Oporavak od katastrofe i upravljanje kontinuitetom poslovanja: usporedba softvera za izradu sigurnosnih kopija

Radić, Ivan

Master's thesis / Diplomski rad

2019

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Economics and Business / Sveučilište u Zagrebu, Ekonomski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:148:162137

Rights / Prava: Attribution-NonCommercial-ShareAlike 3.0 Unported/Imenovanje-Nekomercijalno-Dijeli pod istim uvjetima 3.0

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



Repository / Repozitorij:

REPEFZG - Digital Repository - Faculty of Economcs & Business Zagreb







Sveučilište u Zagrebu

Ekonomski fakultet

Menadžerska informatika

OPORAVAK OD KATASTROFE I UPRAVLJANJE KONTINUITETOM POSLOVANJA: USPOREDBA SOFTVERA ZA IZRADU SIGURNOSNIH KOPIJA

Diplomski rad

Ivan Radić

Zagreb, rujan 2019.

Sveučilište u Zagrebu

Ekonomski fakultet

Menadžerska informatika

OPORAVAK OD KATASTROFE I UPRAVLJANJE KONTINUITETOM POSLOVANJA: USPOREDBA SOFTVERA ZA IZRADU SIGURNOSNIH KOPIJA

DISASTER RECOVERY AND BUSINESS CONTINUITY MANAGEMENT: COMPARISON OF BACKUP SOFTWARES

Diplomski rad

Ivan Radić, 0067488369

Mentor: Prof. dr. sc. Mario Spremić

Zagreb, rujan 2019.

IVAN RADIĆ

Ime i prezime studenta/ice

IZJAVA O AKADEMSKOJ ČESTITOSTI

Izjavljujem i svojim potpisom potvrđujem da je DIPLOMSKI RAD isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju korištene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Student:

U Zagrebu, 16.09.2019.

Sažetak

Kontinuitet poslovanja se definira kao sposobnost organizacije da nastavi isporuku proizvoda ili usluga prema prihvatljivim unaprijed definiranim razinama nakon pojave poremećaja koji remeti redovne poslovne operacije organizacije. Osnovna ideja kontinuiteta poslovanja je zaštita informacija u slučaju nekih većih neočekivanih nezgoda odnosno osiguranje njihove dostupnosti. Neželjeni događaji poput hakerskih napada, terorizma, prirodnih katastrofa ili pak svakodnevnih ljudskih pogrešaka sve su učestaliji i organizacije su toga sve više svjesne. Svaki prekid poslovnih operacija može organizacijama nanijeti značajne financijske gubitke. U tim ekstremnim uvjetima jedini odgovor je imati spremnu strategiju i plan za kontinuitet poslovanja i oporavak od katastrofe što je i predmet ovog rada. Uz detaljnu razradu procesa upravljanja kontinuitetom poslovanja predstavljena će biti i aplikacijska rješenja koja podupiru neprekidnost poslovanja i omogućuju oporavak poslovnih operacija.

Ključne riječi: Kontinuitet poslovanja, upravljanje kontinuitetom poslovanja, organizacija, oporavak od katastrofe, plan kontinuiteta poslovanja

Summary

Business continuity is defined as corporate capability which exists whenever organizations can continue to deliver their products and services at acceptable predefined levels after disruptive incidents have occurred. The basic idea of business continuity is to protect information in the event of some major unexpected incidents and to ensure their availability. Incidents such as hacking, terrorism, natural disasters, or everyday human errors are becoming more common and organizations are becoming more aware of this. Any disruption in business operations could cause significant financial loss to organizations. That's why these extreme conditions require prepared strategy and plan for business continuity and disaster recovery, which is the subject of this paper. In addition to a detailed elaboration of the business continuity management process, I will present application solutions that support business continuity and that have tools for restoring and recovering business operations.

Key words: Business continuity, business continuity management, organization, disaster recovery, business continuity plan

S A D R Ž A J

1. UVOD 1
1.1. Predmet i cilj rada 1
1.2. Izvori podataka i metode prikupljanja 1
1.3. Sadržaj i struktura rada 1
2. KONCEPT POSLOVNOG KONTINUITETA I OPORAVKA OD KATASTROFE 3
2.1. Definiranje poslovnog kontinuiteta 3
2.1.1. Pojam i evolucija poslovnog kontinuiteta 4
2.1.2. Upravljanje kontinuitetom poslovanja 6
2.1.3. Otpornost organizacije 10
2.2. Planiranje poslovnog kontinuiteta 12
2.2.1. Osnovno o planu kontinuiteta poslovanja 13
2.2.2. Vrste planova i temeljne faze planiranja 16
2.3. Oporavak od katastrofe 19
2.3.1. Definicija oporavka od katastrofe 19
2.3.2. Vrste katastrofa u poslovanju 22
2.3.3. Planiranje oporavka od katastrofe 24
3. UPRAVLJANJE RIZICIMA I UTJECAJ NA POSLOVANJE 27
3.1. Pojam i obilježja informatičkih rizika 27
3.2. Koncept upravljanja rizicima organizacije 30
3.3. Procjenjivanje rizika 34
3.4. Analiza utjecaja na poslovanje 37
3.5. Strategije reduciranja utjecaja rizika 40
4. RAZVOJ, TESTIRANJE, REVIZIJA I ODRŽAVANJE PLANA KONTINUITETA POSLOVANJA 43
4.1. Razvijanje plana kontinuiteta poslovanja i plana oporavka u slučaju katastrofe 43
4.2. Testiranje i revizija plana 46
4.3. Ažuriranje BC/DR plana 49
5. USPOREDBA ALATA ZA IZRADU SIGURNOSNIH KOPIJA 52
5.1. Općenito o backup alatima 52

5.2. Veeam Backup and Replication 53
5.3. Commvault Complete Backup and Recovery 63
5.4. Usporedba Veema i Commvaulta 74
6. ZAKLJUČAK 77
POPIS LITERATURE 78
POPIS SLIKA 81
POPIS TABLICA 83
ŽIVOTOPIS 84

1. UVOD

1.1. Predmet i cilj rada

Tehnološka rješenja su esencijalan resurs suvremenog poslovanja koji donosi mnoge koristi, ali ujedno i određene prijetnje. Neželjeni događaji poput hakerskih napada, terorizma, prirodnih katastrofa ili pak svakodnevnih ljudskih pogrešaka sve su učestaliji i organizacije su toga sve više svjesne. Svaki prekid poslovnih operacija može organizacijama nanijeti značajne financijske gubitke. U tim ekstremnim uvjetima jedini odgovor je imati spremnu strategiju i plan za kontinuitet poslovanja i oporavak od katastrofe. Predmet ovog rada jest koncept upravljanja poslovnim kontinuitetom i njegov integralni dio koji se odnosi na oporavak poslovanja u slučaju neželjenih događaja odnosno katastrofe. Cilj rada je detaljno pojasniti proces i planiranje kontinuiteta poslovanja, te zatim predstaviti i prikazati aplikacijska rješenja koja podržavaju neprekidnost informacijskih sustava.

1.2. Izvori podataka i metode prikupljanja

Za pisanje ovog rada korišteni su primarni i sekundarni izori. Sekundarni izvori podataka uključuju stručnu domaću i stranu literaturu iz knjižnice Ekonomskog fakulteta i Nacionalne i sveučilišne knjižnice u Zagrebu. Zatim je korišten portal znanstvenih časopisa Republike Hrvatske - Hrčak, razne publikacije preko Google Scholar pretraživača i različite web izvore relevantne u kontekstu informacijske tehnologije i kontinuiteta poslovanja.

Primarni izvori podataka odnose se na prikaz rada dvije aplikacije u vlastitoj izradi autora.

U obradi rada korištene su metode analiziranja predmetnog sadržaja, opisne metode sadržaja te zatim metode sinteze kojim su se naposljetku povezale činjenice i tvrdnje.

1.3. Sadržaj i struktura rada

Ovaj diplomski radi se sastoji od 6 poglavlja.

Prvo poglavlje se odnosi na uvod u kojem se definira predmet i cilj rada, izvori podataka za pisanje rada te sadržaj i struktura.

U drugom poglavlje obrađeni su pojmovi poslovnog kontinuiteta, poslovne otpornosti, upravljanja kontinuitetom poslovanja i njegovog produkta, plana kontinuiteta poslovanja. Zatim je pojmovno određen oporavak od katastrofe i njegove sastavnice.

Treće poglavlje se odnosi na prvi dio procesa upravljanja kontinuitetom poslovanja, upravljanje rizicima. Ovo poglavlje sadrži pojmovno određenje i analizu rizika, te prikaz tehnika i faza upravljanja rizicima u sklopu kontinuiteta poslovanja.

Četvrto poglavlje govori o razvoju plana kontinuiteta poslovanja i plana oporavka od katastrofe koji se nastavljaju na prethodne faze upravljanja rizicima. Zatim će biti predstavljeni postupci ispitivanja plana i revizija plana, te naposljetku aktivnosti održavanja i ažuriranja.

U petom poglavlju će prvo biti rečeno nešto više o postupcima i alatima sigurnosnog kopiranja. Nakon toga slijedi obrada dva konkurentna programska rješenja, Veeam Backup and Replication i Commvault Complete Backup and Recovery, koja služe za osiguravanje sigurnosti i dostupnosti podataka i informacijskih sustava.

Posljednje poglavlje se odnosi na zaključak diplomskog rada.

2. KONCEPT POSLOVNOG KONTINUITETA I OPORAVKA OD KATASTROFE

Kako tehnologija postaje sve važnija za korporativne operacije na svim razinama organizacije, raspon upotrebe iste se proširio i postao gotovo sveobuhvatan. U suvremenom poslovanju teško je pronaći dijelove kompanije u kojima se ne koristi određena vrsta tehnologije. Kao rezultat toga, potreba za planiranjem mogućih poremećaja u tehnološkim uslugama eksponencijalno se povećava. Planovi kontinuiteta poslovanja (eng. *Business Continuity - BC*) i planovi oporavka od katastrofa (eng. *Disaster Recovery - DR*) još uvijek ne postoje u mnogim kompanijama usprkos sve učestalijim napadima na ključne poslovne procese i resurse.[1]

Planiranje kontinuiteta poslovanja i oporavka od katastrofe inače su podvrsta šire discipline koja se naziva poslovna kontingencija. Osnovna svrha plana poslovne kontingencije je davanje odgovora na pitanja poput: „Što trebamo napraviti ako se ovo dogodi?“. Poslovna kontingencija pruža pregled odluka i mjera koje treba poduzeti u slučaju nastanka okolnosti koje se vežu za određene aktivnosti ili situacije. U suštini, kontingencijski planovi formalno pripremaju organizaciju na različite varijacije u poslovnom okruženju s primarnim ciljem osiguranja opstanka organizacije kroz pripremu, reagiranje i prilagođavanje tim varijacijama.[2]

2.1. Definiranje poslovnog kontinuiteta

Kontinuitet poslovanja i oporavak od katastrofe često se poistovjećuju i koriste naizmjenično jer se sastoje od jednakih elemenata, no nemaju jednako značenje. Zato je potrebno prvo definirati ove ključne pojmove. Poslovni kontinuitet ima šire značenje i odnosi se održavanje neprekidnog i neometanog rada poslovnih procesa. Prema Institutu za poslovni kontinuitet (eng. *The Business Continuity Institute*) pojam podrazumijeva planiranje rješavanja teških situacija kako bi organizacija mogla nastaviti funkcionirati sa što manje poremećaja.[3]

---

[1] Snedaker, S. (2007) *Business Continuity & Disaster Recovery for IT Professionals.* Burlington, MA: Syngress Publishing.

[2] Ransome, J. F. i Rittinghouse, J. W. (2005) *Business Continuity and Disaster Recovery for InfoSec Managers*. Burlington, MA: Elsevier Digital Press.

[3] *Introduction to Business Continuity* [online]. Thebci.org. Dostupno na: https://www.thebci.org/knowledge/introduction-to-business-continuity.html

2.1.1. Pojam i evolucija poslovnog kontinuiteta

Osnovna ideja kontinuiteta poslovanja je zaštita informacija u slučaju nekih većih neočekivanih nezgoda odnosno osiguranje njihove dostupnosti.[4]

Prema ISO 22301: 2012 standardu, poslovni kontinuitet definira se kao sposobnost organizacije da nastavi isporuku proizvoda ili usluga prema prihvatljivim unaprijed definiranim razinama nakon pojave poremećaja koji remeti redovne poslovne operacije organizacije. [5]

Pojedine kompanije poput financijskih institucija, kreditnih kompanija ili najvećih online trgovina ne mogu si dopustiti ni najmanje prekide u poslovanju jer ih isti mogu koštati milijune dolara. Zbog toga, kontinuitet poslovanja mora osigurati stalan i neprekidan rad kompanije bez obzira na rizike, prijetnje i uzroke prekida rada.

Prekid poslovanja označava situaciju kada poslovanje ne raspolaže poslovnim resursima odnosno nema pristup resursima za normalno odvijanje. Prekidi poslovanja su oni događaji koji uzrokuju značajne zastoje ili gubitke ključnih poslovnih procesa što za posljedicu ima velik negativan utjecaj i ozbiljne negativne posljedice za kompaniju. Značajan prekid poslovanja je neželjeni događaj koji narušava jedan od tri temeljna parametra svih informacijskih sustava, a to je raspoloživost sustava ili dijela sustava. U slučaju značajnijeg prekida, nužno je osigurati pravovremen oporavak i nastavak odvijanja ključnih poslovnih aktivnosti, što je zapravo svrha upravljanja kontinuiteta poslovanja (engl. *Business Continuity Management – BCM*).[6]

Na slici 1. je prikazan ciklus kontinuiteta poslovanja koji se sastoji od planiranja, implementacije i procjene plana. Kao što se može iščitati sa slike, nakon nastanka katastrofe prvo se vrše aktivnosti oporavka od katastrofe koje se zatim počinju preklapati s aktivnostima poslovnog kontinuiteta.

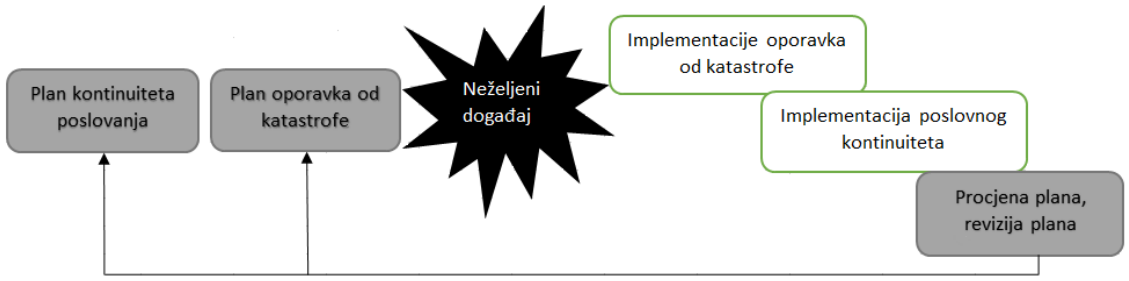
---

[4] CARNet CERT (2010) Upravljanje kontinuitetom poslovnih procesa [online] www.cis.hr. Dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-15-307.pdf

[5] *Introduction to Business Continuity* [online]. Thebci.org. Dostupno na: https://www.thebci.org/knowledge/introduction-to-business-continuity.html

[6] Marinović, D. (2017) *Uspostava neprekinutosti poslovanja, temeljem analize utjecaja na poslovanje*. Završni specijalistički rad. Zagreb: Fakultet strojarstva i brodogradnje.

Slika 1. Ciklus poslovnog kontinuiteta



Izvor: Snedaker, S. (2007) *Business Continuity & Disaster Recovery for IT Professionals*

Upravljanje kontinuitetom poslovanja rezultat je procesa koji je započeo ranih 1970-ih kao računalno planiranje oporavka od katastrofa (engl *Disaster Recovery Planning - DRP*), a zatim prešao kroz doba u kojem je naglasak bio na planiranju kontinuiteta poslovanja, a ne na upravljanju. U 70-ima aktivnostima DRP-a upravljao je računalni menadžer. Uvidjevši da koncentracija sustava i podataka sama po sebi stvara nove rizike, menadžment računalnih operacija uveo je formalne postupke koji reguliraju pitanja poput sigurnosnih kopija i oporavka, ograničenja pristupa, fizičke sigurnosti, mjera otpornosti kao što su alternativno napajanje i kontrola promjena.

U to vrijeme su se stanke i prekidi tolerirali danima, jer su troškovi alternativnih lokacija i rezervnih računala bili preveliki. Međutim, organizacije poput banaka bile su u ranjivijem položaju i uložile su znatna sredstva u instaliranje i testiranje računala na alternativnim mjestima. Rezervne trake ili diskovi sve su se više čuvali na zaštićenim mjestima, daleko od računalnog središta.

U 1980-ima je zabilježen rast komercijalnih web lokacija za oporavak koje nude usluge, često na zajedničkoj osnovi, što je označavalo početak sofisticiranih centara za oporavak koji djeluju i dan danas. No, naglasak je i dalje bio samo na IT-ju. Planovi za oporavak imali su dokumentirane procedure za zaštitu i obnavljanje rada računala.

90-te su donijele značajne promjene u IT okruženju, te se prešlo sa planiranja oporavka od katastrofe na širu aktivnost, planiranje kontinuiteta poslovanja (engl. *Business Continuity*

Planning – BCP). Razvojem informacijske tehnologije i informacijskih sustavi, mijenjali su se i ciljevi plana poput prihvatljivih zastoja i vremenskih prekida operacija. Naglasak je i dalje bio na IT pristupu. Na sljedećem stupnju razvoja BCP je postao BCM čime je stavljen naglasak na upravljanje, a ne samo na planiranje. Upravljanje kontinuitetom poslovanja je obuhvaćalo i upravljanje rizicima i mjerama za smanjenje rizika. BCM se više nije gledao kao projekt, sa svojim početkom i definiranim krajem, već je evoluirao u kontinuirani proces. Nakon poznate katastrofe koja se dogodila 11. rujna u New Yorku, upravljanje kontinuitetom poslovanja dobilo je još više na važnosti. Organizacije su postale svjesne važnosti BCM-a o kojem ovisi i sam opstanak poslovanja. Sljedeći korak u razvoju principa BCM-a jest uključivanje istih kao sastavni dio poslovnog planiranja. [7]

2.1.2. Upravljanje kontinuitetom poslovanja

Britanski institut za standarde (engl. *British Standard Institute – BSI*) je izdao standardiziranu metodologiju BS 25999-1 (2006. godine) i BS 25999-2 (2007. godine) za područje upravljanja kontinuitetom poslovanja. Službena definicija upravljanja kontinuitetom poslovanja prema standardu 25999-1 jest:

„*Holistički postupak upravljanja koji identificira potencijalne prijetnje organizaciji i učinke na poslovanje koje bi one prijetnje, ako su ostvarene, mogle prouzrokovati, i koji pruža okvir za izgradnju organizacijske otpornosti s mogućnošću učinkovitog odgovora koji štiti interese ključnih interesno utjecajnih skupina, ugled, marku i aktivnosti koje stvaraju vrijednost*.“ [8]

Institut za poslovni kontinuitet je definirao upravljanje kontinuitetom poslovanja kao: „*Postupak anticipiranja incidenata koji imaju utjecaj na kritične funkcije i procese organizacije i osiguravanja odgovora na svaki od njih na planiran i uvježban način.“* Ova definicija naglašava tri glavna elementa:

- *Anticipiranje incidenata* – Organizacija mora ispitati rizike i prijetnje kojima je izložena i razmotriti najefikasnije načine postupanja ukoliko eskaliraju.

