe analize utjecaja na poslovanje izložena u ovom radu može naći primjenu u svakodnevnom životu i dati zadovoljavajuće rezultate. Kvaliteta dobivenih rezultata primjenom ove metode zasigurno će rasti sa vremenom i sakupljenim iskustvom i znanjem o poslovanju naše organizacije.

6 LITERATURA

[1] International Organization for Standardization, ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems — Requirements, ICS:03.100.70, International Organization for Standardization, 2013.

[2] International Organization for Standardization, ISO/IEC 27002:2013 : Information technology - Security techniques - Code of practice for information security controls, International Organization for Standardization, 2013.

[3] The British Standards Institution, BRITISH STANDARD; BS 25999:2006 – Business continuity management - Part 1: Code of practice, ICS 03.100.01, The British Standards Institution, 2006.

[4] CARNet, »Sigurnosna politika,« 23 04 2017. [Mrežno]. Available: http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2009-05-265.pdf.

[5] Ž. Putniković, BIA - Analiza utjecaja na poslovanje, primjenjena na informatičke service INA d.d., Zagreb, 2012.

[6] MetricStream, »Business Continuity Planning,« MetricStream, 2017. [Mrežno]. Available: https://www.metricstream.com/solution_briefs/BCP_FFIEC_Compliance.htm. [Pokušaj pristupa 20 July 2017].

[7] ContinuityCentral.com, »Business continuity trends and challenges 2017,« Portal Publishing Ltd., 3 February 2017. [Mrežno]. Available: http://www.continuitycentral.com/index.php/news/business-continuity-news/1738-business-continuity-trends-and-challenges-2017. [Pokušaj pristupa 4 October 2017].

[8] V. Wheatman, »Aftermath: Disaster Recovery,« Gartner.com, 21 September 2001. [Mrežno]. Available: https://www.gartner.com/doc/341017/aftermath-disaster-recovery. [Pokušaj pristupa 2 October 2017].

[9] Vlada RH, Odluka o primjerenom upravljanju informacijskim sustavom, NN 80/2007, Zagreb: Narodne novine, 2007.

[10] A. Hill, The Definitive Handbook of Business Continuity Management, Third Edition ur., Oxton, United Kingdom: Kingswell International, 2010.

[11] S. Snedaker, »BIA for business continuity, Chapter 3,« u *Business Continuity & Disaster Recovery for IT Professionals*, second ur., Stanford, California: Syngress Publishing, 2007, p. 620.

[12] Advisera Expert Solution, »What is ISO/IEC 27001?,« Advisera Expert Solution, [Mrežno]. Available: https://advisera.com/27001academy/what-is-iso-27001/. [Pokušaj pristupa 4 July 2017].

[13] International Organization for Standardization, »ISO 22301:2012,« International Organization for Standardization, May 2012. [Mrežno]. Available: https://www.iso.org/standard/50038.html. [Pokušaj pristupa 23 April 2017].

[14] CERT i LSS, »Upravljanje kontinuitetom poslovnih procesa,« CARNet, July 2010. [Mrežno]. Available: http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-15-307.pdf. [Pokušaj pristupa 24 April 2017].

[15] Wikimedia Commons (FW8100), »PDCA ZIRKEL ENGLISH,« Wikimedia Commons, 2012.

[16] The British Standards Institution, BRITISH STANDARD; BS 25999-2:2007, Business continuity management - Part 2: Specification, ICS 03.100.01, The British Standards Institution.

[17] G. Wrenn, »How to create a business impact analysis for disaster recovery in 10 easy steps,« 1 January 2008. [Mrežno]. Available: http://searchdisasterrecovery.techtarget.com/tip/How-to-create-a-business-impact-analysis-for-disaster-recovery-in-10-easy-steps?mboxConv=searchCIO_RegActivate_Submit&. [Pokušaj pristupa 2 September 2017].

[18] APPRRR, »Procjena rizika informacijske sigurnosti,« Zagreb, 2013.

[19] M. Bača, Uvod u računalnu sigurnost, Zagreb: Narodne novine d.d., 2004, p. 378.

[20] Z. Krakar, "REVIZIJA I SIGURNOST INFORMACIJSKIH SUSTAVA", predavanja sa kolegija "UPRAVLJANJE KONTINUITETOM POSLOVANJA", 2009.

7 PRILOZI

7.1 Prilog A – Katalog informatičkih servisa

KATALOG INFORMATIČKIH SERVISA						
Veza na obrazac	**Tip IT servisa**	**Naziv IT servisa**	**Dio IS-a**	**Vlasnik podataka (OJ)**	**Status**	**Vlasnik aplikacije**
Pisarnica	Aplikativni - eksternalizirani	***Pisarnica***	Informacijski sustav upravljanja dokumentacijom (ISUD)	Odjel pravnih poslova	U produkciji	RKJ
Plavo_Gorivo	Aplikativni - eksternalizirani	***Plavo gorivo***	0	Odjel za odobrenje isplata	U produkciji	SKM
RS_EU	Aplikativni - eksternalizirani	***Računovodstveni sustav pretpristupnih fondova***	Računovodstveni sustav	Odjel za računovoodstvo	U produkciji	RM
Riznica	Aplikativni - eksternalizirani	***Rizinica***	Informacijski sustav strukturne potpore (ISSP)	Sektor za strukturnu potporu	U produkciji	SKS
WEB	Aplikativni – kupljeni	***Javne web stranice***	N/A	Odjel za izvještavanje	U produkciji	LH
Kontrola_prolaza	Aplikativni – kupljeni	***Kontrola prolaza***	N/A	Sektor za informacijsko upravljanje	U produkciji	GBO
SharePoint	Aplikativni – kupljeni	***SharePoint***	N/A	Sektor za informacijsko upravljanje	U produkciji	AD