[7] Gallagher, M. (2003) *Business Continuity Management: How to Protect Your Company from Danger*. Harlow: Pearson Education Limited.
[8] Hiles, A. (2007*) The Definitive Handbook of Business Continuity Management.* Chichester: John Wiley & Sons, Ltd.

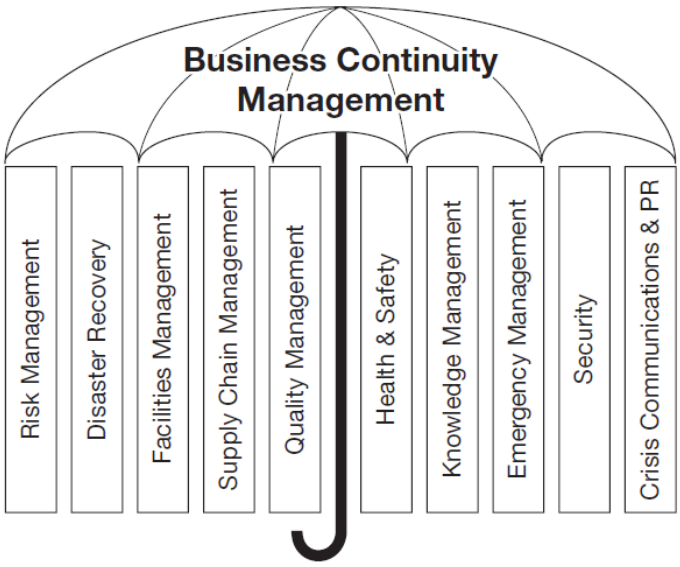
- *Utjecaj na kritične funkcije i procese* – BCM se ne bavi planovima i postupcima za svakodnevne stvari koje mogu poći po zlu, već isključivo incidentima koji imaju značajan utjecaj na temeljne aktivnosti organizacije.
- *Odgovor na planiran i uvježban način* – BCM obuhvaća planiranje, smisleno uključivanje odgovarajućeg osoblja, prihvaćanje i vlasništvo nad planom, te temeljito testiranje plana. [9]

Upravljanje kontinuitetom poslovanja je dinamičan, proaktivan i trajan proces koji mora biti uvijek ažuran i prilagođen svojoj svrsi kako bi postigao učinkovitost. Temeljni ciljevi svake efektivne BCM strategije jesu:

- ✓ osigurati sigurnost zaposlenika,
- ✓ obraniti ugled i imidž organizacije,
- ✓ minimalizirati utjecaj incidenata na kupce i klijente,
- ✓ spriječiti ili bar ograničiti utjecaj van organizacije,
- ✓ prikazati medijima, tržišnim sudionicima i interesno utjecajnim skupinama da organizacija učinkovito i djelotvorno upravlja situacijama,
- ✓ zaštiti imovinu organizacije
- ✓ i udovoljiti zakonima, regulativama i zahtjevima i pravilima osiguravatelja.[10]

[9] Gallagher, M. (2003) *Business Continuity Management: How to Protect Your Company from Danger*. Harlow: Pearson Education Limited.
[10] Reuvid, J. (2005) *The Secure Online Business Handbook: e-commerce, IT functionality & business continuity*. London i Sterling, VA: Kogan Page Limited.

Slika 2. Interdisciplinarni proces upravljanja kontinuitetom poslovanja

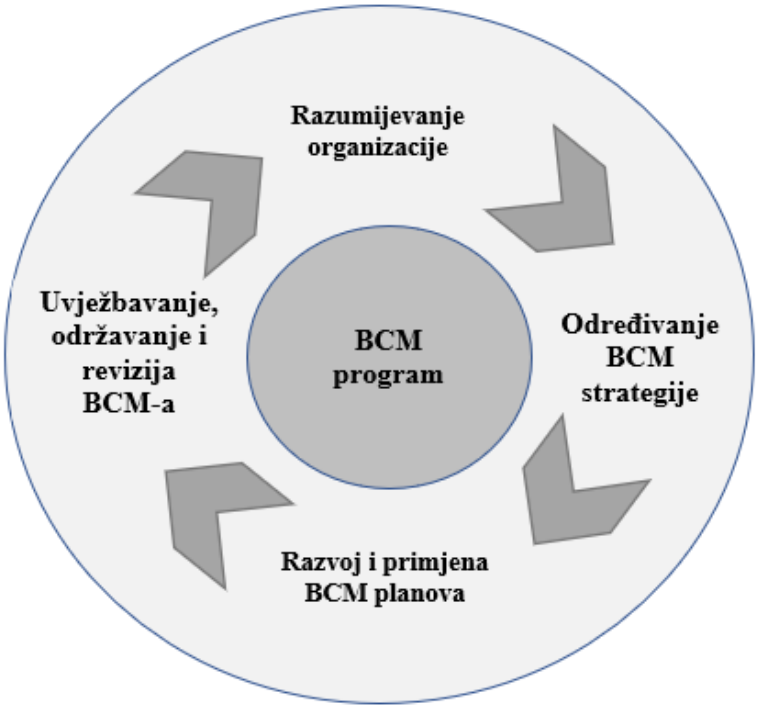


Izvor: Reuvid, J. (2005) The Secure Online Business Handbook

Upravljanje kontinuitetom poslovanja ne bavi se isključivo oporavkom od poremećaja i prevencijom i ublažavanjem štetnih događaja na funkcioniranje poslovnih operacija već je to jedan proces koji ujedinjuje širok spektar poslovnih i upravljačkih disciplina. Na slici iznad je slikovito prikazano koje sve discipline su potpuno ili dijelom dio upravljačkog procesa kontinuiteta poslovanja, od upravljanja rizicima, upravljanja lancem vrijednosti do upravljanja znanjem, sigurnosti i hitnim slučajevima.

Standard 25999-1, kojeg sam se dotakao na početku poglavlja, uključuje i dijagram koji opisuje životni ciklus upravljanja kontinuitetom poslovanja. Ovaj se ciklus sastoji od 4 osnovna elementa prikazana na slici niže. Svaki element je jednako važan za stvaranje učinkovitog procesa BCM-a.

Slika 3. Ciklus upravljanja kontinuitetom poslovanja



Izvor: Hiles, A. (2007) The Definitive Handbook of Business Continuity Management

Razumijevanje organizacije – Aktivnosti ove faze pružaju informacije koje omogućuju određivanje prioriteta proizvoda i usluga organizacije, te žurnost aktivnosti koje su potrebne za njihovo ostvarivanje. Time se postavljaju zahtjevi koji će odrediti odabir odgovarajućih BCM strategija. Ključni koraci za razumijevanje su: 1) prepoznati ciljeve, obveze stakeholdera, aktivnosti, imovinu i resurse; 2) procijeniti učinke zaustavljanja aktivnosti; 3) ocijeniti prijetnje kritičnih aktivnosti; i 4) razmotriti unutarnje i vanjske ovisnosti.

Određivanje BCM strategije – U ovoj se fazi ocjenjuje niz BCM strategija i time se omogućava odabir odgovarajuće za svaki proizvod ili uslugu, tako da organizacija može nastaviti isporučivati te proizvode i usluge na prihvatljivoj razini i unutar prihvatljivog vremenskog okvira tijekom i nakon poremećaja. Odabrana strategija treba uzimati u obzir već implementiranu poslovnu otpornost i zaštitne mjere unutar organizacije.

Razvoj i primjena BCM planova – Ovime se stvara upravljačkog okvir i struktura upravljanja incidentima, kontinuitetom poslovanja i planovima za oporavak poslovanja koji detaljno opisuju korake koje treba poduzeti za vrijeme i nakon incidenta za održavanje ili obnovu operacija.
Uvježbavanje, održavanje i revizija BCM-a – Četvrtom fazom organizacija pokazuje i dokazuje u kojoj mjeri su njene strategije i planovi cjeloviti, aktualni i ispravni, te osluškuje promjene i u skladu s njima određuje moguća poboljšanja. [11]

2.1.3. Otpornost organizacije

U svijetu koji se jako brzo mijenja, organizacije mogu biti izložene prirodnim katastrofama, poremećajima u kritičnoj infrastrukturi i utjecajima poremećaja van organizacije poput neželjenih događaja u mikro okruženju. Ove prijetnje mogu nadmašiti predviđene i planirane razmjere jačine štete ili pak frekventnosti pojave. Zato sposobnost organizacije za preživljavanje ovakvih događaja, a i učenje i iskorištavanje istih za napredak ovisi o njenoj otpornosti (engl. *resilience*). Otpornost se opisuje kao sposobnost organizacije da minimizira utjecaj teških poremećaja na ciljeve organizacije, odnosno sposobnost da "odbije" negativne utjecaje. No, mnoge organizacije su uspjele u iskorištavanju neželjenih događaja za poboljšanje vlastitog položaja poput povećanja tržišnog udjela, rast ugleda, smanjenja zahtjeva za državnim intervencijama i povećanja regulacija i slično. Visoko otporne organizacije imaju sposobnost da iskoriste teške i razorne događaje za brzi napredak. Parsons navodi primjer kompanije Nokia koja je u ožujku 2000. godine doživjela velike poremećaje u lancu opskrbe, te naposljetku učinkovito iskoristila ovaj događaj za povećanje tržišnog udjela na tržištu mobilnih telefona.[12]
Poslovna otpornost i poslovni kontinuitet ne mogu se smatrati sinonimima. Otpornost je širi pojam i obuhvaća upravljanje rizicima, kontinuitetom, sigurnosti i kriznim situacijama. Može se reći da je poslovno otporna organizacija sposobna očuvati neprekidnost poslovnih operacija odnosno da je implementirana otpornost temeljna pretpostavka za očuvanje poslovnog kontinuiteta.

[11] Hiles, A. (2007*) The Definitive Handbook of Business Continuity Management.* Chichester: John Wiley & Sons, Ltd.
[12] Parsons, D. (2010) Organizational Resilience. *The Australian Journal of Emergency Management*, 25 (2), str. 18-20

Parsons je definirao osam ključnih svojstava otpornih organizacija koja omogućuju: predviđanje i razumijevanje prijetnji; razumijevanje utjecaja prijetnji na organizaciju, lanac opskrbe, okruženje na koje djeluje i osoblje; razvijanje i održavanje partnerstva sa ključnim interesno utjecajnim skupinama, sektoru i zajednici; reakciju, oporavljanje i rast nakon disruptivnog događaja; osigurati osoblje voljnim i sposobnim za postizanje organizacijskih ciljeva; artikuliranje ciljeva i osiguranje snažnog osjećaja svrhe i zajedništva kao odgovora na oporavak i rast od poremećaja; vođenje jasnog smjera u rješavanju problema. Ključni atributi otporne organizacije jesu:

Svjesnost – Ovaj atribut omogućava predviđanje i razumijevanje novih prijetnji te razumijevanje utjecaja prijetnji na organizaciju, lanac opskrbe, okruženje u kojem djeluje i osoblje. Svjesna organizacija ima znanje za prepoznavanje i tumačenje slabih signala koji omogućavaju ranu identifikaciju rizika u razvoju.

Prilagodljivost i fleksibilnost – Kompetencije prilagodljivosti i fleksibilnosti se razvijaju razmatranjem i analizom scenarija "što ako", učenjem iz događaja koje su doživjele druge organizacije, pripremom i vježbom strategija reagiranja i oporavka, razvijanjem vještina rješavanja problema te sistemskim razmišljanjem.

Spremnost na promjene - Povećava se anticipiranjem budućih događaja i razmatranjem budućnosti poslovanja. Spremnost na promjene zahtjeva kontinuirano istraživanje novih tehnologija.

Znanje o međuovisnosti - Podrazumijeva pouzdane odnose s ključnim interesnim skupinama, regulatorima i dobavljačima. Organizacije sa snažno razvijenim znanjem o ovisnosti imaju uspostavljene sporazume o uzajamnoj pomoći s interesno utjecajnim skupinama.

Integracija – Rad u timu i dijeljenje informacija i resursa ključno je za razvoj integrirane organizacije.

Kultura i vrijednosti – Organizacijski atribut kulture i vrijednosti jedan je od najvažnijih u postizanju otpornosti. U kriznim i stresnim situacijama organizacija mora imati snažno jedinstvo, svrhu, zajednička vjerovanja, razvijen timski duh i volju da pobijedi neprilike.

Vodstvo - Snažno i odlučno vodstvo je potrebno da bi se postavili jasni ciljevi i omogućilo rješavanje organizacijskih problema. Vodstvo treba graditi nadu i optimizam među zaposlenima, voditi ih, jasno delegirati obaveze i komunicirati ciljeve.

Komunikacija – Nužna je komunikacija informacija između svih sudionika odnosno komunikacijski kanali moraju biti dostupni svima koji su uključeni u poslovne operacije. Informacije koje se prenose moraju biti točne, relevantna, potpuna i pravovremena. [13]

Američko vijeće za konkurenciju je definiralo otpornu organizaciju kao organizaciju koja je fleksibilna, agilna, prilagodljiva i pametno zna upravljati rizicima. Jedan od zaključaka vijeća jest da će se u 21. stoljeću konkurentska prednost i diferencija ostvarivati uspješnim anticipiranjem i upravljanjem rizika i oporavljanjem od poremećaja u poslovanju. Prvi korak k stvaranju otporne organizacije je svjesnost o turbulentnom i brzo promjenjivom vremenu u kojem se nalazi današnji poslovni svijet. Zatim je potrebno ugraditi otpornost u korporativnu kulturu kako bi ista bila temelj poslovanja. Treći korak je iskoristiti prednosti koje nudi otporna organizacija, a odnosi se na pretvaranje rizika i opasnosti u prilike. Nužno je da otpornost bude ugrađena u DNK organizacije i da bude potpomognuta čvrstim i snažnim procesima, programima treninga i agilnim sustavima kako bi organizacija zaista bila spremna i sposobna odgovoriti na sve smetnje u okruženju.[14]

2.2. Planiranje poslovnog kontinuiteta

Planiranje poslovnog kontinuiteta je interdisciplinarna aktivnost i obuhvaća metodologiju koja se koristi za stvaranje plana kontinuiteta poslovanja. Ovaj plan opisuje način na koji se organizacija priprema za buduće incidente koji bi mogli ugroziti osnovnu poslovnu djelatnost i dugoročnu stabilnost poduzeća. Takvi incidenti uključuju:

- Lokalne incidente (npr. požar, poplava),
- Regionalne incidente (npr. zemljotres) ili
- Nacionalne incidente(npr. pandemija).[15]

[13] Parsons, D. (2010) Organizational Resilience. *The Australian Journal of Emergency Management*, 25 (2), str. 18-20

[14] Bates, W. i Von Opstal, D. (2007) *Five for the Future*. Washington, D.C.: Council on Competitivenes. [online]. Dostupno na: http://quoniam.info/competitive-intelligence/PDF/ebooks/Five_Final_8858COC.pdf

[15] CARNet CERT (2010) Upravljanje kontinuitetom poslovnih procesa [online] www.cis.hr. Dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-15-307.pdf

2.2.1. Osnovno o planu kontinuiteta poslovanja

Plan kontinuiteta poslovanja (engl. *Business Continuity Plan – BCP*) je osnovni proizvod upravljanja kontinuitetom poslovanja 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. [16]

BCP se definira i kao identifikacija i zaštita kritičnih poslovnih procesa i resursa potrebnih za održavanje prihvatljive razine poslovanja, štiteći te resurse i pripremajući procedure za opstanak organizacije u vrijeme poremećaja u poslovanju. Plan kontinuiteta poslovanja nije čisto tehnički plan, već pokriva šire područje i smatra se planom upravljanja poslovanja. Razlog tome je što se kvalitetan BCP temelji na razumijevanju alata koji podržavaju svakodnevne poslovne operacije, poznaje procedure koje određuju tko će se i na koji način nositi s kriznom situacijom, te zapravo općenito ima razumijevanje kompletne organizacije. [17]

U planiranju poslovnog kontinuiteta i oporavka od nesreće IT stručnjaci imaju posebnu ulogu. S jedne strane nisu nužno odgovorni za sveukupno planiranje BC plana, ali kako je tehnologija uključena u gotovo svaku poslovnu operaciju, nisu u mogućnosti baviti se IT-ijem kao samostalnim problemom. Zato stvaranje cjelovitog i potpunog BC plana mora uključivati širi tim ljudi koji su stručni u različitim područjima i međusobno se nadopunjavaju.[18]

Na slici niže prikazani su elementi plana poslovnog kontinuiteta koji najčešće ulaze o obzir. Naravno, isti ovise o djelatnosti organizacije, no svakako prelaze granicu IT odjela i tiču se kompletnog poslovanja organizacije.

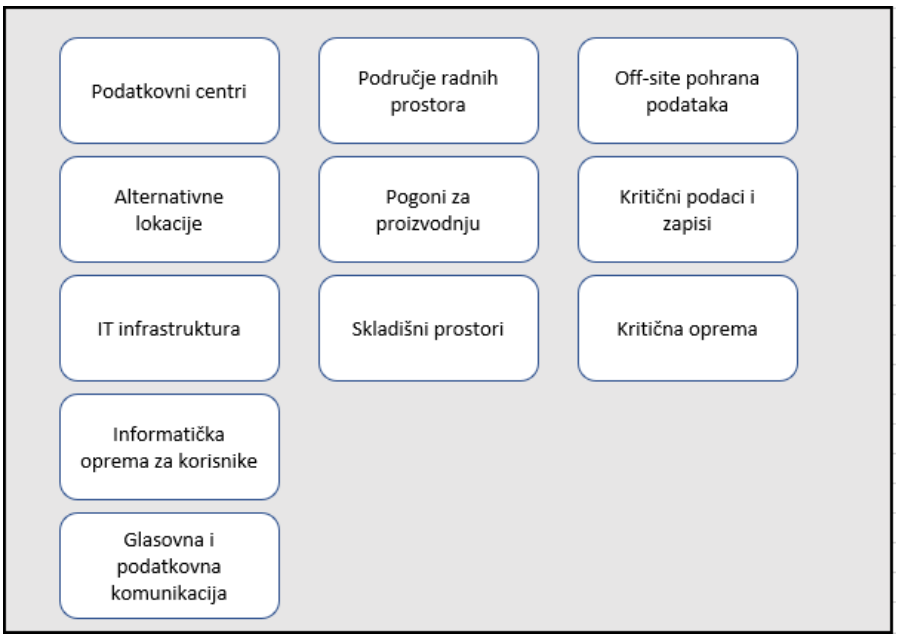
---

[16] Marinović, Dražen (2017) *Uspostava neprekinutosti poslovanja, temeljem analize utjecaja na poslovanje*. Završni specijalistički rad. Zagreb: Fakultet strojarstva i brodogradnje

[17] Hiles, A. (2007*) The Definitive Handbook of Business Continuity Management.* Chichester: John Wiley & Sons, Ltd.