Revizija	Aplikativni – kupljeni	*Sustav za reviziju*	N/A	Sektor za unutarnju reviziju	U planu	VM
agronet	Aplikativni – vanjski razvoj	***agronet***	N/A	Sektor za izravnu potporu	U produkciji	SKS
AMKA	Aplikativni – vanjski razvoj	***Aplikacija za mliječne kvote***	Informacijski sustav upravljanja tržištem (ISUT)	Sektor za tržišnu potporu	U produkciji	SŠ
ARKOD	Aplikativni – vanjski razvoj	***ARKOD***	Informacijski sustav za administraciju izravnih plaćanja (ISAP)	Sektor za registre	U produkciji	MŠ
Daljinsko	Aplikativni – vanjski razvoj	*Daljinsko istraživanje*	Informacijski sustav za administraciju izravnih plaćanja (ISAP)	Sektor za kontrolu	U razvoju	KB
EU_mjere	Aplikativni – vanjski razvoj	*EU trgovinske mjere*	Informacijski sustav upravljanja tržištem (ISUT)	Sektor za tržišnu potporu	U planu	SŠ
FIS_garancije	Aplikativni – vanjski razvoj	***Financijski sustav - garancije***	Financijski sustav	Sektor za financije	U produkciji	RM
FIS_plaćanje	Aplikativni – vanjski razvoj	***Financijski sustav - plaćanje***	N/A	Sektor za financije	U produkciji	RM
FIS_voucheri	Aplikativni – vanjski razvoj	***Financijski sustav - voucheri***	Financijski sustav	Sektor za financije	U produkciji	RM
RS_APPRRR	Aplikativni – vanjski razvoj	***Interni računovodstveni sustav Agencije***	Računovodstveni sustav	Sektor za financije	U produkciji	GI
Jedinstveni_zahtjev	Aplikativni – vanjski razvoj	***Jedinstveni zahtjev***	Informacijski sustav za administraciju izravnih plaćanja (ISAP)	Sektor za izravnu potporu	U produkciji	SKM
Kadrovska	Aplikativni – vanjski razvoj	*Kadrovska*	N/A	Sektor općih i pravnih poslova	U razvoju	GBO
Kontrola_na_terenu	Aplikativni – vanjski razvoj	*Kontrola na terenu*	Informacijski sustav za administraciju izravnih plaćanja (ISAP)	Sektor za kontrolu	U razvoju	KB
Nac_mjere	Aplikativni – vanjski razvoj	*Nacionalne ruralne mjere*	Informacijski sustav strukturne potpore (ISSP)	Sektor za strukturnu potporu	U planu	TMP
Referetne_cijene	Aplikativni – vanjski razvoj	***Referentne cijene***	Informacijski sustav strukturne potpore (ISSP)	Sektor za strukturnu potporu	U produkciji	TMP
Registar_prava	Aplikativni – vanjski razvoj	*Registar prava na plaćanje*	Informacijski sustav za administraciju izravnih plaćanja (ISAP)	Sektor za izravnu potporu	U planu	MŠ

Izvješćivanje	Aplikativni – vanjski razvoj	*Sustav za poslovno izvješćivanje*	Sustav za poslovno izvješćivanje	Odjel za izvještavanje	U razvoju	RM
TIA	Aplikativni – vanjski razvoj	***Trgovinska Internet aplikacija***	Informacijski sustav upravljanja tržištem (ISUT)	Sektor za tržišnu potporu	U produkciji	SŠ
Upisnik	Aplikativni – vanjski razvoj	***Upisnik poljoprivrednih gospodarstva***	Informacijski sustav za administraciju izravnih plaćanja (ISAP)	Sektor za registre	U produkciji	MŠ
Help_desk	Aplikativni - vlastiti razvoj	***Help desk sustav***	N/A	Sektor za informacijsko upravljanje	U produkciji	ZD
anti_malver	Infrastrukturni	***Anti-malver sustav***	N/A	Sektor za informacijsko upravljanje	U produkciji	DM
email	Infrastrukturni	***Elektronička pošta***	N/A	Sektor za informacijsko upravljanje	U produkciji	DM
File_servis	Infrastrukturni	***File servis***	N/A	Sektor za informacijsko upravljanje	U produkciji	DM
FTP	Infrastrukturni	*FTP servis*	N/A	Sektor za informacijsko upravljanje	Ne koristi se	DM
AD	Infrastrukturni	***Imenički servis***	N/A	Sektor za informacijsko upravljanje	U produkciji	DM
LAN	Infrastrukturni	***Interna računalna mreža***	N/A	Sektor za informacijsko upravljanje	U produkciji	DM
PBX	Infrastrukturni	***Interna telefonija***	N/A	Sektor za informacijsko upravljanje	U produkciji	DM
PKI	Infrastrukturni	***PKI sustav***	N/A	Sektor za informacijsko upravljanje	U produkciji	DM
Internet	Infrastrukturni	***Pristup Internetu***	N/A	Sektor za informacijsko upravljanje	U produkciji	DM
SSO	Infrastrukturni	*Sustav jedinstvene autentikacije*	N/A	Sektor za informacijsko upravljanje	U razvoju	DM
Veza_MPRRR	Infrastrukturni	***Veza prema MPRRR***	N/A	Sektor za informacijsko upravljanje	U produkciji	DM
Virtualnizacija	Infrastrukturni	***Virtualizacijski servis***	N/A	Sektor za informacijsko upravljanje	U produkciji	DM

VPN	Infrastrukturni	***VPN***	N/A	Sektor za informacijsko upravljanje	U produkciji	DM
Mrežni_nadzor	Uslužni IT servisi	***Mrežni nadzor***	N/A	Sektor za informacijsko upravljanje	U produkciji	DM
Back_up	Uslužni IT servisi	***Sigurnosna pohrana***	N/A	Sektor za informacijsko upravljanje	U produkciji	DM
Update	Uslužni IT servisi	***Update servis***	N/A	Sektor za informacijsko upravljanje	U produkciji	DM
Video_nadzor	Uslužni IT servisi	***Video nadzor***	N/A	Sektor za informacijsko upravljanje	U produkciji	DM

7.2 Prilog B – Obrazac definicije uspostavljenog informatičkog servisa

UPITNIK ANALIZE IT SERVISA

OSNOVNE INFORMACIJE O IT SERVISU

Naziv IT servisa	Tip IT servisa

Dio informacijskog sustava	Modul

STATUS SERVISA

Trenutni status servisa:	

INFORMACIJE PRIKUPLJENE OD

Ime i prezime	Organizacijska jedinica / tvrtka	Kontakt podaci (telefon/e-mail)	Funkcija u kontekstu servisa (DBA, razvoj, sistem, odgovorna osoba)

VLASNIK APLIKACIJE

Ime i prezime	Organizacijska jedinica	Funkcija u kontekstu servisa prema sistematiziciji radnih uloga

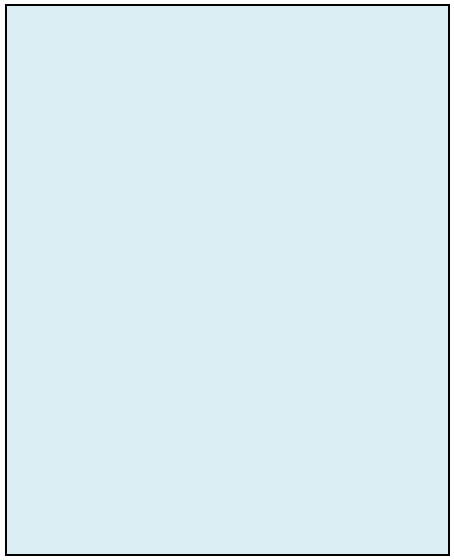
KONTAKTI ZA PODRŠKU

Kontakt podaci osobe/osoba ili tvrtki zaduženih za podršku (rangirati po redoslijedu važnosti)

	Ime i prezime	Organizacijska jedinica / tvrtka	Kontakt podaci (telefon, e-mail)
Primarni kontakt za podršku			
Sekundarni kontakt za podršku			
Tercijarni kontakt za podršku			

OPIS ARHITEKTURE SERVISA

Kratak opis funkcionalnosti i načina rada servisa (mrežna arhitektura, način pristupa)



KRITIČNE IT KOMPONENTE

Navesti kritične IT komponente

Naziv	Opis IT komponente	Funkcija IT komponente	Lokacija IT komponente

OVISNOSTI O DRUGIM SERVISIMA

Navesti ovisnosti o drugim IT servisima

Naziv IT servisa	Opis (razlog)ovisnosti	Period ovisnosti

BROJ KORISNIKA

Organizacijske jedinice, procesi ili osobe (poslovne funkcije/uloge) koje izravno koriste IT servis

Naziv organizacijske jedinice, procesa ili radne uloge	Broj otvorenih korisničkih računa

PREPOZNATI RIZICI I KORIŠTENE MJERE

Navesti značajne rizike kojima je IT servis izložen kao i mjere kojima se rizici ograničavaju

Rizici	Mjere

TRENUTNI BACKUP

Trenutna periodičnost izrade back-up?