[18] Snedaker, S. (2007) *Business Continuity & Disaster Recovery for IT Professionals.* Burlington, MA: Syngress Publishing.

Slika 4. Elementi plana kontinuiteta poslovanja i plana oporavka od katastrofe

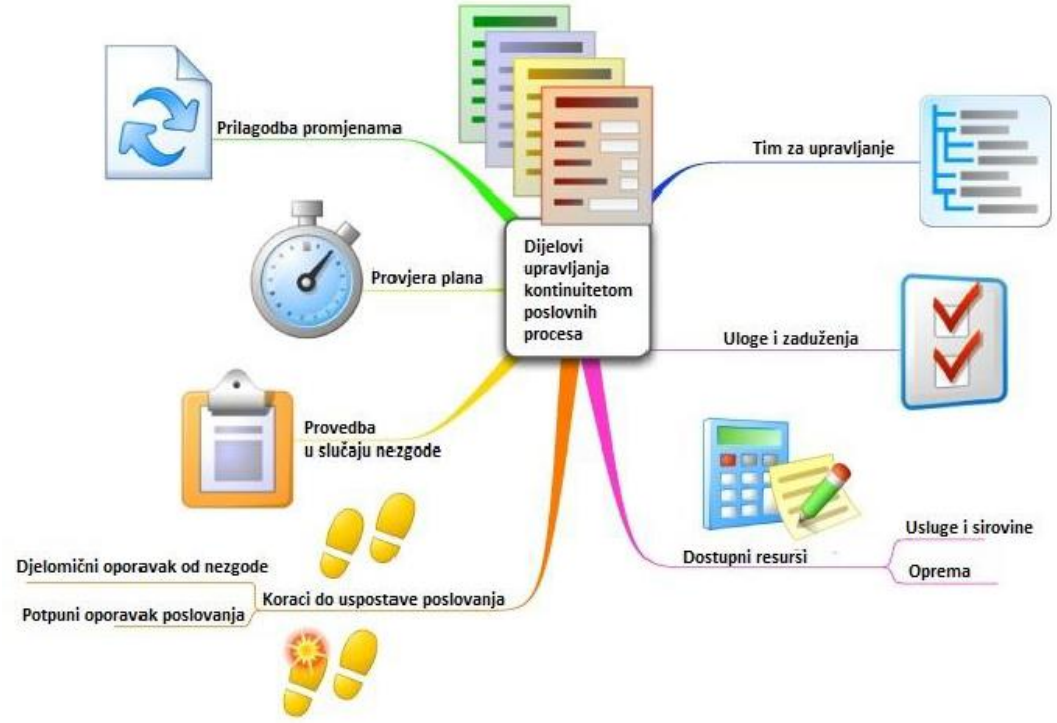


Izvor: Snedaker, S. (2007) Business Continuity & Disaster Recovery for IT Professionals

Metodologija planiranja kontinuiteta poslovanja služi stvaranju i validaciji plana za održavanje neprekidnosti poslovnih operacija prije, tijekom i nakon neželjenih događaja. Samim time ova metodologija omogućava uredno funkcioniranje poslovni procesa i ostvarivanje poslovnih ciljeva. Čest je slučaj da BCP služi kompanijama kao norma za stvaranje vlastitih strategija vezanih za tehnologiju i informatiku. Implementacija sustava sa stalnom dostupnosti može biti ogromna investicija odnosno trošak u vrijednosti od milijun dolara. Za neke kompanije to može biti investicija vrijedna ulaganja jer trošak stanke poslovanja od samo desetak minuta može koštati nekoliko puta više. Ključni pokretač u planiranju kontinuiteta poslovanja je novac odnosno razina tolerancije poduzeća na prekide poslovanja, te shodno tome želja i financijske mogućnosti za izbjegavanje neželjenih prekida. Da novac nije problem, svako poduzeće koje koristi neku vrstu tehnologije zasigurno bi se odlučilo na primjenu potpuno redundantnih sustava nulte stanke. No, naravno to nije slučaj jer mnogim poduzeća trošak implementacije sustava s

stalnom dostupnosti je jednostavno preskup i neisplativ. Stoga je nužno da plan kontinuiteta poslovanja odgovara veličini poduzeća, njegovom proračunu i raznim drugim ograničenjima.[19] Osnovna svrha svakog plana kontinuiteta poslovanja jest osigurati nastavak kritičnih poslovnih operacija i oporavak istih u slučaju javljanja incidenta. Primjenom BCP-a moguće je spriječiti potencijalne poremećaje od najnižih do katastrofalnih razmjera ili pak ublažiti veličini štete.

Slika 5. Dijelovi upravljanja kontinuitetom poslovanja



Izvor: Centar informacijske sigurnosti (2011) Upravljanje kontinuitetom poslovnih procesa

Na slici su prikazani sastavni dijelovi BCM procesa kako ih je definirao Centar informacijske sigurnosti. Nastavno na ovo, dalje u radu biti će pojašnjene faze u planiranju poslovnog kontinuiteta.

Neki od ciljeva plana kontinuiteta poslovanja obično se odnose na:

[19] Snedaker, S. (2007) *Business Continuity & Disaster Recovery for IT Professionals.* Burlington, MA: Syngress Publishing.

- pružanje određene razine sigurnosti osoblja za vrijeme katastrofe,
- minimalizacija financijskog gubitka,
- omogućavanje redovnog i učinkovitog prelaska operacija iz normalnih u hitne uvjete,
- ublažavanje negativnih učinaka na poslovanje, strateške planove, reputaciju, financijske pokazatelje i tržišnu poziciju ,
- davanje posebnih smjernica primjerenih za kompleksne i nepredvidive događaje,
- omogućavanje dosljednosti tijekom izvanrednih aktivnosti,
- prevenciju aktivnosti koje nisu u skladu s filozofijom organizacije,
- uspostavljanje praga za pokretanje hitnog odgovora,
- određivanje ovlasti za vrijeme diskontinuiteta poslovanja,
- i koordinaciju zadataka oporavka. [20]

2.2.2. Vrste planova i temeljne faze planiranja

Testiranje, ažuriranje i održavanje plana kontinuiteta poslovanja nije definirano u smislu učestalosti tih aktivnosti. U nekim organizacijama aktivnosti se vrše svakodnevno ili jednom tjedno, dok u drugima jednom mjesečno ili čak i rjeđe, što ovisi o veličini organizacije, kompleksnosti njenog poslovanja i djelatnosti kojom se bavi. Također, o tome ovisi i oblik te obuhvat plana kontinuiteta poslovanja. Općenito, univerzalno prihvaćene definicije za plan kontinuiteta i povezana područja planiranja nisu bila dostupna, te je to dovelo često do zabune i preklapanja u pogledu stvarnog opsega i svrhe različitih vrsta planova. U tablici niže su prikazane vrste planova zajedno sa svojom svrhom i opsegom.

[20] Fulmer, K.R. i Rothstein, P.J. (2004) Business Continuity Planning: A Step-by-Step Guide with Planning Forms

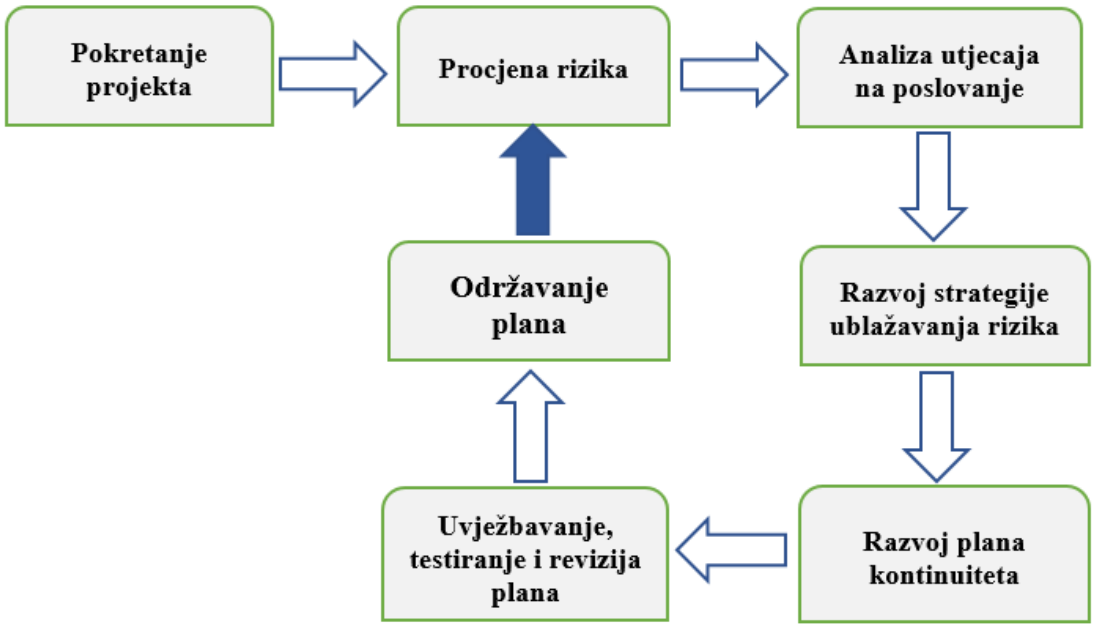
Tablica 1. Vrste planova unutar procesa upravljanja kontinuitetom poslovanja

PLAN	SVRHA	OPSEG
Plan poslovnog kontinuiteta (*engl. Business Continuity Plan – BCP*)	Osigurati procedure za održavanje ključnih poslovnih operacija u vrijeme oporavka sustava od značajnih poremećaja.	Poslovni procesi i IT podršku za poslovne procese
Plan oporavka poslovanja (*engl. Business Recovery Plan -BRP*)	Osigurati postupke i procese za brzi oporavak poslovnih operacija odmah nakon nastanka katastrofe. Ne osigurava kontinuitet procesa.	Poslovni procesi i IT podršku za poslovne procese
Plan oporavka od katastrofe (*engl. Disaster Recovery Plan - DRP*)	Osigurati detaljne procedure za obnovu podataka i uspostavu obrade na alternativnoj lokaciji ili sustavu.	Fokusiran na IT procese (sustave, aplikacije)
Plan operativnog kontinuiteta (*engl. Continuity of Operations Plan - COOP*)	Uspostaviti procedure i uvjete za održavanje temeljnih strategijskih funkcija na alternativnoj lokaciju do 30 dana.	Najkritičniji procesi na nivou sjedišta organizacije; često ne uključuje IT procese
Plan odgovora na incidente (*engl. Incident Response Plan - IRP*)	Definirati strategije za otkrivanje, odgovor i ograničavanje posljedica štetnih sigurnosnih incidenata.	Odnosi se na sigurnost informacijskih sustava i mreže
Plan za hitne slučajeve (engl. *Occupant Emergency Plan - OEP*)	Omogućiti koordinaciju postupaka za minimiziranje ljudskih gubitaka i ozljeda, te zaštitu štete nad imovinom	Odnosi se na osoblje i imovinu unutar određenog objekta; nije fokusiran na poslovne procese i IT sustav

Izvor: Fulmer, K.R. i Rothstein, P.J. (2004) Business Continuity Planning: A Step-by-Step Guide with Planning Forms

Stvaranje plana za kontinuitet poslovanja je vrlo slično svakom projektnom planiranju, no jednom kada se plan napravi, potrebno je održavati ga i prilagođavati stalnim promjenama u okruženju s kojima se organizacija susreće.

Slika 6. Koraci u planiranju poslovnog kontinuiteta



Izvor: Snedaker, S. (2007) Business Continuity & Disaster Recovery for IT Professionals

Osnovni koraci svakog plana kontinuiteta poslovanja su prikazani poviše.

Pokretanje projekta jedan je od najvažnijih elemenata u planiranju BC-a. Cjelokupna organizacija od najviše razine, njenog rukovodstva, do najnižih operativnih odjela, treba pružiti punu potporu u inicijalizaciji plana zbog postojanja mnogih ograničenja. Potpuna podrška je ključ uspjeha u pokretanju projekta. *Procjena rizika* odnosi se na proces pregledavanja i analize svih potencijalnih rizika kojima je poslovanje izloženo zajedno s njenim ključnim članovima organizacije. Ti rizici se mogu odnositi od uobičajenih do izvanrednih – od gubitka struje, požara do katastrofalnog gubitka poput zemljotresa. *Analiza utjecaja na poslovanje* podrazumijeva aktivnosti kojima se ocjenjuje utjecaj različitih rizika koje smo predvidjeli i procijenili u

prethodnom koraku. Ovaj korak je temelj za kreiranje strategije izbjegavanja ili ublažavanja rizika. *Razvoj strategije ublažavanja rizika* bavi se pitanjima kako tolerirati, smanjiti, izbjeći ili prenijeti rizik i njegov utjecaj na organizaciju. To je zadnji korak koji se tiče aktivnosti upravljanja rizikom. *Razvoj plana kontinuiteta poslovanja* može započeti kada se dovrše procjene, analize i strategije upravljanja rizicima. U ovom koraku se opisuju metode i procedure poslovnog kontinuiteta, uključujući standardne procese poput razvijanja poslovnih i tehničkih zahtjeva, definiranja opsega plana, proračuna, vremenskih rokova, metrika kvalitete i slično. *Uvježbavanje, testiranje i revizija plana* slijedi nakon što se napravi BC plan. Ovaj korak se odnosi na osposobljavanje zaposlenika za provođenje plana kroz različite vježbe i simulacije, te revidiranje plana i pronalaženje područja za modifikaciju i unaprjeđenje. *Održavanje plana* je posljednji korak u procesu planiranja BC-a i tiče se konstantnog praćenja promjena i shodno tome ažuriranja i dopunjavanja plana čineći plan kontinuirano relevantnim.[21]

2.3. Oporavak od katastrofe

Prema rječniku Merriam Webster katastrofa se definira kao „iznenadni štetni događaj koji donosi veliku štetu, gubitak ili uništenje; iznenadna ili velika nesreća ili neuspjeh“. U suvremenom informatičkom kontekstu, katastrofa je događaj koji uzrokuje prekid rada računalne okoline više od nekoliko minuta, često i nekoliko sati, dana ili čak godina. Katastrofa može izbrisati uobičajeni radni dan tvrtke ili pak dogoditi čitavu IT infrastrukturu. Iako se ne razlikuje od drugih vrsta kvarova, kvar informatičke infrastrukture tvrtke širi se na veće područje i utječe na više komponenti. Danas više nije uopće pitanje hoće li doći do katastrofe: hoće. Pitanje je jedino: kada. Stoga je uspostavljanje pouzdanog sustava za oporavak od katastrofe presudno za osiguravanje organizaciji da preživi značajne događaje.[22]

2.3.1. Definicija oporavka od katastrofe

Oporavak od katastrofe dio je kontinuiteta poslovanja i bavi se neposrednim utjecajem nakon nastanka neželjenog događaja. U ovu kategoriju spadaju svi ispadi od prekida poslužitelja,

[21] Snedaker, S. (2007) *Business Continuity & Disaster Recovery for IT Professionals.* Burlington, MA: Syngress Publishing.
[22] Omar, A., Alijani, D. i Roosevelt, M. (2011) Information Technology Disaster Recovery Plan: Case Study. *Academy of Strategic Management Journal*, 10 (2), str. 127-142

sigurnosnih napada do prirodnih katastrofa poput uragana. Obnova od katastrofe obično ima nekoliko diskretnih koraka u fazama planiranja. No, kako situacija nakon krize gotovo nikad ne ide očekivanim tokom, tako se ti koraci često miješaju i gubi se njihova distinkcija. Ključna zadaća oporavka od katastrofe jest zaustaviti njene učinke i što je brže moguće riješiti neposredne posljedice.[23]

Definira se i kao dokumentirani proces kojim se određuje kako organizacija treba djelovati u iznenadnim, neplaniranim katastrofalnim događajima koji ju sprječavaju da nastavi svoje kritične procese.[24]

Pojam oporavka od katastrofe se razlikuje od pojma visoke raspoloživosti. Oba su pojma vezana za kontinuitet poslovanja, no odnose se na različite slučajeve. Visoka raspoloživost podrazumijeva neprekidnost operacija odnosno ima nultu toleranciju na prekide rada. S druge strane, oporavak od katastrofe uključuje i djelomične prekida rada, koji mogu varirati od nekoliko sekundi do čak nekoliko dana ukoliko IT infrastruktura nije esencijalna za normalno funkcioniranje poslovanja.[25]

Plan oporavka od katastrofe (engl. *Disaster Recovery Plan - DRP)* definira se kao poslovni plan koji opisuje načine kako poslovne operacije mogu brzo i efikasno nastaviti svoj rad. [26]

Stvaranje postupaka za oporavak u slučaju katastrofe velik je izazov za svaku organizaciju. Učinkovitost stvorenog okvira i procedura moguće je provjeriti simuliranim scenarijima, ali se stvarno funkcioniranje može vidjeti tek nakon što nastane katastrofa. Plan oporavka od katastrofe sastoji se od procesa, politika i postupaka koji se odnose na obnovu kritičnih tehnologija.

---

[23] Snedaker, S. (2007) *Business Continuity & Disaster Recovery for IT Professionals.* Burlington, MA: Syngress Publishing.

[24] Partio, A. (2017) *Data center Disaster Recovery & Major Incident Management.* Master's Thesis in Information and Communications Technology. Lahti: University of Applied Sciences.