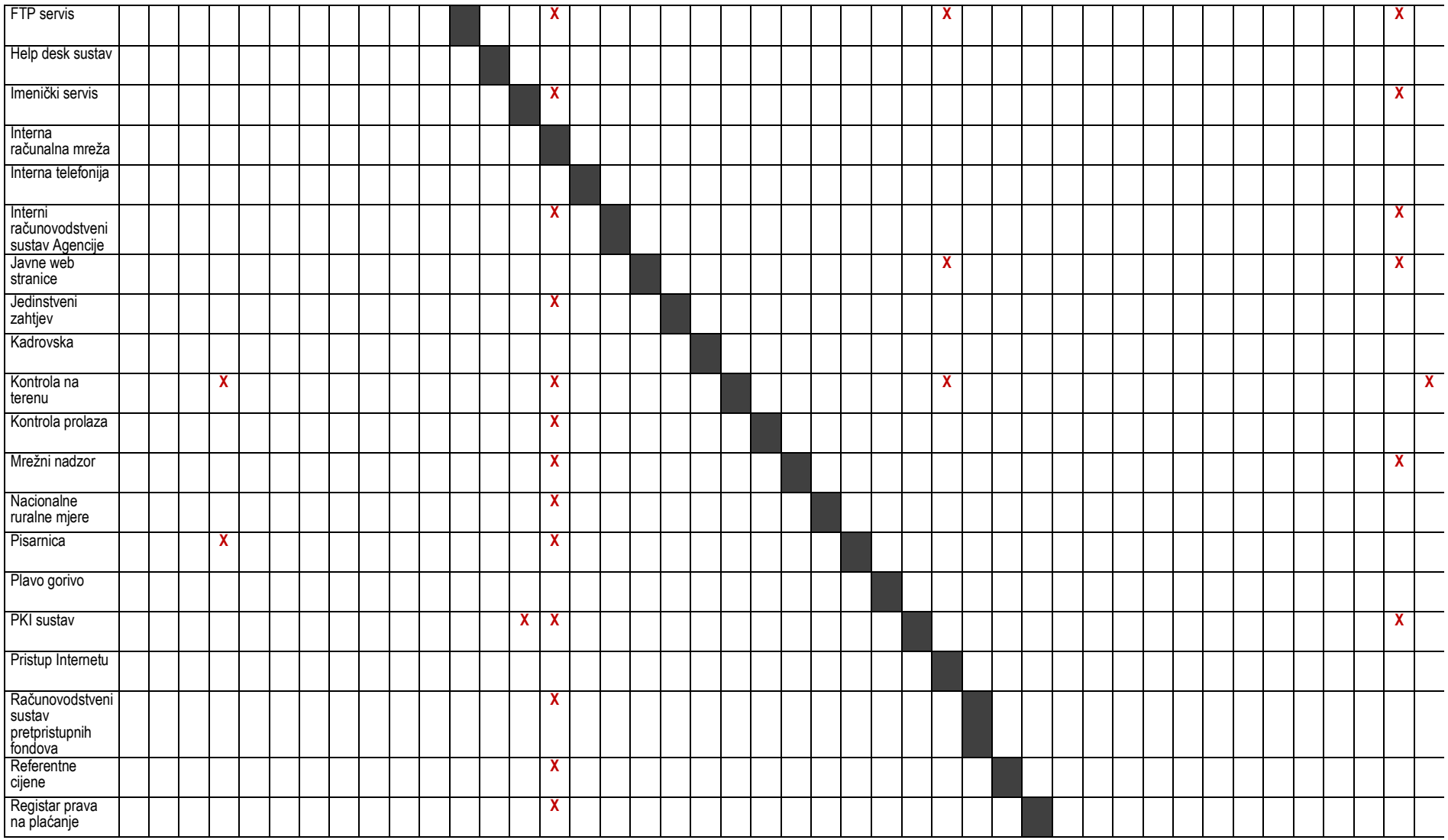
Metoda pohrane	Vrsta ili tip podataka (uključuje i backup poslužiteljske konfiguracije)	Količina podataka	Frekvencija pohrane (svakih x sati)

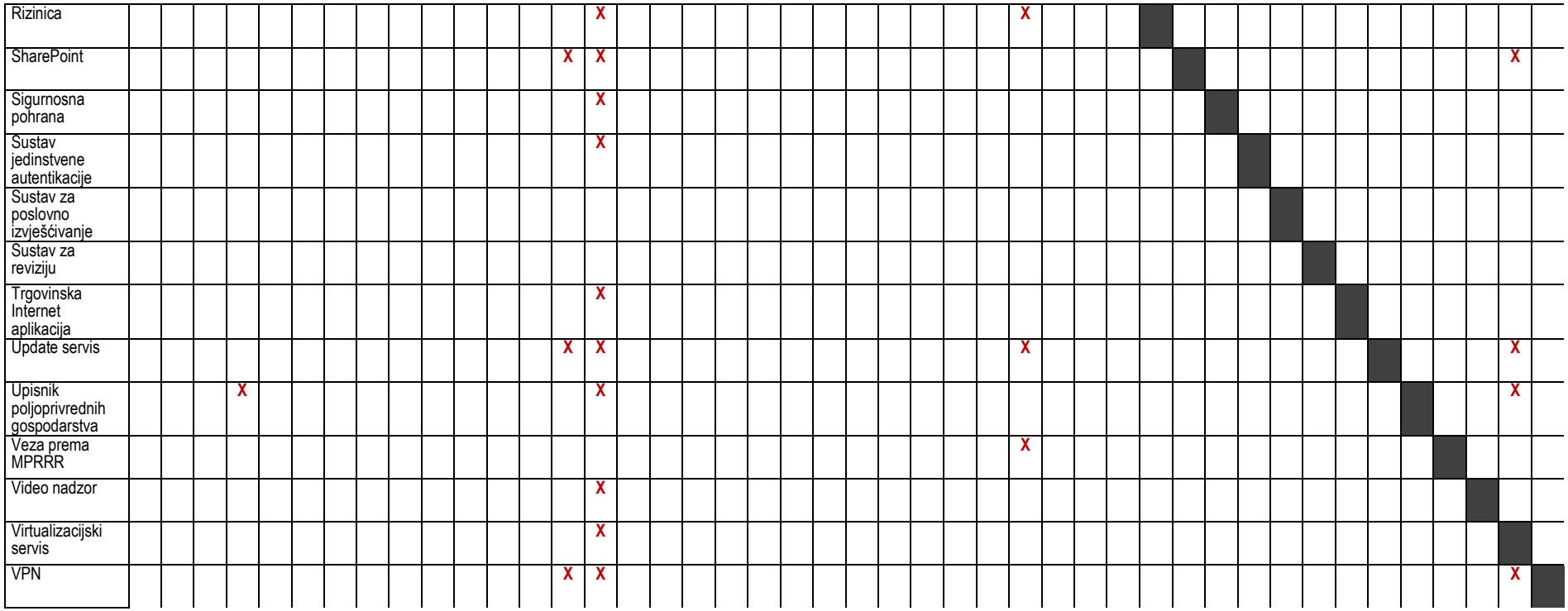
NAPOMENE

Dodatne napomene (budući planovi za IT servis, inherentni problemi, …)

7.3 Prilog C - Tablica korelacija informatičkih servisa, poslovnih funkcija i aktivnosti

Među-ovisnost IT servisa	agronet	Anti-malver sustav	Aplikacija za mliječne kvote	ARKOD	Daljinsko istraživanje	Elektronička pošta	EU trgovinske mjere	File servis	Financijski sustav - garancije	Financijski sustav - plaćanje	Financijski sustav - voucheri	FTP servis	Help desk sustav	Imenički servis	Interna računalna mreža	Interna telefonija	Interni računovodstveni sustav Agencije	Javne web stranice	Jedinstveni zahtjev	Kadrovska	Kontrola na terenu	Kontrola prolaza	Mrežni nadzor	Nacionalne ruralne mjere	Pisarnica	Plavo gorivo	PKI sustav	Pristup Internetu	Računovodstveni sustav pretpristupnih fondova	Referentne cijene	Registar prava na plaćanje	Rizinica	SharePoint	Sigurnosna pohrana	Sustav jedinstvene autentikacije	Sustav za poslovno izvješćivanje	Sustav za reviziju	Trgovinska Internet aplikacija	Update servis	Upisnik poljoprivrednih gospodarstva	Veza prema MPRRR	Video nadzor	Virtualizacijski servis	VPN
agronet															X													X															X	X
Anti-malver sustav															X																												X	
Aplikacija za mliječne kvote															X																													
ARKOD															X																					X								
Daljinsko istraživanje				X											X																													
Elektronička pošta														X	X																												X	
EU trgovinske mjere															X																													
File servis														X	X																												X	
Financijski sustav - garancije															X																													
Financijski sustav - plaćanje															X																												X	
Financijski sustav - voucheri															X																												X	


FTP servis
Help desk sustav
Imenički servis
Interna računalna mreža
Interna telefonija
Interni računovodstveni sustav Agencije
Javne web stranice
Jedinstveni zahtjev
Kadrovska
Kontrola na terenu
Kontrola prolaza
Mrežni nadzor
Nacionalne ruralne mjere
Pisarnica
Plavo gorivo
PKI sustav
Pristup Internetu
Računovodstveni sustav pretpristupnih fondova
Referentne cijene
Registar prava na plaćanje


Rizinica
SharePoint
Sigurnosna pohrana
Sustav jedinstvene autentikacije
Sustav za poslovno izvješćivanje
Sustav za reviziju
Trgovinska Internet aplikacija
Update servis
Upisnik poljoprivrednih gospodarstva
Veza prema MPRRR
Video nadzor
Virtualizacijski servis
VPN

7.4 Prilog D – Analiza visokih rizika i potrebni resursi za obnovu procesa (primjer)

Sektor	Sektor za informacijsko upravljanje
Direktor / Voditelj	DM/DV
Poslovni proces	Upravljanje specijaliziranim softverom za potporu poslovanju Agencije
Vlasnik procesa	DV
Kratki opis procesa	
Organizacija razvoja softvera za posebne potrebe Agencije, nazdoz rada vanjskih izvođača, upravljanje informatičkim projektima, suradnja s tijelima državne uprave i drugim zainteresiranim stranama na području pristupa i razmjene podataka.	
Interakcija s drugim procesima	
X DA □ NE	
X unutar organizacije X izvan organizacije	Cijela Agencija vanjski izvođač XXXX-ICT
Napomena:	
Planirane promjene u skoroj budućnosti	
X DA □ NE	

Opis:
Uvođenje CA Service Desk alata za praćenje promjena, zapošljavanje dodatnih ljudi

Kada je *peak time?*

□ kvartalno:	□ 1 □ 2 □ 3 □ 4
□ mjesečno:	□ I. □ II. □ III. □ IV. □ V. □ VI. □ VII. □ VIII. □ IX. □ X. □ XI. □ XII.
□ tjedno:	□ Pon □ Uto □ Sri □ Čet □ Pet □ Sub □ Ned
X dnevno:	□ početak dana □ kraj dana □ vrijeme: 8-16; pon-pet
□ ostalo:	

Napomena:
Peak time ovisi o planu nadogradnje.

Kakav bi utjecaj na organizaciju imao prekid procesa u *peak time*-u?

1 sat:	X NIZAK	□ SREDNJI	□ KATASTROFALAN
8 sati:	X NIZAK	□ SREDNJI	□ KATASTROFALAN
2 dana:	X NIZAK	□ SREDNJI	□ KATASTROFALAN
1 tjedan:	□ NIZAK	X SREDNJI	□ KATASTROFALAN
1 mjesec:	□ NIZAK	X SREDNJI	□ KATASTROFALAN

Napomena:
Opipljivi gubici
X Smanjena potražnja za uslugama □ Smanjeni prihodi □ Kašnjenje prihoda X Povećani operativni trošak X Penali (od SLA i sl.)
Napomena: Zatezne kamate banaka u slučaju kašnjenja isplata (faktoring, voucheri,…)
Neopipljivi gubici
□ Gubitak ugleda NEMA UTJECAJA X Gubitak povjerenja VISOKI X Kršenje zakonske regulative VISOKI □ Sigurnost korisnika NEMA UTJECAJA X Negativan utjecaj na djelatnike VISOKI
Napomena: unijeti jednu od opcija - NEMA UTJECAJA, NISKI, SREDNJI, VISOKI, KATASTROFALNI

Koji su podaci nužni za funkcioniranje procesa
□ real-time baza podataka □ non-real-time baza podataka x dokumenti (ugovori i sl.)
Napomena: Ugovori, projektna dokumentacija.
Koliko korisnika pristupa navedenim podacima?
5 korisnika
Napomena: 5 korisnika i vlasnici poslovnih procesa.
Koliko se često (u prosjeku) pristupa navedenim podacima?
puta □ po minuti □ po satu X dnevno

Napomena:
Svakodnevno se pristupa podacima.

Koliko stari smiju biti podaci?

5 □ sati X dana □ tjedana

Napomena:

Koliko se dugo proces može neometano odvijati bez vanjske podrške?