[25] Valenčić, D., Ćavar, I. i Lebinac, V. (2012) Provedba oporavka od katastrofe u računalstvu u oblaku. *Zbornik radova 5. Međunarodne konferencije: Dani kriznog upravljanja. 24-25 svibnja 2012, Velika Gorica, Hrvatska*. Veleučilište Velika Gorica, str. 674-692

[26] *Disaster Recovery Plan (DRP)* [online]. Techopedia.com. Dostupno na: https://www.techopedia.com/definition/1074/disaster-recovery-plan-drp

Kvalitetan plan oporavka od katastrofe trebao bi imati jasno utvrđene mjere i kontrolne mehanizme za prevenciju neželjenih događaja, ili u slučaju pojave istih, za njihovo efikasno uklanjanje.[27]

„Informatičke kontrole su kontrole ugrađene u rad informacijskog sustava koje predstavljaju skup međusobnih integrirajućih komponenti, koje, djelujući jedinstveno i usklađeno, potpomažu ostvarivanju ciljeva informacijskog sustava. Kontrole se usmjeravaju na neželjene događaje ili procese u informacijskom sustavu koji mogu nastati odnosno biti aktivirani iz različitih razloga koji se odnose na unutarnje djelovanje informacijskog sustava ili uzroke iz okruženja.“ [28]

Svaki plan za prevladavanje nesreća trebao bi sadržavati tri različita skupa mjera koje se provode u obliku kontrola: preventivne kontrole, detektivne kontrole i korektivne kontrole. Nužno je da su sve kontrolne mjere dokumentirane u planu i testirane kroz simulacijske testove kako bi se utvrdila njihova učinkovitost.

[27] Tijan, E., Kos., S. i Ogrizović, D. (2009) Disaster recovery and business continuity in port community systems. *Pomorstvo*, 23 (1), str. 243-260

[28] Spremić, M. (2017) *Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije*. Zagreb: Ekonomski fakultet.

Tablica 2. Vrste kontrolnih mjera

Preventivne kontrole	Nazivaju se još i prethodne ili procesne kontrole. Svrha im je otkriti probleme ili neželjene događaje prije njihovog nastanka tj. predvidjeti ih i spriječiti njihovu pojavu. Primjeri preventivnih kontrola su zapošljavanje educirane i kvalificirane radne snage, organiziranje ovlaštenih organa za nadzor rada sustava unutar organizacije, ustroj odjela za unutarnju reviziju informacijsko sustava, podizanje razine svijesti o nužnosti zaštitnih mjera, logičke i fizičke kontrole pristupa sustavu, donošenje pravilnika o sigurnosnoj politici i slično.
Detektivne kontrole	Kontrole koje otkrivaju razne propuste, probleme ili neželjene događaje. Primjeri detektivnih kontrola su kontrole unosa podataka, autorizacijske kontrole, fizičke i logičke kontrole pristupa, nadzor mrežnog prometa i općenito informacijskog sustava, procedure izdvajanja sumnjivih zapisa rada sustava , provjere ovlaštenja itd.
Korektivne kontrole	Kontrole čiji je zadatak umanjiti učinke neželjenih događaja. Korektivne kontrole su zadužene za utvrđivanje uzrok nastanka problema i izvođenje potrebnih akcija za rješavanje uočenih problema. Primjeri ovih kontrola su procedure za kopiranje i arhiviranje važnih podataka, procedure ponovnog uspostavljanja rada sustava, kontrole prijenosa podataka i sl.

Izvor: Spremić, M. (2017) *Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije*

2.3.2. Vrste katastrofa u poslovanju

Katastrofe se mogu pojaviti u bilo kojem trenutku iz više razloga. Plan kontinuiteta poslovanja (BCP) bi trebao biti pripremljen i spreman za sprečavanje ili smanjenje posljedica katastrofa. Prema The Disaster Recovery Institute International (www.drii.org), 93% tvrtki koje su iskusile neku vrstu katastrofe, bez da su imale plan oporavka, zatvorile su se u roku od pet godina. Također, 50% tvrtki koje dožive prekide kritičnih poslovnih funkcija duže od 10 dana nikada se potpuno ne oporave. Posebice je zanimljiv podatak za tvrtke koje pripadaju Fortune 500. Zastoji poslovnih operacija i poslovnog sustava u prosjeku ih košta 96.000 USD po minuti.

Katastrofe s kojima se organizacije suočavaju obično se svrstavaju u tri osnovne kategorije.

1. *Elementarne nepogode* - Kada se spomenu katastrofalni događaji koji imaju nepoželjne učinke na poduzeće, prvo napamet najčešće padaju prirodne katastrofe. Pojave i jačina pojedinih

prirodnih katastrofa poput oluja, snijega, uragana ili pak jakih kiša mogu se predvidjeti i približno procijeniti. Bez obzira na to, posljedica može biti kompletna devastacija pogođenog područja kao u slučaju uragana Katrina. Uragan je bio predviđen ali ujedno i grubo podcijenjen što je rezultiralo velikom katastrofom. S druge strane, neke opasnosti kao što su potresi, požari, vulkanske erupcije i klizišta imaju nepredvidivu narav i time predstavljaju potencijalno puno veću prijetnju. [29]

Slika 7. Vrste prirodnih katastrofa

OPASNOSTI I KATASTROFE POVEZANE S HLADNIM VREMENOM	OPASNOSTI I KATASTROFE POVEZANE S TOPLIM VREMENOM	GEOLOŠKE OPASNOSTI I KATASTROFE
Lavina	Obilna i dugotrajna kiša	Potresi
	Poplave	
Jak snijeg	Suša	Tsunami
	Požari	
Ledena oluja	Tropske oluje	Vulkanske erupcije
	Uragani, pijavice, tajfuni	
Jak vjetar	Tornado	Klizišta
	Olujni vjetar	

Izvor: Snedaker, S. (2007) Business Continuity & Disaster Recovery for IT Professionals

2. Katastrofe uzrokovane ljudskim faktorom - Osim prirodnih katastrofa, velik udio u sveukupnim katastrofama čine one uzrokovane ljudskim nemarom i pogreškama. Terorizam, bombardiranje, cyber napadi, krađe i otmice, otpuštanja opasnih tvari i mnogi drugi primjeri katastrofa izravna su posljedica ljudskog djelovanja. Nazivaju se još i antropogenim katastrofama. Za većinu katastrofa uzrokovanih ljudskom aktivnosti može se reći da su namjerno *izazvane,* dok se samo pojedine mogu pripisati slučajnosti i nenamjernim greškama. S obzirom da ih nije lako kategorizirati, nabrojat ću neke od njih:

- teroristički napadi – bombaški napadi, prijetnje bombama i eksplozivnim materijalima, oružani napadi, otpuštanje toksičnog materijala, kibernetičko ratovanje, biološki napadi, napadi na infrastrukturu i napadi na transportna sredstva;
- eksplozije;
- požari - namjerno i slučajno izazvani;

[29] Snedaker, S. (2007) *Business Continuity & Disaster Recovery for IT Professionals.* Burlington, MA: Syngress Publishing.

- cyber napadi – prijetnje, manji upadi u sustave, veliki proboji sustava, totalni prekidi rada, krađa podataka i napad na širu mrežnu infrastrukturu;
- građanski nemiri i neredi;
- radioaktivno onečišćenje;
- i krađe, otmice, pronevjere i iznuđivanje.[30]

3. *Nesreće i tehnološke katastrofe* – Često su izazvane ljudskim faktorom, no razlika od prethodno nabrojanih katastrofa jest namjera. Katastrofe koje spadaju u ovu kategoriju nisu namjerno uzrokovane, već su posljedica nedovoljnog ili nepažljivog održavanja, nepostojanja regulacija, previda u planiranju i izvršavanju procesa ili jednostavno vanjskog faktora na koje se teško može utjecati. Neke od njih su:

- prometne nesreće - nesreće na cestama, kolapsi ili nesreće u zračnim lukama, pomorske i željezničke nesreće;
- infrastrukturne nesreće i kvarovi;
- nesreće povezane s električnom energijom – prekid napajanja, isključenja struje, kvarovi na infrastrukturi;
- pad i nedostupnost informacijske i komunikacijske infrastrukture;
- incidenti u elektranama (termo, hidro, vjetro i solarne);
- urušavanja građevinskih objekata;
- i razni manji materijalni incidenti.[31]

2.3.3. Planiranje oporavka od katastrofe

Planiranje oporavka od katastrofe je tradicionalno imalo fokus na računalne sustave i infrastrukturu. Međutim, oporavak poslovnih operacija uključuje više od samo računalnog sustava. Danas je više nego ikad potrebno razmotriti pitanja poput pružanja usluga s drugih lokacija i udaljenih lokacija, sigurnih ranih lokacija za zaposlenike, kao i spašavanja ili zamjene

[30] Snedaker, S. (2007) *Business Continuity & Disaster Recovery for IT Professionals.* Burlington, MA: Syngress Publishing.
[31] Snedaker, S. (2007) *Business Continuity & Disaster Recovery for IT Professionals.* Burlington, MA: Syngress Publishing.

građevinskih sadržaja. Budući da kritične funkcije obično ovise o tehnologiji i telekomunikacijskim mrežama, brzi oporavak istih je vrlo važan, ali je od male vrijednosti bez obnavljanja poslovnih operacija širom poduzeća.

Za kreiranje uspješne strategije i plana kontinuiteta poslovanja nužno je slijediti ove ključne korake:

- Prije katastrofe, identificirati sve računalne sustave, aplikacije, ljude, opremu i zalihe potrebne za oporavak.
- Imati sigurnosnu kopiju za kritične datoteke i sustave i sigurnu pohranu izvan mjesta.
- Imati jedno ili više zamjenskih mjesta za obradu podataka i poslovne operacije.
- Biti u stanju održavati učinkovitu kontrolu nad naporima oporavka.
- Identificirati vanjske resurse koji mogu pomoći u procesu oporavka.
- Testirati plan kako bi se napravila procjena sposobnosti pružanja potrebne razine podrške osnovnom poslovnom procesu i konačnom oporavku.
- Održavati i ažurirati plan. Možda je i gore ovisiti o zastarjelom planu nego ga uopće ne imati.[32]

Osnove koje svaki DR plan treba osigurati u slučaju katastrofalnog događaja jesu:

1. *Zamjenska lokacija tvrtke* - U slučaju nastanka događaja koji bi spriječio pristup objektima organizacije, oštetio ih ili potpuno uništio, organizacija mora imati alternativnu lokaciju koja je funkcionalna i lako upotrebljiva za nastavak poslovanja.
2. *Pristup vitalnim podacima i resursima za vrijeme oporavka* - Svi zapisi i podaci potrebni za vraćanje kritičnih funkcija i uspostavljanje rada trebaju biti spremljeni izvan web mjesta (engl. off-site).
3. *Ključni ljudi sa zadaćama i ulogama u oporavku* - Proces oporavka zahtijeva dobro koordinirano i uvježbano osoblje tvrtke zajedno sa vanjskim dobavljačima i drugim stakeholderima.

[32] Fulmer, K. L. (2005) *Business Continuity Planning: A Step-by-Step Guide with Planning Forms, Third Edition*. Brookfield, CT: Rothstein Associates Inc.

4. *Plan za brzi oporavak* - Pouzdan i ažuran plan će zasigurno smanjiti vrijeme oporavka. Ako se dogodi katastrofa većih razmjera, tada sve informacije vezane za poslovne operacije, spremni timovi i postupci za oporavak dobivaju kritičnu funkciju.[33]

[33] Wallace, M. i Webber, L. (2004) *The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities and Assets*. New York, NY: AMACOM

3. UPRAVLJANJE RIZICIMA I UTJECAJ NA POSLOVANJE

„Upravljanje rizicima treba biti ključna stavka svake poslovne odluke.“

Upravljanje kontinuitetom poslovanja usko je povezano s upravljanjem rizicima. Štoviše, u mnogim organizacijama BCM je dio funkcije upravljanja rizikom. To se posebno odnosi na financijske organizacije u kojima je upravljanje rizikom ključna funkcija i ima veliku značajnost u korporativnom programu, te je najčešće i zastupljeno na razini upravnog odbora. [34]

3.1. Pojam i obilježja informatičkih rizika

„Rizik predstavlja opasnost ili vjerojatnost da će odgovarajući izvor prijetnje u određenim okolnostima iskoristiti ranjivost sustava, čime se, posljedično, može počiniti neka šteta imovini organizacije.“ [35]

Rizik se može definirati i kao mjera opsega koja prijeti određenom entitetu potencijalnim okolnostima ili događajima. Uobičajeno je funkcija:

1. Vjerojatnosti pojave neželjenih događaja
2. Štetnosti učinaka u slučaju pojave neželjenih događaja. [36]

Rizik za organizaciju ne predstavlja prijetnju ukoliko ne postoji određena ranjivost koja se može iskoristiti. Za potrebe ovog rada objasnit ću razliku i povezanost između pojmova prijetnje, ranjivosti i rizika.

Prijetnja je mogućnost nastanka neželjenog događaja. Definira se i kao: „*Mogućnost ili namjera neke osobe da poduzme akcije koje nisu u skladu s ciljevima organizacije*.“ Izvori prijetnje su:

- prirodni (prirodne katastrofe poput požara, potresa, poplava i sl.)
- ljudske pogreške i čimbenici unutar organizacije

[34] Gallagher, M. (2003) *Business Continuity Management: How to Protect Your Company from Danger*. Harlow: Pearson Education Limited.

[35] Spremić, M. (2017) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet.

[36] NIST Special Publication 800-12, Revision 1 (2017) *An Introduction to Information Security*. Gaithersburg, Maryland: National Institute of Standards and Technology. [online]. Dostupno na: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

- slučajan događaj ili nenamjerne aktivnosti
- namjerno počinjenje štete ili ugroza rada informacijskog sustava
- čimbenici van sustava organizacije.“[37]

Ranjivost sustava predstavlja slabost sustava koju prijetnja može iskoristiti i napraviti štetu organizaciji. Definira se kao nedostatak ili slabost u sigurnosnim postupcima sustava, dizajnu, implementaciji ili internim kontrolama. Da bi se utvrdila vjerojatnost prijetnje, potrebno je uzeti u obzir izvore prijetnji, potencijalne ranjivosti i postojeće kontrole. Analiza ranjivosti povezanih s okruženjem sustava namijenjena je izradi popisa ranjivosti sustava (nedostataka ili slabosti) koje bi potencijalni izvori prijetnji mogli iskoristiti. Takve prijetnje mogu uključivati ljude, procese, sustave ili vanjska događanja.[38]

„Informatički rizici su poslovni rizici koji proizlaze iz intenzivne uporabe informacijskih sustava i tehnologije u okruženju digitalne ekonomije kao važne podrške odvijanju i unaprjeđenju poslovnih procesa i poslovanja uopće. Ti se odnose na opasnosti i prijetnje da intenzivna primjena informacijskih tehnologija može uzrokovati neželjene i neočekivane posljedice i možebitne financijske i druge štete unutar organizacije i njenog okruženja. Informatički rizici se mogu predočiti funkcijom koja predstavlja međudjelovanje varijabla poput imovine organizacije (materijalna, financijska), prijetnji (incidenti, neželjeni događaji i ranjivosti (slabost sustava, koja predstavlja razinu implementiranih kontrola čiji je cilj spriječiti pojavu neželjenih događaja).“[39]

RIZIK = f (imovina, prijetnja, ranjivost)

[37] Spremić, M. (2017) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet.
[38] Ransome, J. F. i Rittinghouse, J. W. (2005) *Business Continuity and Disaster Recovery for InfoSec Managers*. Burlington, MA: Elsevier Digital Press.
[39] Varga, M., Strugar, I., Pejić Bach, M., Srića, V., Spremić, M., Bosilj Vukšić, V., Ćurko, K., Vlahović, N., Milanović Glavan, Lj., Zoroja, J. i Jaković B. (2016) Informacijski sustavi u poslovanju. Zagreb: Ekonomski fakultet

Dva osnovna obilježja informatičkih rizika su:

- težina – mjera veličine štete koju može određena aktivnost izazvati, a uobičajeno se može procijeniti i prikazati u financijskom smislu
- učestalost pojave – procijenjeni broj poduzimanja aktivnosti u jedinici vremena koje štete mogu izazvati.[40]

Ovisno o uzroku odnosno izvoru, rizici mogu biti objektivni i subjektivni.

Tablica 3. Izvori rizika

Objektivni rizici	Subjektivni rizici
➢ proizlaze iz naravi i zakonitosti funkcioniranja sustava u kojemu se primjenjuje informacija tehnologija	➢ nastaju namjerom pojedinaca ili skupina, ili pak onda kada se u sustavu ne poduzimaju raspoložive mjere zaštite (prevencije) od objektivnih rizika
➢ teško je boriti se i štititi od njih, te ih nije moguće u potpunosti izbjeći	➢ mogu se u potpunosti izbjeći poduzimanjem odgovarajućih zaštitnih mjera u sustavu

Izvor: Panian, Ž. i Strugar, I. (2013) Informatizacija poslovanja

Rizici se obično kategoriziraju prema području unutar organizacije:

❖ „*Strateški (korporativni) informatički rizici* – rizici na najvišoj razini upravljanja koji se odnose na neusklađenost poslovanja i informatike odnosno sve one rizike kojima se ugrožavaju strateški poslovni interesi radi pogrešnih odluka ili ne donošenja odluka koje

[40] Varga, M., Strugar, I., Pejić Bach, M., Srića, V., Spremić, M., Bosilj Vukšić, V., Ćurko, K., Vlahović, N., Milanović Glavan, Lj., Zoroja, J. i Jaković B.

se vezane za pozitivne učinke primjene digitalne i informacijske tehnologije u inovaciji poslovnog modela i ostvarenju poslovnih ciljeva.

- *Rizici provedbe informatičkih programa i projekata* – odnose se na rizike da investicije u informacijske tehnologije neće biti ispravno upravljanje, kao i rizici da provedba tih investicija kroz informatičke programe i projekte neće biti učinkovite ili neće doprinijeti stvaranju nove vrijednosti.
- *Rizici provedbe poslovnih procesa (operativni ili transakcijski rizici)* – rizici primjene informacijske tehnologije u redovitom poslovanju. U ovu kategoriju spadaju svi informatički rizici koji imaju utjecaj na načine izvedbe poslovnih procesa.
- *Infrastrukturni informatički rizici* – rizici rada informatičke infrastrukture i opreme te svi ostali rizici koji se odnose na redovito funkcioniranje informatičke infrastrukture. Preciznije, odnose se na dostupnost i funkcionalnost računalne mreže, infrastrukturne podrške podatkovne osnovice, komunikacijske infrastrukture, servisa elektroničke pošte i svih ostalih informatičkih servisa koje kompanija pruža.“ [41]

3.2. Koncept upravljanja rizicima organizacije

Sposobnost organizacije, a i svakog menadžera, da učinkovito i djelotvorno upravlja raznim vrstama rizika u svakodnevnim operacijama vrlo je važan čimbenik poslovanja. Upravljanje rizicima ne bi smjelo biti dodatna funkcija upravljanju, već njen sastavni dio.