3 □ sati X dana □ tjedana

Napomena:

Koliko ljudi je potrebno za obnovu procesa i kakve vještine trebaju posjedovati?

Vještina:	instalacija opreme	Ljudi:	informatičar
Vještina:	specifikacija zahtjeva za razvoj softvera	Ljudi:	vlasnici procesa

Vještina:	poznavanje poslovnog procesa	Ljudi:	DV
Vještina:	razvoj softvera	Ljudi:	vendor
Vještina:		Ljudi:	

Napomena:

Ostali resursi nužni za obnovu procesa

X DA □ NE

Potrebni resursi za različite scenarije:
SOFTWARE:
Share Point, CA Service Desk

HARDWARE:
Računalo

USLUGE VANJSKIH DOBAVLJAČA:
Telekomunikacije

RTO i RPO za različite scenarije (veza prema BCM strategiji)
1. Glavna lokacija i sva oprema van uporabe: VJEROJATNOST POJAVLJIVANJA: NISKA UTJECAJ: VISOK RTO: 7 dana RPO: 5 dana STRATEGIJA: preseljenje na unajmljenu sekundarnu lokaciju koja nije ugrožena te ponovna dobava HW-a i SW-a te instalacije, organizacija ljudi i puštanje u produkciju.
2. Sekundarna lokacija i oprema na toj lokaciji nedostupna: VJEROJATNOST POJAVLJIVANJA: NISKA UTJECAJ: VISOK RTO: 2 dana RPO: 5 dana STRATEGIJA: nabavka nove komunikacijske opreme i instalacija iste na glavnoj lokaciji. Postoji redundantni optički link te bi relativno brzo bilo moguće novu komunikacijsku opremu instalirati i pustiti u produkciju.
3. Uništena oprema na glavnoj lokaciji (HW, SW): VJEROJATNOST POJAVLJIVANJA: SREDNJA UTJECAJ: VISOK RTO: 2 dana RPO: 5 dana STRATEGIJA: nabavka nove opreme uz dostupnost backupa te instalacija opreme i puštanje u produkciju.
4. SW (sistemski i aplikativni) nije u funkciji: VJEROJATNOST POJAVLJIVANJA: NISKA UTJECAJ: VISOK RTO: 24 sata RPO: 5 dana STRATEGIJA: ponovna instalacija uz dostupnost backupa ili papirnate arhive, restauracija podataka i ponovna produkcija.

5. Nisu dostupne ključne usluge vanjskih dobavljača (Internet, el.energija, telekomunikacije): VJEROJATNOST POJAVLJIVANJA: NISKA UTJECAJ: VISOK RTO: 24 sata RPO: 24 sata STRATEGIJA: za napajanje el. energijom postoji UPS u data centru i vanjski generator, traženje drugog operatera.
6. Nisu dostupne ključne usluge vanjskih dobavljača (XXXX- ICT): VJEROJATNOST POJAVLJIVANJA: NISKA UTJECAJ: VISOK RTO: 10 dana RPO: 24 sata STRATEGIJA: uspostava sustava iz vlastitih resursa, backup, monitoring, traženje drugog vendora.
7. Nisu dostupni ključni ljudi: VJEROJATNOST POJAVLJIVANJA: NISKA UTJECAJ: VISOK RTO: 10 dana RPO: 5 dana STRATEGIJA: uključivanje novih ljudi u rad, edukacija još jednog djelatnika u proces.

SAŽETAK

Polazna pretpostavka rada jeste da je danas poslovanje gotovo svake organizacije, tvrtke a i pojedinca, snažno ovisno o informatičko-komunikacijskim servisima. Stoga, cilj je ovog rada bio odrediti mogući postupak provedbe analize utjecaja prekida poslovnih procesa a da isti bude promatran kroz informatičke servise u svrhu planiranja kontinuiteta poslovanja. Analiza je provedena na primjeru poslovnih procesa i funkcija i informatičkih servisa koji podržavaju njihovo odvijanje u Agenciji.

Polazna točka provedene analize jeste katalog informatičkih servisa. Nakon toga, potrebno je načiniti zavisnosti tj. korelaciju informatičkih servisa i poslovnih funkcija, nakon čega se utvrđuje ovisnost odvijanja poslovnih aktivnosti o raspoloživosti informatičkih servisa. U tom kontekstu određuju se operativni utjecaji prekida poslovnih funkcija uslijed prekida informatičko-komunikacijskih servisa koji ih podržavaju i preko zahtijevanih vremena oporavka poslovnih funkcija određuju i zahtijevana vremena oporavka informatičko-komunikacijskih servisa.

Krajnji rezultat analize jesu razine kritičnosti svakog pojedinog informatičkog servisa koja su temeljna polazišta za određivanje strategije kontinuiteta poslovanja. Postupak prikazuje i načine prikupljanja podataka za provedbu analize, definira razine kritičnosti i kroz analizu prikupljenih podataka definira određivanje kritičnosti i vremena oporavka informatičko-komunikacijskih servisa.

Summary

The starting assumption of my work is that today's business of almost each organization, company and an individual, strongly depends on IT communicating services. Therefore, the aim of this paper was to determine the possible process of conducting an analysis of the impact of business interruptions and to look at it through IT services for the purpose of business continuity planning. The analysis was carried out on the example of business processes and functions and IT services as well that support their implementation in the Agency.

The starting point of the implemented analysis is the Catalog of IT services. That, it is necessary to make dependencies, ie the correlation of IT services and business functions, after which it is determined the dependence of business activities on the availability of IT services. In this context, the operational impacts of interrupting business functions due to IT service interruptions that support them and the required time of recovery of business functions determine the required time of recovery of IT services

The final result of the analysis is the level of critical point of each IT service that is the basic starting point for determining the business continuity strategy. The process also shows ways of collecting data to conduct the analysis, defining the levels of criticality and analyzing collected data defining the criterion and time of recovery of IT services.

Dokumentacijske kartice

ŽIVOTOPIS

Dražen Marinović

Curriculum Vitae

Rodio sam se u Zagrebu, gdje sam završio osnovno i srednje obrazovanje. Diplomirao sam na fakultetu strojarstva i brodogradnje u Zagrebu 2006. godine. U 1993. godini osnovao sam vlastitu tvrtku kojoj je glavno poslovanje bilo razvoj aplikativne podrške i razvoj infrastrukturnih rješenja a od 2002. godine radim isključivo na informatičkim poslovima u tijelima državne uprave i imam više od 25 godina radnog iskustva.

Osobni podaci

Mjesto rođenja:	Zagreb, Hrvatska
Datum rođenja:	23. travnja 1967.
Kućna adresa:	Zlatarova zlata 8, 10020 Zagreb, Hrvatska
Telefon:	+385 / (0)1 – 6547 975 (kućni)
	+385 / (0)99 – 6169 064 (mobilni)
e-mail:	drazen.marinovic@apprrr.hr

Školovanje:

Poslijediplomski specijalistički studij	Fakultet organizacije i informatike, Varaždin (pred dovršetkom)
Diplomski studij	Fakultet strojarstva i brodogradnje, Zagreb, (diplomirao 2006)
Srednja škola	*Tehnička škola "O.C. Nikola Tesla"*, Zagreb (1986)

Doškolovanje:

Tijekom radnog perioda završio sam niz specijalističkih tečajeva iz različitih područja informatičkih tehnologija. U posljednje vrijeme najviše se obrazujem u području upravljanja projektima, upravljanja informatičkim servisima i informacijske sigurnosti. Neka uvjerenja iz doškolovanja su:

- *MCP – Microsoft Certified Professional*
- *MCSA – Microsoft Certified System Administrator*
- *MCSE – Microsoft Certified System Engineer*
- *Certified Lead Provisional Implementer for ISO/IEC 27001*
- *Certified Internal Auditor for ISMS - ISO/IEC 27001:2005*
- *BCP – uspostava prema normi ISO/IEC 22301:2012*
- *Članstvo: ISACA*
- *Niz seminara iz područja sigurnosti, infrastrukturnih rješenja i razvoja aplikativne podrške*

Jezici:

Hrvatski - materinji

Engleski - vrlo dobro

12 godina kroz redovno obrazovanje

Radno iskustvo:

Datum (od – do)	Prosinac 2009 - danas
Naziv i sjedište tvrtke zaposlenja	AGENCIJA ZA PLAĆANJA U POLJOPRIVREDI, RIBAR-STVU I RURALNOM RAZVOJU, ulica grada Vukovara 269d, Zagreb (kraće APPRRR, u daljnjem tekstu Agencija)
Vrsta posla ili područje	Sektor za informacijsko upravljanje
Zanimanje i položaj koji obnaša	Direktor sektora
Osnovne aktivnosti i odgovornosti	Upravljanje rada sektora u cjelinama: tehnička podrška, razvoj aplikativne podrške i informatička sigurnost
Projekti	Nadogradnja informacijskog sustava APPRRR – aplikativna podrška (2010, 2011, 2012, 2013 i 2014) - Voditelj projekata Usklađivanje trenutnog poslovanja sa ISO/IEC 27002 (2010) Projektni odbor – član Uspostava BCM sustava u APPRRR (2012) Voditelj projekta Uspostava sekundarne lokacije računskog centra APPRRR (2012) – Voditelj projekta Certifikacija poslovanja Agencije sa ISO/IEC 27001:2013 (2015) Projektni odbor - član

Datum (od – do)	Svibanj 2005 - Prosinac 2009
Naziv i sjedište tvrtke zaposlenja	RAVNATELJSTVO ZA TRŽIŠNU I STRUKTURNU POTPORU U POLJOPRIVREDI, ulica grada Vukovara 269d, Zagreb
Vrsta posla ili područje	Sektor za informacijsko upravljanje
Zanimanje i položaj koji obnaša	Direktor sektora
Osnovne aktivnosti i odgovornosti	Upravljanje rada sektora u cjelinama: tehnička podrška, razvoj aplikativne podrške i informatička sigurnost
Projekti	Nadogradnja informacijskog sustava APPRRR – aplikativna podrška (2005, 2006, 2007, 2008 i 2009) - Voditelj projekta Uspostava cjelokupne informatičke infrastrukture potrebne za poslovanje APPRRR u RH (2005-2006) Voditelj projekta Inicijalna uspostava ISO/IEC 27002 (2005) Provođenje natječaja Svjetske banke za nabavu i opremanje APPRRR suvremenim data centrom – Voditelj projekta

Datum (od – do)	2002 - Svibanj 2005
Naziv i sjedište tvrtke zaposlenja	MINISTARSTVO POLJOPRIVREDE, ŠUMARSTVA I VODNOGA GOSPODARSTVA, ulica grada Vukovara 78, Zagreb
Vrsta posla ili područje	Tajništvo, informatičko odjeljenje
Zanimanje i položaj koji obnaša	Stručni referent za informatičku podršku
Osnovne aktivnosti i odgovornosti	Tehnička podrška korisnicima, razvoj informatičke podrške, razvoj IT infrastrukture i informatička sigurnost, pomoć pri razvoju aplikativne podrške

Projekti	Nadogradnja IT infrastrukture MPŠ (redundantni Active Directory imenik, e-mail sustav MS Exchange, antivirusni sustav Sophos)