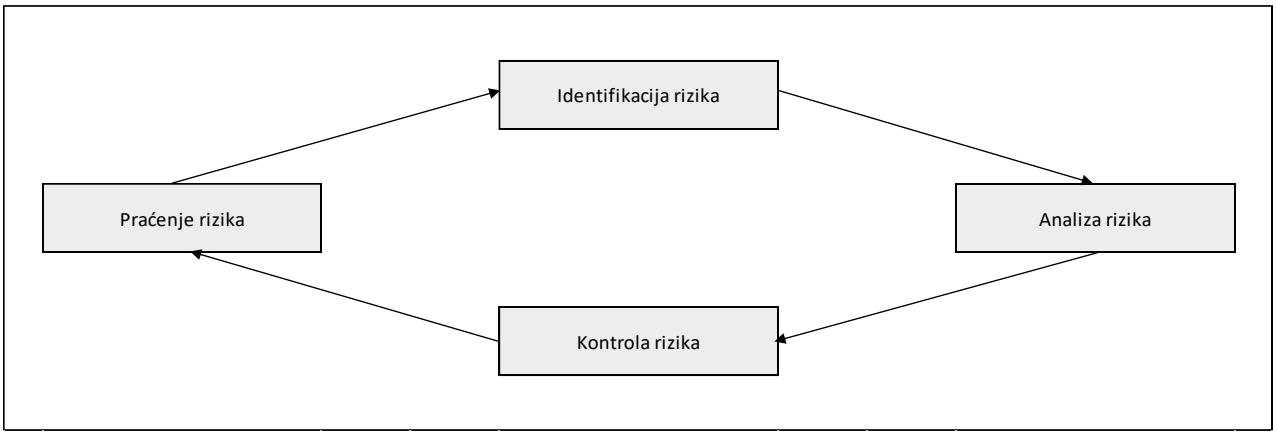
„Upravljanje rizicima predstavlja sistematičan analitički proces kojima organizacija otkriva, prepoznaje, umanjuje i nadzire potencijalne rizike kojima je izložena.“ [42] Osnovna svrha upravljanja rizikom jest analizirati sustav i identificirati slabosti u sustavu organizacije, procijeniti razinu opasnosti kojom su izloženi organizacijski resursi, predložiti učinkovit način smanjivanja intenziteta rizika i stalno ih nadzirati. Ovaj proces omogućuje organizacijama određivanje veličine i efekte potencijalnih gubitaka, vjerojatnosti i frekvencije pojave tih gubitaka te uspostavljanje potrebnih protumjera. Prema ovome, cilj upravljanja rizikom bio bi

[41] Spremić, M. (2017) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet.
[42] Panian, Ž., Spremić, M. i suradnici (2007) Korporativno upravljanje i revizija informacijskih sustava. Zagreb: Zgombić i partneri.

smanjiti vjerojatnost pojave i učestalost pojave neželjenog događaja, te ublažiti ozbiljnost jednom kada se dogodi.

„Osnovni zadatak procesa upravljanja rizicima jest sustavnim metodama i mjerama održavati poželjnu razinu sigurnosti poslovanja odnosno održavati prihvatljivim razine rizika kojima je izloženo poslovanje organizacije. Prihvatljiva razina rizika podrazumijeva intenzitet rizika koji još uvijek nije ugroza za poslovanje i funkcioniranje poslovnih procesa i samim time za ostvarenje ciljeva organizacija.“ [43]

Slika 8. Ciklus upravljanja rizicima



Izvor: Gallagher, M. (2002) Business Continuity Management: How to Protect Your Company from Danger

Rizici se trebaju sistematski identificirati, analizirati, kontrolirati i pratiti kako bi se njima efektivno upravljalo. Taj proces, prikazan na slici poviše, naziva se ciklus upravljanja rizicima. [44]

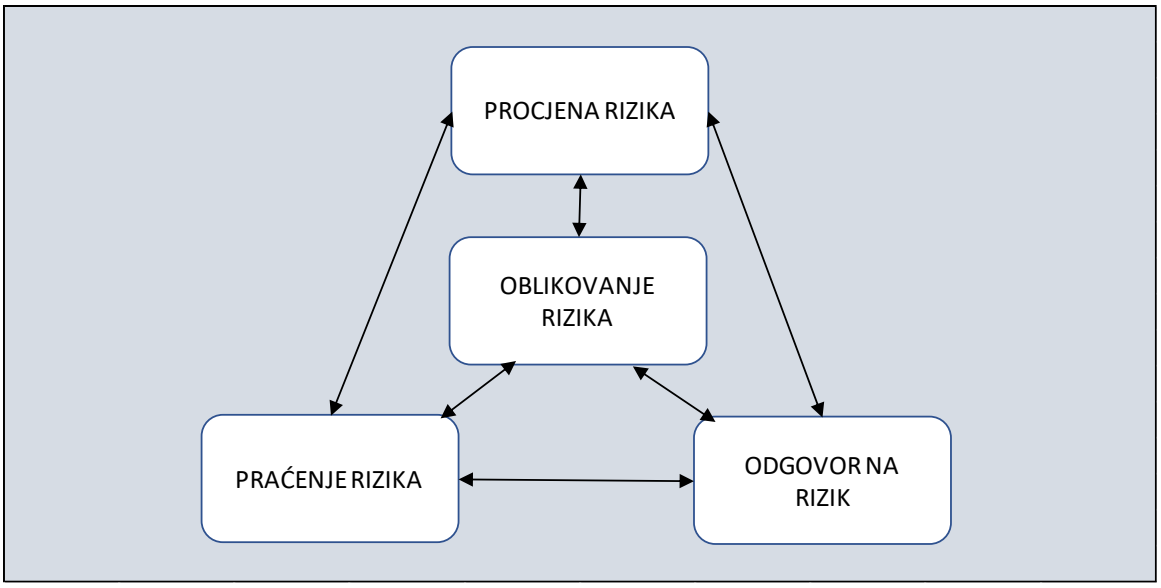
Nacionalni institut za standarde i tehnologiju (engl. *National Institute of Standards and Technology - NIST*) definirao je upravljanje rizikom kao složenu i sveobuhvatnu aktivnost koja zahtijeva sudjelovanje cijele organizacije: (i) od višeg rukovodstva koji pruža stratešku viziju i

[43] Spremić, M. (2017) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet.
[44] Gallagher, M. (2003) *Business Continuity Management: How to Protect Your Company from Danger*. Harlow: Pearson Education Limited.

ciljeve na najvišoj razini; (ii) menadžera srednje razine koji planiraju, izvršavaju i upravljaju projektima; (iii) do operativnih menadžera i pojedinaca na najnižim razinama koji upravljaju informacijskim sustavima i podržavaju poslovne funkcije organizacije. Slično ciklusu poviše, NIST je identificirao 4 temeljna koraka u procesu upravljanja rizikom: oblikovanje rizika, procjena rizika, odgovor na rizik i praćenje rizika.

Na slici 9. je ilustriran proces upravljanja rizicima i tok informacijskog i komunikacijskog procesa među različitim fazama upravljanja. Strelice se odnose na primaran tok upravljanja rizicima. Oblikovanje rizika je središnja faza jer se prema njoj određuju sve ostale aktivnosti.
Oblikovanje rizika - prvi korak opisuje kako organizacije uspostavljaju kontekst rizika odnosno govori o okruženju u kojem se donose odluke utemeljenje na riziku. Svrha oblikovanja rizika jest stvaranje strategije upravljanja rizicima koja se bavi načinom na koji organizacije namjeravaju procijeniti rizik, reagirati na rizik i zatim ga nadzirati. Ujedno oblikovanje okvira rizika uspostavlja izričito i transparentno poimanje rizika koje organizacija koristi u donošenju investicijskih i poslovnih odluka.

Slika 9. Proces upravljanja rizicima



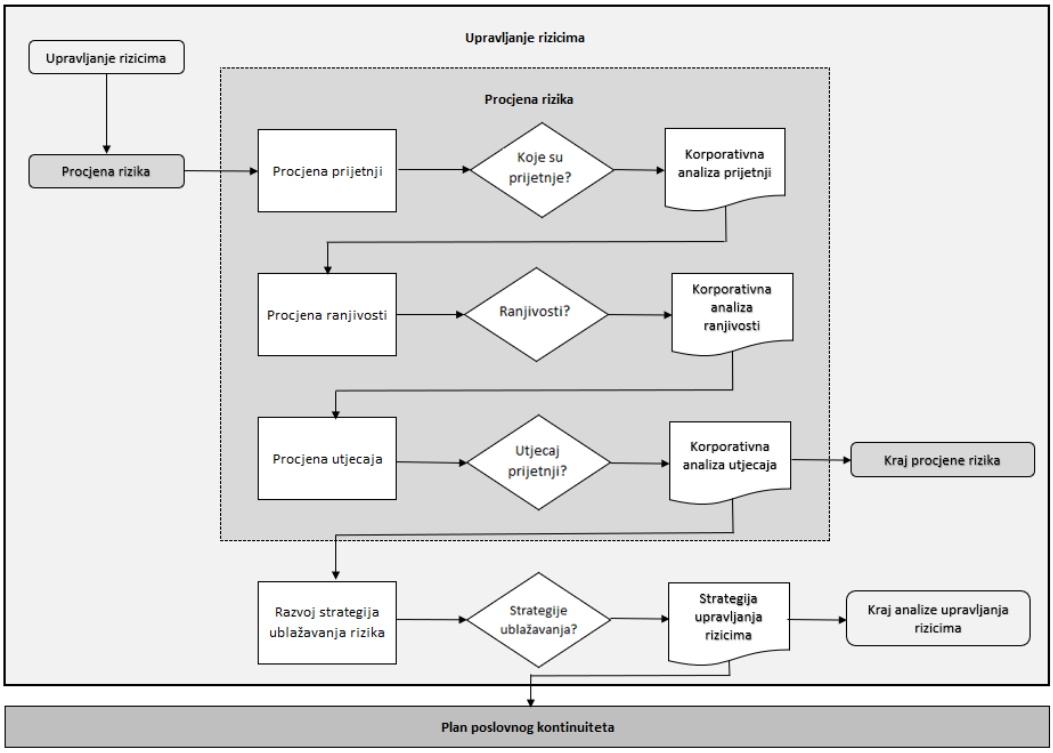
Izvor: NIST Special Publication 800-39 (2011) Managing Information Security Risk

Procjena rizika – druga faza bavi se načinom na koji organizacije ocjenjuju rizik unutar stvorenog okvira organizacijskog rizika. Svrha procjene rizika je određivanje: 1) prijetnji organizacijskoj imovini, operacijama ili osoblju te prijetnjama upućenim drugim organizacijama ili naciji; 2) internih i eksternih ranjivosti organizacije; 3) veličinu štete koja može nastati ukoliko se prijetnje ostvare i iskoriste organizacijske ranjivosti; i 4) vjerojatnosti pojave štetnog događaja. Krajnji rezultat ove faze jest utvrđivanje rizika (veličina štete i vjerojatnost pojave).
Odgovor na rizik - odnosi se na reagiranje organizacije na rizike nakon njegove procjene. Svrha ove faze jest pružanje dosljednog odgovora na rizik u cijeloj organizaciji koji je u skladu sa stvorenim okvirom rizika na način da se: 1) razviju alternative djelovanja za odgovor na rizik; 2) napravi procjena kreiranih alternativa; 3) odredi prikladan način djelovanja u skladu s tolerancijom organizacijskog rizika; i 4) provedu odgovori na rizik temeljem odabranih postupaka i procedura.
Praćenje rizika – zadnji korak opsuje na koje sve načine organizacija nadzire i prati rizik. Svrha praćenja rizika je: 1) provjeriti je li se provode planirane mjere reakcije na rizik i jesu li zahtjevi za informacijskom sigurnosti zadovoljeni i usklađeni s organizacijskom misijom, ciljevima, poslovnim funkcijama, zakonima, direktivama, politikama, propisima, standardima i smjernicama; 2) utvrditi trajnu učinkovitost mjera odgovora na rizik nakon što se provedu; 3) identificirati promjene koje utječu na rizik informacijskog sustava i okruženja. [45]

Slika 10. prikazuje dijagram procesa upravljanja rizikom kao dio upravljanja kontinuitetom poslovanja. Prema dijagramu postoje 4 osnovna koraka: procjena prijetnji, procjena ranjivosti, procjena utjecaja i razvoj strategije ublažavanja utjecaja. Kao što se vidi, svaka faza započinje s procjenom, a završava s analizom koja najčešće rezultira određenim izvješćem ili pisanim dokumentom, čime je omogućen uredan prelazak iz jedne faze u drugu.

[45] NIST Special Publication 800-39 (2011) *Managing Information Security Risk*. Gaithersburg, Maryland: National Institute of Standards and Technology. [online]. Dostupno na: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

Slika 10. Pregled procesa upravljanja rizicima



Izvor: Snedaker, S. (2007) Business Continuity & Disaster Recovery for IT Professionals

Proces upravljanja rizicima uglavnom odnosi na upravljanje unutarnjim rizicima i rizicima koji se direktno tiču organizacije. No, organizacija bi trebala također obratiti pažnju na utjecaj rizika na njene interesno utjecajne skupine poput kupaca, dobavljača, poslovnih partnera te dijeliti međusobno informacije o ranjivostima i prijetnjama. Time će osigurati višu razinu sigurnosti vlastitog poslovanja jer će se smanjiti vjerojatnost pojave štete koja se u jednoj ili više iteracija može prenijeti na samu organizaciju.

3.3. Procjenjivanje rizika

Jedna od ključnih analiza prilikom izrade plana kontinuiteta poslovanja jest i procjena rizika. Ona se mora provoditi na sustavan način, prema unaprijed definiranoj metodologiji. Cilj takvog sustavnog pristupa upravljanju rizicima jest uspostaviti jednoznačan mehanizam za nadzor i upravljanje rizicima u cijeloj organizaciji. Svi vlasnici rizika su odgovorni za provedbu procjene

i obradu rizika, u domeni svoje odgovornosti, definiranje prihvatljive razine rizika i održavanje rizika na prihvatljivoj razini.[46]

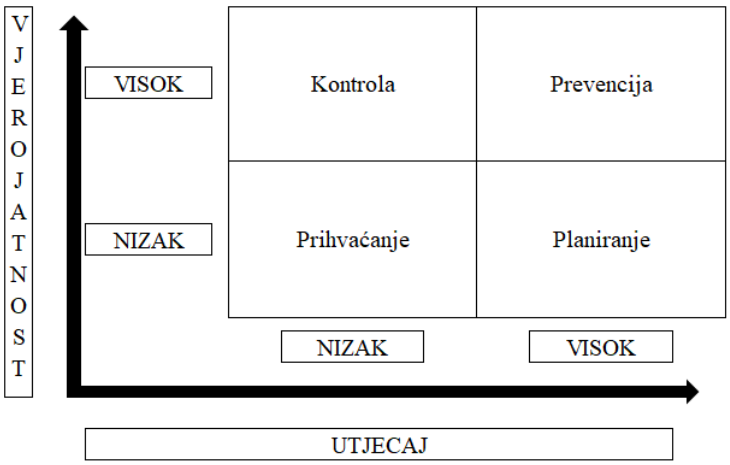
Procjena poslovanja se može podijeliti na dvije sastavnice, procjenu rizika i analizu utjecaja na poslovanje. Procjena rizika služi za vrednovanje izloženosti organizacije prijetnjama i rizicima prisutnim u okruženju, dok analiza utjecaja procjenjuje potencijalne gubitke koji mogu nastati ukoliko se prijetnje realiziraju.[47] Procjenom rizika definiraju se izvori potencijalnih opasnosti, procjenjuju vjerojatnosti pojave krizne situacije i moguće posljedice. Proces procjene rizika zahtjeva poznavanje organizacije, njezinog tržišta i okruženja u kojem posluje, razumijevanje operativnih i strateških ciljeva, te poznavanje opasnosti i prijetnji povezanih s tim ciljevima. [48]

Cilj procjene i kontrole rizika, u kontekstu upravljanja kontinuitetom poslovanja, jest utvrditi događaje koji mogu negativno utjecati na organizaciju, štetu koju takvi događaji mogu uzrokovati, vremenski raspon potreban za obnavljanje normalnog poslovanja i kontrole koje se mogu primijeniti za smanjenje vjerojatnosti utjecaja. U postizanju ovih ciljeva identificirano je pet faza:

- razumijevanje potencijala gubitaka i ranjivosti koje slijede,
- vrednovanje alata i tehnika za analizu rizika,
- definiranje strategije za procjenu rizika,
- odabir postupaka za procjenu rizika,
- i uspostavljanje mjera za prevenciju ili reduciranje utjecaja.

[46] Tomić Rotim, S. i Komnenić, V. (2017) Kako pripremiti sveobuhvatan plan kontinuiteta poslovanja? U: I. Nađ, ur. *Zbornik radova 10. Međunarodne znanstveno-stručne konferencije: Dani kriznog upravljanja. 24-26 studeni 2017, Terme Tuhelj, Hrvatska*. Velika Gorica: Veleučilište Velika Gorica, str. 475-489.
[47] Barnes, J. C. (2001) *A Guide to Business Continuity Planning*. Chichester: John Wiley & Sons, Ltd.
[48] Udovičić, A., Kadlec, Ž. (2013) Analiza rizika upravljanja poduzećem. *Praktični menadžment*, 4(1), str. 50-60

Slika 11. Matrica vrednovanja rizika



Izvor: Gallagher, M. (2002) Business Continuity Management: How to Protect Your Company from Danger

Matrica vrednovanja rizika prikazuje 4 osnovne kategorije rizika s obzirom na njihovu veličinu utjecaja i vjerojatnost pojave, te kontrolne mjere koje se poduzimaju za svaku kategoriju.

Prihvaćanje rizika – U slučaju niske vjerojatnosti pojave rizika sa slabim utjecajem na poslovanje rizik se prihvaća.

Kontrola rizika – Učestale rizike sa slabim utjecajem potrebno je konstantno pratiti, nadzirati i kontrolirati te uvesti mjere koje će zadržati njihov utjecaj na niskoj razini i dodatno smanjiti frekvenciju pojave.

Prevencija ili smanjivanje rizika – Rizici s velikim utjecajem i vjerojatnosti pojave mogu imati katastrofalne posljedice po poslovanje stoga organizacija treba provesti mjere sprječavanja nastanka takvih rizika, ublažiti njihov utjecaj ili ga transferirati na drugu organizaciju u vidu osiguranja.

Planiranje rizika – Odnosi se na rizike koji imaju malu vjerojatnost pojave, ali čiji utjecaj može biti velike negativne posljedice na organizaciju. Za ove rizike je potrebno imati stvorene procedure i postupke u planovima kontinuiteta poslovanja i oporavka od katastrofe.