Datum (od – do)	1993 – 2002
Naziv i sjedište tvrtke zaposlenja	Euro-NET d.o.o., informatički inženjering i usluge, Zlatareva zlata 8, 10020 Zagreb
Vrsta posla ili područje	Programer, sistem analitičar, dizajner aplikacija, infrastrukturni projekti
Zanimanje i položaj koji obnaša	Programer, sistem analitičar, direktor u privatnoj tvrtki
Osnovne aktivnosti i odgovornosti	Razvoj, testiranja i isporuke aplikacija prema zahtjevima korisnika, prodaja aplikacija, infrastrukturna rješenja, umreženi sustavi.
Projekti	Autor niza aplikativnih rješenja od komercijalnih aplikacija do aplikacija prema zahtjevu korisnika

Glavna područja interesa:

Profesionalno:

Informatička tehnologija – primjena, upravljanje

Sigurnost informacija,

Sigurnost informatičke tehnologije i usluga,

Upravljanje neprekidnošću poslovanja/Planovi oporavka od katastrofe

Privatno:

Programiranje, DIY projekti, Linux, mikroprocesori

Curriculum Vitae

Dražen Marinović

I was born in Zagreb, where I finished elementary and secondary education. I graduated from the Faculty of Mechanical Engineering and Naval Architecture in Zagreb in 2006. In 1993, I have established my own company whose main business was the development of application support and development of infrastructure solutions. Since 2002 I work exclusively on IT sector in public sector and I have more than 25 years of working experience.

Personal information

Place of birth:	Zagreb, Croatia
Date of birth:	23 April 1967
Address:	Zlatarova zlata 8, 10020 Zagreb, Croatia
Phone:	+385 / (0)1 – 6547 975 (home)
	+385 / (0)99 – 6169 064 (mobile)
e-mail:	drazen.marinovic@apprrr.hr

Education:

Postgraduate specialist study	Faculty of organization and informatics, Varaždin (ongoing)
Graduate	Faculty of Mechanical Engineering and Naval Architecture Zagreb, (2006), University of Zagreb

Secundary School *Technical School "O.C. Nikola Tesla"*, Zagreb (1986)

Trainings:

During the working period, I have completed a series of specialized courses from various fields of IT technology. Recently, I am most involved in project management, information management and information security management. Please find below the list of certificates:

- *MCP – Microsoft Certified Professional*
- *MCSA – Microsoft Certified System Administrator*
- *MCSE – Microsoft Certified System Engineer*
- *Certified Lead Provisional Implementer for ISO/IEC 27001*
- *Certified Internal Auditor for ISMS - ISO/IEC 27001:2005*
- *BCP – uspostava prema normi ISO/IEC 22301:2012*
- *Membership: ISACA*
- *A series of seminars on security, infrastructure solutions and application support development*

Language skills (Mark 1 to 5 for competence, where 5 is the highest):

Croatian - Mother Tongue

English - 4

Working expirience:

Date (from – to)	December 2009 - to date
Company	Paying Agency For Agriculture, Fisheries And Rural Development, ulica grada Vukovara 269d, Zagreb (abr. PAAFRD)
Scope of work	Sector for IT Management
Position	Head of Sector
Responsibility	Management and coordination of Sector including technical support, application management and application development and information security management
Projects	Upgrading the PAAFRD Information System - Application Support (2010, 2011, 2012, 2013 and 2014) - Project Manager Aligning current business with ISO / IEC 27002 (2010) Project Board – a member Establishment of BCM system in APPRRR (2012)- Project manager Establishment of the secondary location of the APPRRR (2012) Computing Centre - Project Manager Certificate of Business Agency with ISO / IEC 27001: 2013 (2015), a Member of Project Board

Date (from – to)	May 2005 - December 2009
Company	Ministry of Agriculture, Fisheries and Rural Development; Directorate for Market and Structural support in Agriculture, ulica grada Vukovara 269d, Zagreb
Scope of work	Sector for IT Management
Position	Head of Sector
Responsibility	Management and coordination of Sector including technical support, application management and application development and information security management

Projects	Upgrading the PAAFRD Information System - Application Support (2005, 2006, 2007, 2008 and 2009) - Project Manager Establishment of the entire IT infrastructure needed for the operation of PAAFRD in the Republic of Croatia (2005-2006) Project Leader Initial Establishment of ISO / IEC 27002 (2005) World Bank project - Supply and Equipping the PAAFRD's Data Centre - Project Leader
Date (from – to)	2002 - May 2005
Company	Ministry of Agriculture, Fisheries and Water Management, ulica grada Vukovara 78, Zagreb
Scope of work	General Secretariat, IT Department
Position	Expert clerk for IT support
Responsibility	Customer Technical Support, Development of IT Infrastructure and IT Security, development information system, development of IT infrastructure information security management, consultant in the development of application support
Projects	Upgrading IT Infrastructure of Ministry of Agriculture (Redundant Active Directory Directory, MS Exchange Email System, Sophos AntiVirus System)
Date (from – to)	1993 – 2002
Company	Euro-NET d.o.o., IT engineering and services, Zlatareva zlata 8, 10020 Zagreb
Scope of work	Software developer, Information system analyst, Solution Architect, infrastructural projects
Position	Software developer, Information system, Director at private firm
Responsibility	Development, testing and delivery of applications according to user requirements, application sales, infrastructure solutions, networking systems.

Projects	Author of a number of application solutions from commercial applications to applications based on customer request

Main areas of interest:

Professionally:

Implementation of information security management system

Systems Information Development

Security of Information Technology and Services

Business Continuity Management / Disaster Recovery Plans

Privately:

Programming, DIY Projects, Linux, Microprocessors