Kao što je prikazano prethodno na dijagramu upravljanja rizikom, podproces procjena rizika započinje procjenom i analizom svih prijetnji. Rezultat ovog koraka predstavlja doprinos i ulaz u sljedeću fazu u kojoj se procjenjuju i analiziraju ranjivosti organizacije. Izvori podataka u procjeni ranjivosti su, osim prethodnih procjena prijetnji, regulatorni zahtjevi, zakonski i sigurnosni propisi. Nakon što se dovrši procjena ranjivosti, slijedi analiza ranjivosti i vrednovanje rizika koje se prikazuje numerički ili opisno ovisno o tome je li korišten kvantitativni ili kvalitativni sustav vrednovanja. Uobičajena jednadžba rizika koja se koristi u vrednovanju jest:

$$\text{RIZIK} = \text{prijetnja} + (\text{vjerojatnost} + \text{ranjivost}) + \text{utjecaj}$$ [49]

Slika 12. Prikaz zadnje faze u procjeni rizika



Izvor: Snedaker, S. (2007) Business Continuity & Disaster Recovery for IT Professionals

Rezultati odnosno outputi ove faze su vrijednosti rizika koji služe kao inputi za provođenje analize utjecaja rizika na poslovanje o čemu će biti riječ u nastavku.

3.4. Analiza utjecaja na poslovanje

Analiza utjecaja na poslovanje (engl. *Business Impact Analysis - BIA*) postupak je prepoznavanja kritičnih poslovnih funkcija, te negativnih učinaka ukoliko te funkcije nisu dostupne. Analiza uključuje i razgovore s ključnim osobama zaduženim za vođenje ključnih operacija kako bi se procijenio utjecaj neželjenih događaja na redovno poslovanje. [50] Svrha

[49] Snedaker, S. (2007) *Business Continuity & Disaster Recovery for IT Professionals.* Burlington, MA: Syngress Publishing.
[50] Ransome, J. F. i Rittinghouse, J. W. (2005) *Business Continuity and Disaster Recovery for InfoSec Managers*. Burlington, MA: Elsevier Digital Press.

analize utjecaja na poslovanje je povezati sustav kritičnih poslovnih procesa s uslugama koje se pružaju i temeljem tih podataka odrediti posljedice koje može uzrokovati poremećaj procesa. BIA sadrži tri osnovna koraka:

1. *Određivanje vitalnih poslovnih procesa i kritične razine oporavka* – Identificiraju se vitalni poslovni procesi i utjecaj poremećaja sustava na te procese zajedno s utjecajem nedostupnosti sustava. Prekid bi se trebao odnositi na maksimalno vrijeme koje organizacija tolerira, a da još uvijek postiže svoju misiju.
2. *Određivanje potreba za resursima* – Potrebno je napraviti temeljitu procjenu resursa nužnih za nastavak kritičnih poslovnih procesa. Primjeri tih resursa uključuju objekte, zaposlenike, opremu, softver, datoteke s podacima, komponente sustava i vitalne zapise.
3. *Određivanje prioriteta oporavka za resurse sustava* - Temeljem rezultata iz prethodnih koraka, resursi sustava mogu se jasnije povezati s vitalnim procesima. U ovom se koraku određuju razine prioriteta za resurse i slijed aktivnosti za oporavak. [51]

Osnovni zadatak analize je razumijevanje vitalnih procesa za poslovanje organizacije i razumijevanje utjecaja poremećaja na te procese. Analiza utjecaja na poslovanje se često miješa s pojmom obrađenim u prethodnom dijelu rada, procjenom rizika. Osnovna razlika između ova dva pojma se odnosi na perspektivu promatranja organizacije i njenog poslovanja. Procjena rizika razmatra različite prijetnje s kojima se suočava organizacija, dok BIA promatra kritične poslovne procese i učinke koji mogu nastati ukoliko te funkcije budu nedostupne. Odnosno, procjena rizika započinje sa strane prijetnje, dok BIA započinje sa strane poslovnog procesa. [52]

Središnja točka svake analize utjecaja na poslovanje su zahtjevi za oporavak sustava u slučaju prekida i nedostupnosti. Američki Nacionalni institut za standarde i tehnologiju (engl. *National Institute of Standards and Technology – NIST*) definira tri takva elementa objašnjena u tablici niže.

[51] NIST Special Publication 800-34, Revision 1 (2010) *Contigency Planning Guide for Federal Information Systems*. Gaithersburg, Maryland: National Institute of Standards and Technology. [online]. Dostupno na: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

[52] Snedaker, S. (2007) *Business Continuity & Disaster Recovery for IT Professionals.* Burlington, MA: Syngress Publishing.

Tablica 4. Tri osnovne stavke analize utjecaja na poslovanje

Maksimalno prihvatljivi prekid (engl. *Maximum Tolerable Downtime - MTD*)	Predstavlja ukupnu količinu vremena nedostupnosti vitalnih poslovnih procesa koju organizacija može prihvatiti. Veća kritičnost poslovnog procesa uobičajeno znači kraće prihvatljivo vrijeme nedostupnosti.
Ciljno vrijeme oporavka (engl. *Recovery Time Objective - RTO*)	Odnosi se na vrijeme potrebno za oporavak sustava i njegovih resursa. Najčešće je dio MTD-a i predstavlja najduže dopušteno vrijeme trajanja prekida sustava.
Ciljna točka oporavka (engl. *Recovery Point Objective - RPO*)	Predstavlja trenutak u vremenu prije nastanka prekida sustava do koje se mogu oporaviti podaci. Osnovni faktor RPO-a je odrediti prihvatljivu razinu gubitka podataka u slučaju prekida.

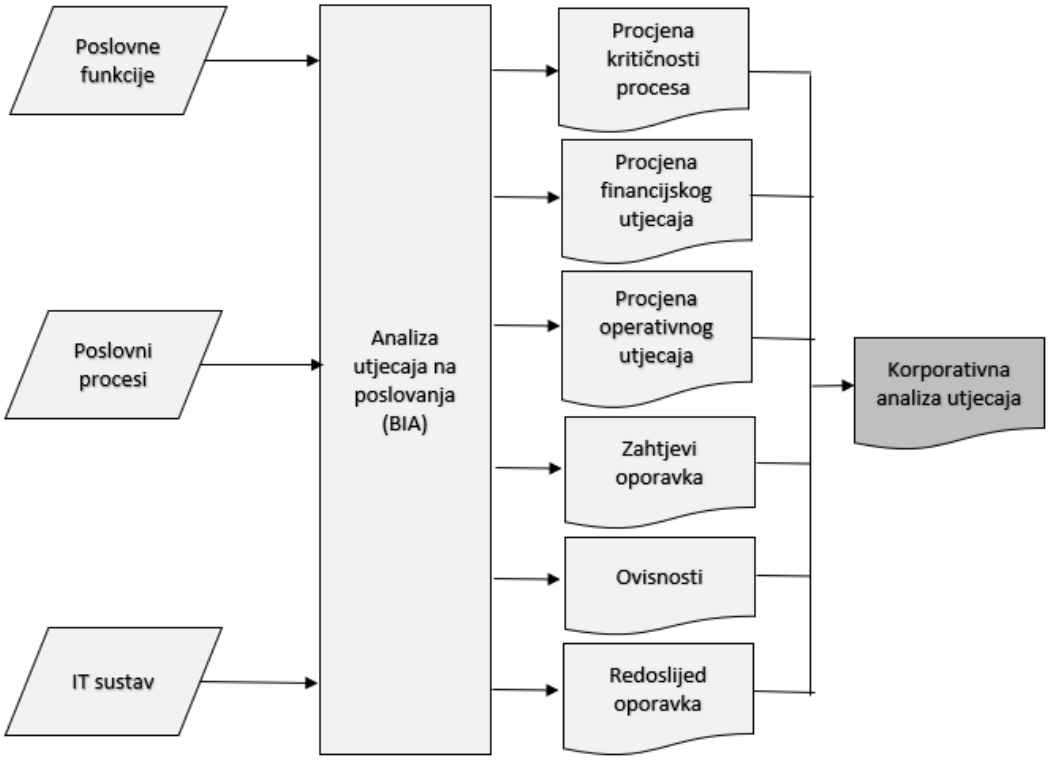
Izvor: NIST Special Publication 800-34, Revision 1 (2010) Contigency Planning Guide for Federal Information Systems

BIA pruža organizaciji:

- neovisan pogled na rizike iz katastrofalnih situacija,
- osnovu za utvrđivanje troškovno-učinkovite strategije,
- pregled kritičnih i potrebnih poslovnih procesa i povezanih resursa,
- prepoznavanje kritičnih dijelova sustava i toleranciju nedostupnosti i
- procjenu financijskih i operativnih učinaka poremećaja i potrebnog okvira za oporavak.[53]

[53] Barnes, J. C. (2001) *A Guide to Business Continuity Planning*. Chichester: John Wiley & Sons, Ltd.

Slika 13. BIA dijagram



Snedaker, S. (2007) Business Continuity & Disaster Recovery for IT Professionals

Na slici 13. je prikazan dijagram analize utjecaja na poslovanje. Prvo je potrebno identificirati poslovne funkcije, poslovne procese i aktivnosti te informacijske sustave koji ih podržavaju i prikupiti podatke. Nakon toga slijedi analiza koja uključuje procjenu kritičnosti procesa, procjenu financijskog i operativnog utjecaja, zatim vremenske zahtjeve oporavka, ovisnosti o resursima i redoslijed oporavka. Produkt ovih analiza je cjelovita korporativna analiza utjecaja na poslovanje koja služi organizaciji kao input u daljnjem procesu upravljanja kontinuitetom poslovanja.

3.5. Strategije reduciranja utjecaja rizika

Nakon što je organizacija identificirala i analizirala rizike, prijetnje i ranjivosti, te procijenila utjecaj na poslovne procese i poslovanje općenito, slijedi razvoj i uspostavljanje strategija i metoda za smanjivanje njihovog utjecaja.

Smanjivanje rizika je sustavna metodologija korištena od strane strateškog menadžmenta za njegovo ublažavanje kroz sljedeće opcije:

Preuzimanje rizika – Podrazumijeva prihvaćanje rizika i nastavljanje s redovnim poslovnim operacijama te primjenu kontrola za ublažavanje rizika.

Izbjegavanje rizika – Strategija koja se odnosi na eliminiranje rizičnih situacija obustavom procesa i sustava u slučaju sumnje da će se pojaviti i odricanjem određenih funkcija koje su izložene riziku.

Ograničavanje rizika – Odnosi se na selektivnu primjenu odgovarajućih načela i tehnika kako bi se smanjila vjerojatnost pojave prijetnje i veličina štete. Koriste se preventivne i detektivne kontrolne mjere kao dio plana kontinuiteta poslovanja i plana hitnog odgovora.

Planiranje rizika – Ova opcija podrazumijeva razvijanje plana reduciranja rizika kroz prioritiziranje, primjenu i održavanje zaštitnih mjera. Planiraju se buduće situacije i shodno tome donose mjere. [54]

U drugim literaturama može se naići na još jednu bitnu strategiju smanjivanja utjecaja rizika, prebacivanje rizika. Prijenos rizika uključuje prebacivanje rizika trećoj voljnoj strani. Mnoge tvrtke izdvajaju vlastite poslove kao što su usluge kupcima ili izvršavanje naloga drugim tvrtkama, transferirajući time i rizik tih aktivnosti.[55]

Strategije smanjivanja utjecaja rizika se mogu promatrati i iz drugih perspektiva. Jedna od najčešćih pogleda jest s obzirom na vrstu oporavka informacijskog sustava. Ove strategije se nazivaju strategije oporavka sustava. Odnose se na primjenu procedura i postupaka sigurnosnog kopiranja podataka te oporavka poslovnih procesa i sustava od prekida. 4 su osnovne BC strategije oporavka informacijskog sustava: zrcaljenje, vruća lokacija, topla lokacija i hladna lokacija.

Zrcaljenje (engl. *Mirroring*) - Strategija s iznimno visokim troškovima jer omogućava potpunu redundanciju, duplicirano odvijanje svih operacija i potpuno sinkronizirane podatke, te zahtijeva

[54] Ransome, J. F. i Rittinghouse, J. W. (2005) *Business Continuity and Disaster Recovery for InfoSec Managers*. Burlington, MA: Elsevier Digital Press.

[55] Snedaker, S. (2007) *Business Continuity & Disaster Recovery for IT Professionals.* Burlington, MA: Syngress Publishing.

kontinuirano održavanje cijele infrastrukture. U slučaju odabira ove strategije, na pričuvnoj lokaciji osigurava se dostupnost svih resursa koji su u stalnoj upotrebi. Pričuvna lokacija se koristi paralelno s primarnom („active-active“) i raspoloživa je 24/7.

Vruća lokacija (engl. *Hot site*) - Strategija s visokim troškovima jer zahtijeva postojanje i redovito održavanje ICT opreme na pričuvnoj lokaciji, potpunu konfiguraciju opreme i instalaciju softvera te njenu spremnost da se u slučaju potrebe može aktivirati unutar 8 sati. Osigurava se replikacija podataka, a u pravilu na pričuvnoj lokaciju nema potrebe za stalnim angažmanom osoblja.

Topla lokacija (engl. *Warm site*) - strategija sa srednje visokim troškovima koji uključuju nabavu i redovito održavanje ICT opreme koja je parcijalno konfigurirana. U slučaju incidenta potrebno je provesti potpunu instalaciju i konfiguraciju te opreme vraćanje podataka iz raspoloživih sigurnosnih kopija. Spremnost pričuvne lokacije za rad može se osigurati unutar 48 sati.

Hladna lokacija (engl. *Cold Site*) - je strategija s niskim troškovima i jednostavnim održavanjem jer omogućava samo osnovno okruženje bez ikakve ICT i programske opreme. U slučaju odabira ove strategije, back-up podataka se osigurava fizičkim nošenjem back-up traka na pričuvnu lokaciju. U slučaju incidenta potrebno je provesti nabavu kompletne mrežne, hardverske i softverske opreme. Po završenoj instalaciji i konfiguraciji opreme, provodi se vraćanje podataka iz raspoloživih back-up traka. [56]

[56] Tomić Rotim, S. i Komnenić, V. (2017) Kako pripremiti sveobuhvatan plan kontinuiteta poslovanja? U: I. Nađ, ur. *Zbornik radova 10. Međunarodne znanstveno-stručne konferencije: Dani kriznog upravljanja. 24-26 studeni 2017, Terme Tuhelj, Hrvatska*. Velika Gorica: Veleučilište Velika Gorica, str. 475-489.

4. RAZVOJ, TESTIRANJE, REVIZIJA I ODRŽAVANJE PLANA KONTINUITETA POSLOVANJA

Nakon što su usvojene strategije za smanjenje rizika slijedi izrada priručnika plana kontinuiteta poslovanja, odnosno dokumentacije procedura koje je potrebno pokrenuti u slučaju pojave poremećaja kako bi se organizacija što prije oporavila i nastavila redovne poslovne aktivnosti. Plan kontinuiteta poslovanja određuje metode za primjenu strategija koje su razvijene u prethodnoj fazi te definira tko i kako treba izvršiti nužne aktivnosti. Ovo poglavlje govori o razvoju plana kontinuiteta poslovanja, zatim o testiranju i reviziju plana te naposljetku o načinima održavanja i ažuriranja.

4.1. Razvijanje plana kontinuiteta poslovanja i plana oporavka u slučaju katastrofe

Plan poslovnog kontinuiteta i oporavka od katastrofe je integrirani skup postupaka i informacija o resursima koji se koriste za oporavak od događaja koji su uzrokovali poremećaje u poslovanju. Odgovara na pitanja poput: tko (tko vrši oporavak), što (što će se učiniti), kada (redoslijed postupaka), gdje (gdje će se odvijati oporavak) i kako (koji resursi, dobavljači i kupci moraju biti uključeni). Nakon proglašenja katastrofe, plan aktivira unaprijed odobrene politike i postupke.
Planom se vraća odljev usluga s najmanjim mogućim troškovima za organizaciju. Cilj plana je ponovo omogućiti funkcioniranje organizacije. Jedan od osnovnih ciljeva jest svesti izvanredne troškove na minimum.
Tipična struktura BC/DR plana je:

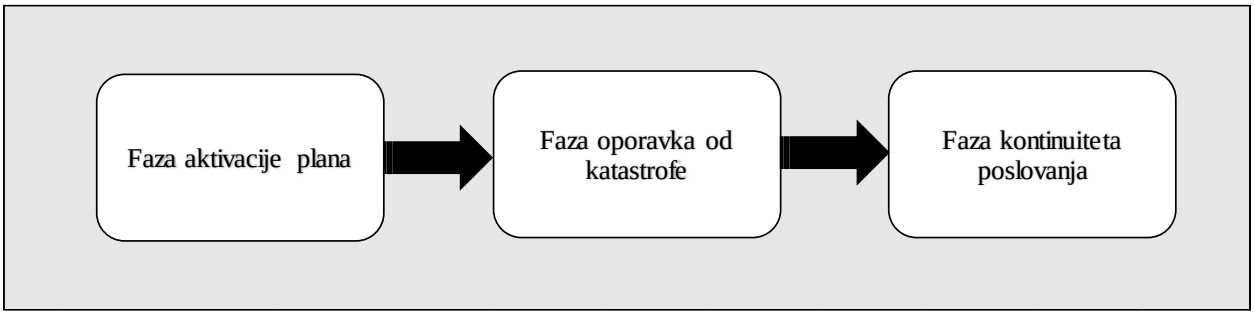
- početni odgovor,
- procjena štete,
- obavještavanje i mobilizacija zaposlenika,
- uloge, dužnosti i procedure timova za oporavak,
- informacije o zaposlenicima, dobavljačima i kupcima te
- postupci ispitivanja i održavanja.[57]

[57] Barnes, J. C. (2001) *A Guide to Business Continuity Planning*. Chichester: John Wiley & Sons, Ltd.

Svaki plan BC i DR plan treba imati navedene prijetnje, ranjivosti, rizike i potencijalni utjecaj na svaku od kritičnih poslovnih funkcija. Za sve značajnije prijetnje i rizike potrebno je imati povezane strategije ublažavanja utjecaja. U slučaju da se dogodi poremećaj poslovanja, kontinuitet poslovanja definira sljedeće faze u procesu obnove.

Aktivacijska faza – Odnosi se na definiranje okidača za aktivaciju plana oporavka i kontinuiteta poslovanja. Potrebno je razraditi jasan skup parametara prema kojima se određuje aktivacija plana. Ovo je izrazito bitno da se ne bi dovelo do problema učestale aktivacije plana za svaki manji poremećaj. Za ovu fazu se definiraju različite razine poremećaja i katastrofe i njihovi *triggeri* kako bi se mogla primijeniti sukladna protumjera. Aktivaciju plana čini obično osoba ili tim ljudi zaduženih za procjenu izvanrednih situacija. Neki od timova koji se definiraju za ovaj proces su krizni timovi, timovi za procjenu štete, timovi za obavještavanje, timovi za hitne situacije i krizni timovi za komunikaciju. Jednom kada je okidač aktiviran, poduzimaju se hitni koraci predviđeni za takve situacije poput obavještavanja kriznog tima, prikupljanja informacija s terena i aktiviranja tima za procjenu štete. Nakon zauzdavanja hitne situacije slijedi prelazak iz aktivacijske faze u fazu oporavka.[58]

Slika 14. Faze procesa oporavka



Izvor: Vlastiti rad

Faza oporavka – Ova faza uobičajeno pretpostavlja da je uzrok poremećaja zaustavljen ili pod kontrolom. Fazu oporavka obično vodi tim za upravljanje krizama te koordinira svoje napore temeljem specifičnosti situacije. Aktivnosti koje obavlja mogu uključivati hitne slučajeve,

[58] Snedaker, S. (2007) *Business Continuity & Disaster Recovery for IT Professionals.* Burlington, MA: Syngress Publishing

reakcije na katastrofe, stavljanje alternativne lokacije u funkciju, upravljanje kriznim komunikacijama i druge zadatke ovisno o vrsti poslovanja. Znak prelaska u sljedeću fazu je onaj kada se učinci poremećaja riješe ili dovedu u potpunu kontrolu, te se recimo aktivira sekundarna oprema ili lokacija.

Faza poslovnog kontinuiteta – Aktivnosti kontinuiteta poslovanja započinju završetkom napora za oporavak. Ova faza se odnosi na načine ponovnog započinjanja poslovnih operacija i potpornog sustava s privremene lokacije. Kontrolni popis kontinuiteta bi trebao sadržavati korake potrebne za nastavak ograničenih operacija, identificirati zahtjeve i ovisnosti, te uključivati vremenske rokove i ciljne točke. Posljednji koraci odnose se na premještanje na izvornu lokaciju i prijelaz u uobičajene poslovne operacije. Za navedene korake kontinuitet poslovanja treba sadržavati okidače koji će definirati kraj faze i time povratak u normalno poslovanje.[59]

Produkt procesa kontinuiteta poslovanja je plan u vidu priručnika za kontinuitet poslovanja. Osnovne informacije koje priručnik treba sadržavati su:

- imena, adrese i telefonske brojeve kriznog rukovodstva,
- listu zaposlenih u generalnim/općim službama,
- listu najvažnijih klijenata i dobavljača,
- točnu lokaciju udaljenih sigurnosnih kopija podataka,
- kopije ugovora o osiguranju te
- kopije drugih kritičnih materijala nužnih za ostvarenje kontinuiteta poslovanja organizacije.[60]

Kompleksniji priručnik može sadržavati i sljedeće elemente:

- opis sekundarne (rezervne) radne pozicije,
- tehničke zahtjeve poslovanja organizacije,
- zakonske zahtjeve za izvješćivanjem i akcijama po nastupu katastrofalnog događaja,

[59] Snedaker, S. (2007) *Business Continuity & Disaster Recovery for IT Professionals.* Burlington, MA: Syngress Publishing.
[60] CARNet CERT (2010) Upravljanje kontinuitetom poslovnih procesa [online] www.cis.hr. Dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-15-307.pdf

- mjere za početak oporavka radne aktivnosti poduzeća,
- mjere za ponovno uspostavljanje integriteta fizičkih zapisa,
- načine ponovnog uspostavljanja lanca nabave i
- načine izgradnje novih proizvodnih centara.[61]

4.2. Testiranje i revizija plana

Postupak testiranja plana određuje jesu li izvedive dokumentirane strategije oporavka i njima pridruženi postupci za oporavak kritičnih proslovnih funkcija u okviru navedenih vremenskih rokova. Ispitivanjem plana potvrđuju se napisane pretpostavke i identificiraju jake i slabe strane plana. Minimalne preporuke predlažu testiranje svih komponenti BCP-a jednom godišnje kako bi se provjerila djelotvornost. No, ujedno se preporučuje da ispitivanja ne prelaze definirane granice učestalosti. Za stvarno dokazivanje efektivnosti plana potrebno je testirati sve njegove dijelove zajedno jer će se time neke jedinice prvi put naći u situaciji suradnje. To predstavlja sasvim nove koordinacijske zahtjeve i napore. Stoga je bolje razumjeti i ispraviti moguće probleme prije nego zaista nastane izvanredni slučaj. [62]

Provedbom testne provjere utvrđuju se slabosti plana koji je potrebno doraditi ili zamijeniti, ili uopće provedivost tog plana. Uzimajući u obzir složenost i obuhvatnost provjere, mogu se odrediti tri kategorije plana prikazane u tablici.

[61] CARNet CERT (2010) Upravljanje kontinuitetom poslovnih procesa [online] www.cis.hr. Dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-15-307.pdf
[62] Barnes, J. C. (2001) *A Guide to Business Continuity Planning*. Chichester: John Wiley & Sons, Ltd.

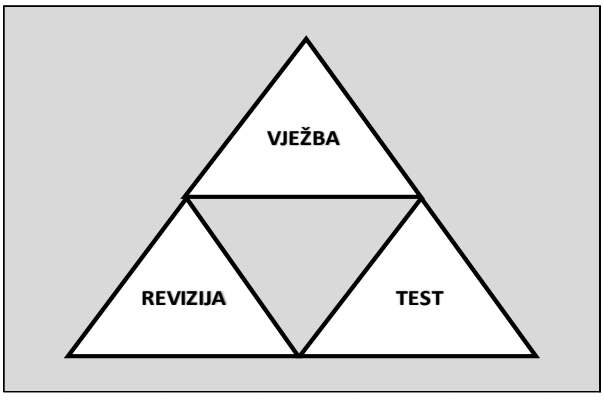
Tablica 5. Kategorije testne provjere plana

Jednostavna provjera	Sastoji se od testiranja specifičnog dijela plana za ponovno uspostavljanje poslovnih procesa. Ovaj tip provjere obično ne oduzima previše vremena i resursa. Primjer je recimo provjera informatičke opreme što bi uključivalo samo zaposlenike tog područja u organizaciji.
Srednje složena provjera	Ova vrsta provjere se odnosi na više odjela unutar organizacije prilikom koje dolazi do potrebe za suradnjom među svim uključenim odjelima. Ovakva testiranja i vježbe mogu potrajati i po nekoliko dana.
Složena provjera	Sveobuhvatna provjera plana koja uvježbava sve zaposlenike za izvanredne slučajeve. Predstavlja stvaran pokušaj rješavanja prijetnje s kojom je suočena organizacija. Primjer je stvarno aktiviranje alternativne lokacije i prijenos poslovanja na to mjesto. Prilikom ove provjere dolazi se do vrijednih informacija za sam plan i njegove buduće inačice.

Izvor: Centar informacijske sigurnosti – CIS (2011.) Upravljanje kontinuitetom poslovnih procesa

U ovoj fazi upravljanja kontinuitetom poslovanja aktivnosti su povezane, kao što je prikazano na slici poviše. Ukoliko se provodi ispitivanje plana, tada se u jednu ruku i uvježbava zaposlenike u slučaju neželjenog događaj a zatim se rezultatom testiranja dolazi do eventualnih slabijih područja plana koje je potrebno revidirati i prilagoditi.

Slika 15. Veza između uvježbavanja, testiranja i revizije



Izvor: Snedaker, S. (2007) Business Continuity & Disaster Recovery for IT Professionals

Uvježbavanje i obuka trebaju biti usredotočeni na upoznavanje osoblja s ulogama, odgovornostima i vještinama potrebnim za izvršenje plana. Potrebno ih je organizirati najmanje jednom godišnje kako bi se osiguralo spremnost zaposlenika ukoliko dođe do stvarnog prekida. Također, zaposlenici bi trebali biti osposobljeni za hitne situacije u onoj mjeri u kojoj je moguće izvršiti sve zadatke plana za bez pomoći stvarnog priručnika za plan kontinuiteta poslovanja. To je važan cilj u slučaju da papirnata ili elektronička verzija plana bude nedostupna prvih nekoliko sati, kao rezultat poremećaja. Osoblje za oporavak treba biti obučeno za sljedeće elemente plana:

- svrha plana;
- koordinacija i komunikacija između timova;
- postupci izvještavanja;
- sigurnosni zahtjevi;
- procesi specifični za tim (faze aktivacije i obavijesti, oporavka i rekonstitucije); i
- individualne odgovornosti (faze aktiviranja i obavještavanja, oporavka i rekonstitucije).[63]

Revizija i procjena cjelokupnog BCM procesa uključuje sve faze životnog ciklusa od inicijacije projekta do testiranja i uvježbavanja. Nekada su revizori ograničavali svoje aktivnosti samo na traženje postojanja plana kontinuiteta ili plana oporavka bez da su provodili revizorke postupke i testove. Takva percepcija revizije postoji i dan danas u dosta organizacija. Osnovna svrha funkcije revizije unutar BCM-a jest uklanjanje nesigurnosti oko mnogih pitanja. Koji su primjenjivi standardi ili propisi? Kako se prepoznaje puna sukladnost? Što znači prihvatljiva razina rizika? Koji je sveukupni cilj revizije? Odgovori na ova i slična pitanja definiraju okvir revizije BCM-a.[64]

Interna revizija u sklopu upravljanja kontinuitetom poslovanja ima zadatak revidirati strategiju i procese planiranja kako bi ih uskladila sa zakonskim i industrijskim zahtjevima i standardima.

[63] NIST Special Publication 800-34, Revision 1 (2010) *Contigency Planning Guide for Federal Information Systems*. Gaithersburg, Maryland: National Institute of Standards and Technology. [online]. Dostupno na: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

[64] Hiles, A. (2007*) The Definitive Handbook of Business Continuity Management.* Chichester: John Wiley & Sons, Ltd.

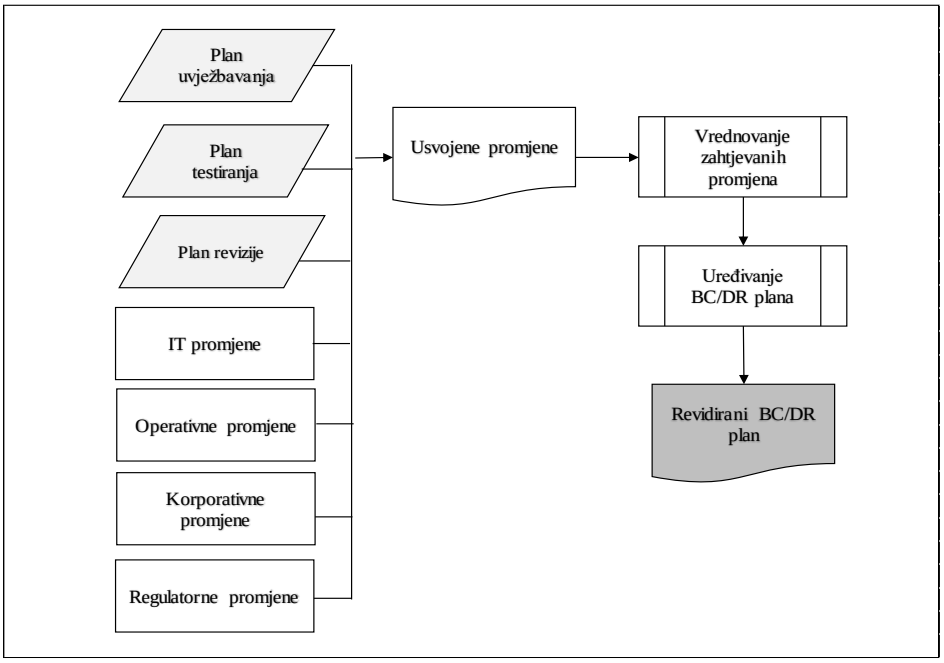
Učestalost revizije BCM-a ovisi o organizaciji, njenim internim standardima i regulativama koje mora poštivati. U većini slučajeva se provodi jednom godišnje u sklopu aktivnosti testiranja, uvježbavanja i održavanja plana. Vještine i znanja koja su povezana s BCM-om donekle već postoje u funkcijama interne revizije. Stoga, revizori imaju potrebne kompetencije da aktivno sudjeluju i budu dio razvoja procesa nastavka poslovanja zajedno s menadžmentom u čijoj je ovlasti i odgovornosti donošenje odluka o oblikovanju tog programa.[65]

4.3. Ažuriranje BC/DR plana

Promjene u okruženju organizacije su konstantne bilo da se radi o promjenama u poslovanju, tehnologiji, ljudskim resursima, zakonima i propisima itd. Zato je vrlo važno stalno pratiti te promjene i usklađivati svoje poslovne procese. Na slici niže je prikazan proces održavanja i ažuriranja plana kontinuiteta poslovanja i plana oporavka od katastrofe. Nakon što je završena faza testiranja, uvježbavanja i revizije plana, slijedi proces praćenja promjena koje utječu na poslovanje Nakon toga je potrebno odrediti koje promjene utječu na poslovanje, vrednovati im utjecaj i zatim ažurirati plan.

[65] Tomić Rotim, S. i Komnenić, V. (2017) Kako pripremiti sveobuhvatan plan kontinuiteta poslovanja? U: I. Nađ, ur. *Zbornik radova 10. Međunarodne znanstveno-stručne konferencije: Dani kriznog upravljanja. 24-26 studeni 2017, Terme Tuhelj, Hrvatska*. Velika Gorica: Veleučilište Velika Gorica, str. 475-489.

Slika 16. Proces održavanja i ažuriranja plana



Izvor: Snedaker, S. (2007) Business Continuity & Disaster Recovery for IT Professionals

Redovnim praćenjem promjena i održavanjem BC i DR plana organizacija je pripremna na poremećaje kad god da se realiziraju, te samim time izbjegava situaciju izrade novog plana iz početka, što naravno oduzima mnogo vremena i resursa.

Neki podaci koje je potrebno identificirati i osvježavati unutar plana su:

- promjene u rasporedu zaposlenika,
- promjene dobavljača i kupaca, i njihovi kontakt podaci te
- promjene odjela unutar poduzeća ili organizacije (poput otvaranja novog odjela, zatvaranja postojećeg odjela ili fundamentalnih organizacijskih promjena).

Kao dio tekućeg održavanja, svako tehničko rješenje mora imati provjerenu funkcionalnost. Aktivnosti u sklopu održavanja mogu biti provjera distribucije novih virusnih definicija, sigurnost aplikacija, distribucija sigurnosnih zakrpa, provjera operativnosti hardvera i aplikacija te provjera sigurnosti podataka. Pošto se poslovni procesi mijenjaju tijekom vremena, organizacijske procedure oporavka iz prošlosti mogu postati neadekvatne. Najčešće provjere se odnose na:

- provjeru dokumentiranosti,
- provjeru sustava zaduženih za izvođenje kritičnih funkcija,
- jesu li dokumentirane radne liste provjera smislene i točne te
- provjeru omogućuju li dokumentirane procedure oporavka i potporna infrastruktura oporavak unutar unaprijed određenog vremena.[66]

[66] CARNet CERT (2010) Upravljanje kontinuitetom poslovnih procesa [online] www.cis.hr. Dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-15-307.pdf

5. USPOREDBA ALATA ZA IZRADU SIGURNOSNIH KOPIJA

„Backup je rezervna kopija svih podataka koji se mogu koristiti za vraćanje podataka u izvornom oblik kada je to potrebno. To je kopija svih validnih podataka, datoteka, aplikacija ili operativnih sustava koji se mogu koristiti u svrhu oporavka.“[67]

Navedena definicija sigurnosne kopije naglašava osnovnu svrhu njene izrade, a to je oporavak. Sigurnosno kopiranje kritičnih podataka bez razvijenih funkcionalnosti za povrat napravljenih kopija jednostavno ne ispunjava vlastitu svrhu.

5.1. Općenito o backup alatima

Sigurnosno kopiranje podataka se izrađuje kako bi se omogućilo organizaciji da nastavi s poslovnim operacijama u slučaju poremećaja. Sigurnosno kopiranje se izvršava pomoću aplikacija za izradu istih. Uobičajeno backup aplikacije omogućuju izradu sigurnosnih kopija podataka, datoteka, mapa, dokumenata, aplikacija te čitavih korisničkih ili poslužiteljski računala. Stvaranje rezervne kopije podataka se može koristiti za povrat podataka u slučaju da se dogodi neželjeni događaj koji bi prouzrokovao gubitak originalnih.

Alati za izradu sigurnosnih kopija obično koriste ove metode:

Full Backup – izrada potpuno sigurnosne kopije svih označenih objekata.

Incremental Backup – izrada sigurnosne kopije samo onih podataka koji su se promijenili u odnosu na posljednju kopiju.

Differential Backup – izrada sigurnosne kopije onih podataka koji su se promijenili u odnosu na posljednji potpuni backup.

Consolidated Backup – izrada sigurnosne kopije u kojoj se spaja prvi potpuni backup s ostalim kasnije izvršenim inkrementalnim ili diferencijacijskim backupima.[68]

Dvije vrste sigurnosnih kopija s obzirom na arhitekturu su sigurnosna kopija na razini podatka i na razini preslike. Sigurnosna kopija na razini podatka je spremljena kako i sam naziv govori u formi datoteka. Obično ima dodatne funkcionalnosti kompresije i deduplikacije kojima se

[67] De Guise, P. (2008) *Enterpise Systems Backup and Recovery: A Corporate Insurance Policy*. Boca Raton, FL: CRC Press

[68] De Guise, P. (2008)

smanjuje veličina kopiranih podataka odnosno ne kopiraju duple datoteke. Sigurnosna kopija na razini preslike sprema kopiju kao jednu datoteku koja sadrži čitav operacijski sustav zajedno sa svim podacima, aplikacijama i konfiguracijom backupiranog objekta, bilo fizičkog ili virtualnog. Prednosti i slabosti pojedine su prikazane niže u tablici.

Tablica 6. Usporedba vrsta sigurnosnih kopija

Vrsta sigurnosne kopije	Prednosti	Mane
Sigurnosna kopija na razini podatka (engl. *File-level Backup*)	• Učinkovit za povrat manjeg broja datoteka • Fleksibilnost u odabiru željenih datoteka za backup • Fleksibilnost u odabiru pravila sigurnosnog kopiranja	• Može trošiti previše vremena u slučaju velikog broja manjih podataka • Manja promjena u datoteci traži ponovni backup
Sigurnosna kopija na razini preslike (engl. *Image-level Backup*)	• Učinkovit za oporavak cijelog sustava • Kratko vrijeme oporavka • Manji problemi s performansama	• Nije učinkovit za oporavak malog broja datoteka • Zahtijeva više prostora za pohranu kopija

Izvor: Vašak, J. (2017) Analysis of Backup for Small and Medium-sized Enterprises (SME) in the Czech Republic

Dalje u radu ću predstaviti dva softvera za izradu sigurnosnih kopija i oporavak u slučaju katastrofe, te zatim usporediti njihove funkcionalnosti i dati osobno mišljenje kao korisnika.

5.2. Veeam Backup and Replication

Veeam je jedan od vodećih proizvođača rješenja za sigurnosnu pohranu virtualiziranih okolina u VMware i Microsoft Hyper-V okruženju. Vodeći proizvod kompanije je rješenje Veeam Backup and Replication. Softver Veeam Backup & Replication predstavlja sigurnosno rješenje za dostupnost potpune radne okoline bilo da se radi o fizičkoj, virtualnoj ili baziranoj na oblaku. Ovaj softver pruža skup različitih mogućnosti za zaštitu podataka i zadatke oporavka od

katastrofe. Jedinstvena upravljačka konzola softvera omogućuje upravljanje svim sigurnosnim kopijama, replikacijama i oporavkom podataka, aplikacija ili pak poslužitelja.

Tri osnovne funkcionalnosti Veeam Backup & Replication alata su backup, replikacija i povrat usluge.

Backup funkcionalnost radi način da prvo napravi snimi virtualni stroj u nekoj točki u vremenu, tzv. checkpoint, koji zatim koristi kao izvor za izradu kopije. Za vršenje ove funkcije potrebno je napraviti i konfigurirati zadatak za sigurnosno kopiranje (engl. *backup job*).

Značajke unutar sustava izrade sigurnosnim kopija:

- **Veeam Cloud Tier** – neograničen kapacitet za dugoročno čuvanje podataka omogućujući skalabilnost lokalno i u oblaku.
- **Veeam Plug-ins for SAP HANA and Oracle RMAN** - poboljšana skalabilnost i operacijska učinkovitost u upravljanju poslovnih okruženjem.
- **Built-in management for Veeam Agent for Microsoft Windows and Veeam Agent for Linux** - izravno upravljanje sigurnosnim kopijama svih radnih okolina unutar jedinstvene aplikacijske konzole.
- **Image-level VM backups** – stvaranje sigurnosnih kopija aplikacija pomoću napredne aplikacijske obrade.
- **Backup from Storage Snapshots** – generiranje ultra brzih sigurnosnih kopija s niskim RPO-om iz snimke spremišta podataka.
- **Scale-out Backup Repository** – jedinstvena baza podataka sigurnosnih kopija za upravljanje kopijama bilo u oblaku ili lokalno..
- **Veeam Cloud Connect** – omogućava off site izradu kopije bez potrebe za informatičkom infrastrukturom van organizacije odnosno mogućnost brzog i sigurnog backupa u oblaku kod davatelja usluga.
- **SureBackup** – mogućnost automatskog testiranja vraćanja u rad i verifikacije svake sigurnosne kopije i virtualnog stroja.
- **Direct Storage Access** – izvršavanje bržih backupa virtualnih strojeva VMware platforme direktno preko mreže spremišta podataka.
- **Native tape support** – potpuna podrška sustava za izradu backupa preko vrpce što uključuje kopiranje na istu, povrat kopija s vrpce i paralelnu obradu.

Replikacija ima isti zadatak kao i funkcionalnost izrade backupa, napraviti sigurnosnu kopiju. Razlika je u tome što se stvara potpuna jednaka replika podataka u početnom formatu bez kompresije, što nije slučaj kod backupa. Ovime je omogućena visoka dostupnost i potpuni povrat u jako kratko vrijeme jer je kopija virtualnog stroja u spremnom stanju. Ova funkcionalnost je preporučena za najkritičnije poslužitelje na kojem se nalazi baze podataka za rad sustava ili kritične aplikacije.

Osnovne mogućnosti replikacije su:

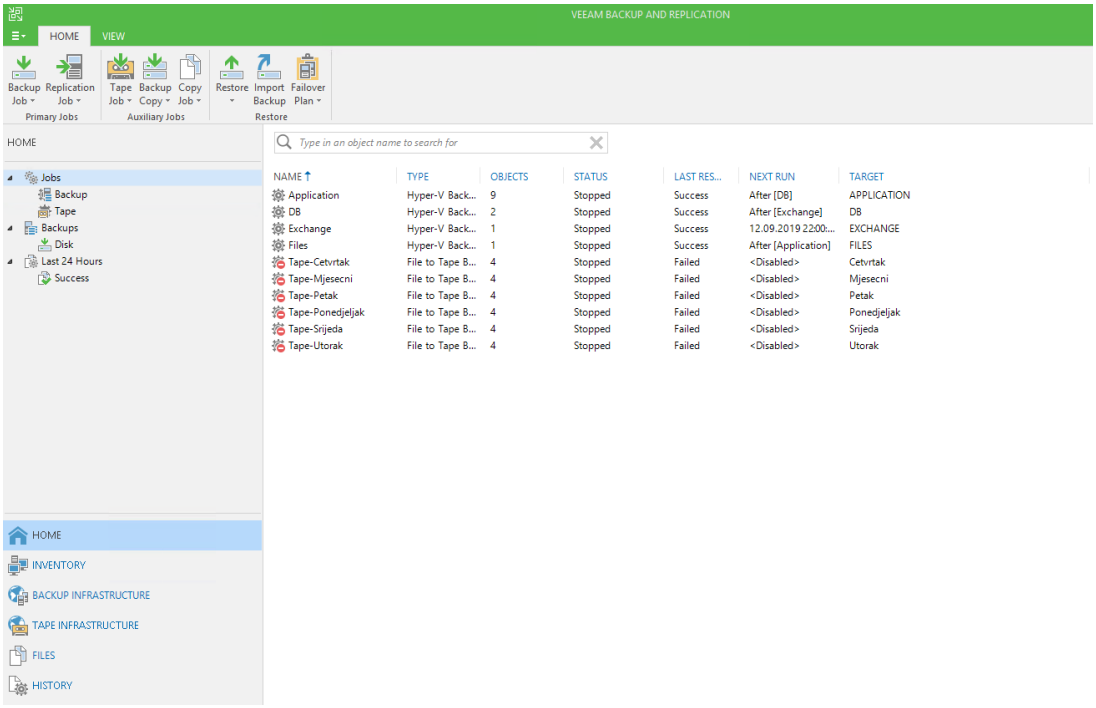
- **Image-based VM replication** – mogućnost replikacije virtualnog stroja on site za scenarij visoke dostupnosti i off site za slučaj oporavka od nepogode.
- **Veeam Cloud Connect Replication** - omogućava off site izradu replike bez potrebe za informatičkom infrastrukturom van organizacije. Temelji se na oblaku kod davatelja usluga.
- **SureReplica** - testiranje i verifikacija povrata replike virtualnog stroja u operativno stanje
- **Failover and Failback** – povrat replike stroja i potpomognuto prebacivanje servisa u funkciju s minimalnim ili nikakvim prekidima operacija.

Povrat usluge pruža brzu i pouzdanu obnovu pojedinačnih datoteka, čitavih virtualnih strojeva i aplikacija uz veoma kratko ciljno vrijeme oporavka. Glavne značajke ove funkcionalnosti su:

- **Instant VM Recovery** - omogućava povrat i pokretanje virtualnog stroja izravno iz sigurnosne kopije uz RTO od 2 minute.
- **Instant File-Level Recovery** - omogućava povrat datoteka operacijskog sustava određenog virtualnost stroja i drugih specificiranih dijelova mapa, konfiguracijskih datoteka i sl.
- **Veeam Cloud Mobility** – laka prenosivost i oporavak bilo koje lokalne radne okoline ili u oblaku na AWS, Azure i Azure Stack u samo par koraka.
- **Recover with added confidence** – Povrat backupa s dodanim sigurnosnim mjerama Veeam DataLabs Secure Restore-a i implementiranim GDPR smjernicama Veeam DataLabs Staged Restore-a.

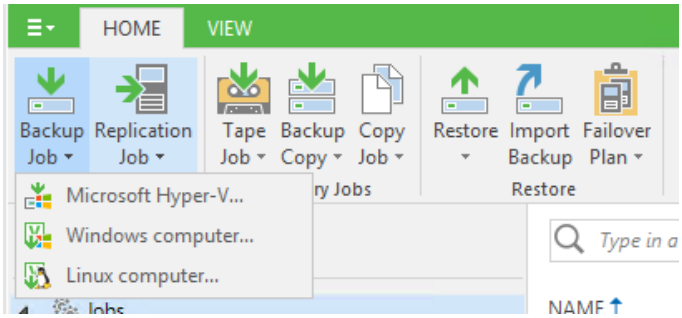
- **Veeam Explore for Microsoft Active Directory –** Brzi oporavak pojedinih objekata iz Active Directoryja ili cijelih spremnika; jednostavno vraćanje korisničkih računa i pripadajućih lozinki; omogućen povrat objekata pravilnika skupine (engl. *Group Policy Objects – GPO)*, DNS zapisa i sl.
- **Veeam Explorer for Microsoft Exchange** – brz i detaljan oporavak objekata Exchangea uključujući teško izbrisive stavke, detaljna izvješća i druge stvari.
- **Veeam Explorer for Microsoft SharePoint** – jednostavan pregled SharePoint kopija i brz oporavak stavki i određenih web lokacija.
- **Veeam Explorer for Microsoft SQL Server** – mogućnost preciziranog oporavka SQL baza podataka u nekoj točki u vremeni.
- **Veeam Explorer for Oracle –** oporavak Oracle baza podataka na razini transakcije uključujući transakcijske logove.
- **Veeam Explorer for Storage Snapshots** – povrat individualnih datoteka i čitavih virtualnih strojeva iz snimke stroja pohranjene na spremniku.

Slika 17. Prikaz upravljačke konzole Veeam Backup and Recovery aplikacije



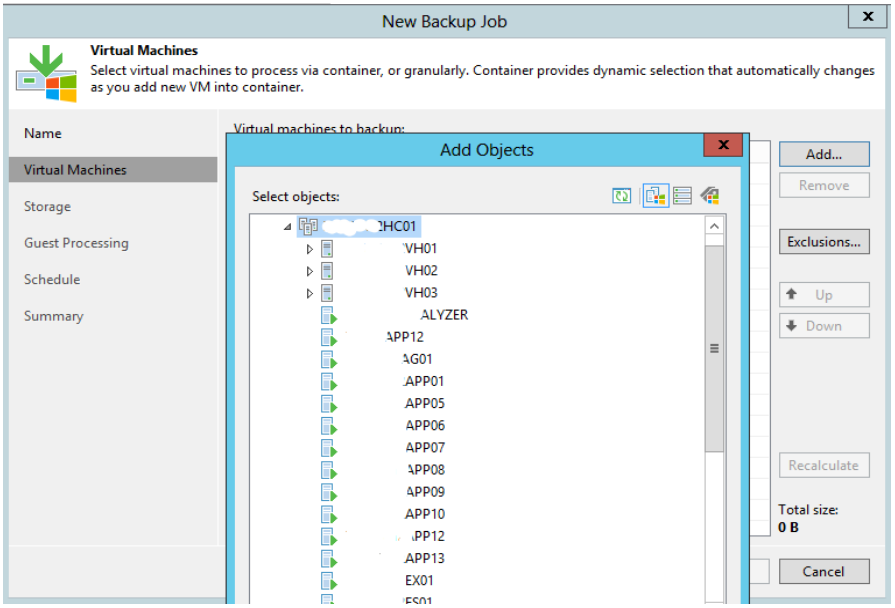
Na slici 17. je prikazan početni ekran upravljačke konzola aplikacije. Traka s izbornicima se sastoji od 8 glavnih izbornika – „*Backup Job*“, „*Replication Job*“, „*Tape Job*“, „*Backup Copy*“, „*Copy Job*“, „*Restore*“, „*Import Backup*“ i „*Failover Plan*“ – koji će biti u nastavku objašnjeni. „*Backup Job*“ služi za kreiranje zadatka za izradu sigurnosne kopije. Odabirom na taj izbornik otvara se padajući izbornik s tri vrste backupa.

Slika 18. Odabir objekta za sigurnosno kopiranje



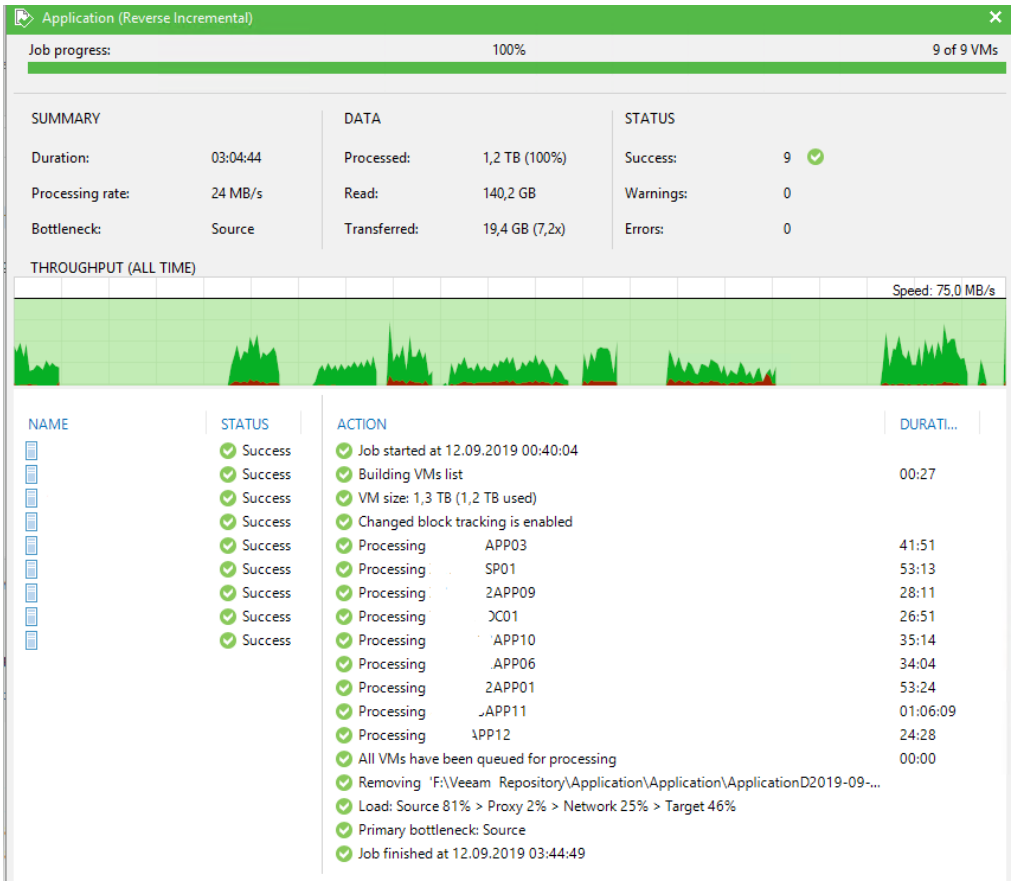
„*Microsoft Hyper-V*“ se odnosi na izradu sigurnosne kopije Hyper-V hosta i pripadajućih virtualnih strojeva, dok se odabirom „*Windows computer*“ i „*Linux computer*“ konfigurira zadatak za izradu kopija odabranih fizičkih poslužitelja.

Slika 19. Novi zadatak za izradu sigurnosne kopije



Odabirom „*Microsoft Hyper-V*“ otvara se novi prozor za konfiguraciju backup zadatka. Prvo je potrebno unijeti ime zadatka. Zatim pod „*Virtual Machines*“ se klikne na „*Add*“ i doda željeni objekt za kojeg želimo izraditi sigurnosnu kopiju. Može se izabrati izrada kopije cijelog klastera HC01, nekog od Hyper-V hostova VH01, VH02 i VH03, ili pojedini virtualni stroj na popisu poput APP01, APP05 itd. Zatim se odabire mjesto i pravila pohrane unutar postavke „*Storage*“. „*Guest processing*“ pruža dodatne mogućnosti napredne aplikacijske obrade i indeksiranja podatkovnog sustava na virtualnim strojevima. Te stavke omogućuju konzistentni backup aplikacija i njenih logova odnosno pretragu i vraćanje pojedinačnih datoteka. Za kraj se definira vrijeme i učestalost izvršavanja ovog posla.

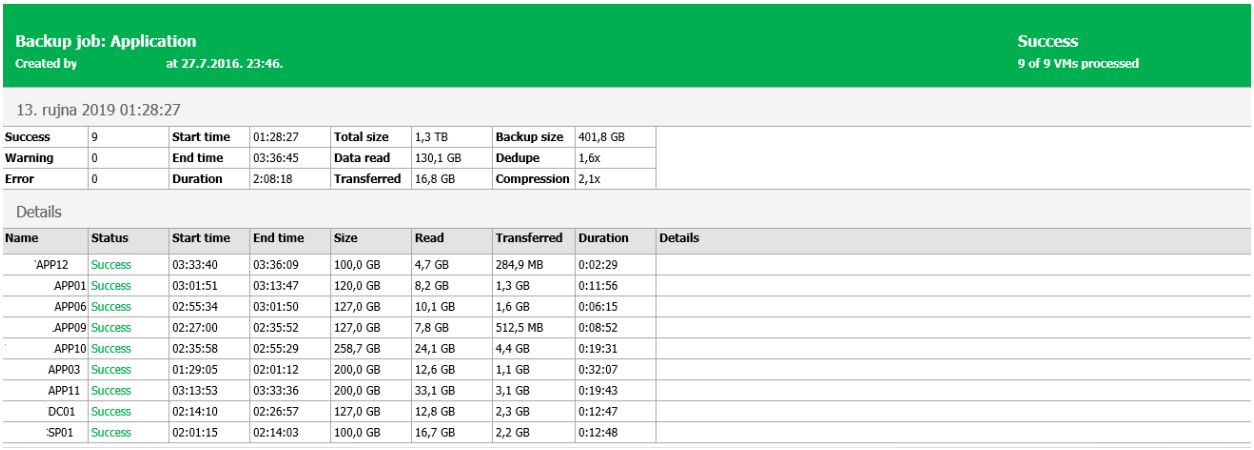
Slika 20. Primjer izvršenog zadatka sigurnosnog kopiranja



Ispod „*SUMMARY*“ možemo vidjeti koliko je bilo trajanje zadatka (3h i 4min), brzinu obrade (24 MB/s), ukupnu količinu obrađenih podataka (1.2 TB), uspješnost obrade i druge korisne

detalje. Također se može vidjeti koliko je trajala izrada kopije za svaki pojedini virtualni stroj. Recimo za stroj APP03 je trajalo 41 minutu i 51 sekundu. Dodatna mogućnost je slanje izvještaja o uspješno provedenom radnom zadatku na email što olakšava sistemski posao održavanja sustava.

Slika 21. Primjer izvještaja o uspješno provedenom backupu



Backup job: Application — **Success**
Created by at 27.7.2016. 23:46. — 9 of 9 VMs processed

13. rujna 2019 01:28:27

Success	9	**Start time**	01:28:27	**Total size**	1,3 TB	**Backup size**	401,8 GB
Warning	0	**End time**	03:36:45	**Data read**	130,1 GB	**Dedupe**	1,6x
Error	0	**Duration**	2:08:18	**Transferred**	16,8 GB	**Compression**	2,1x

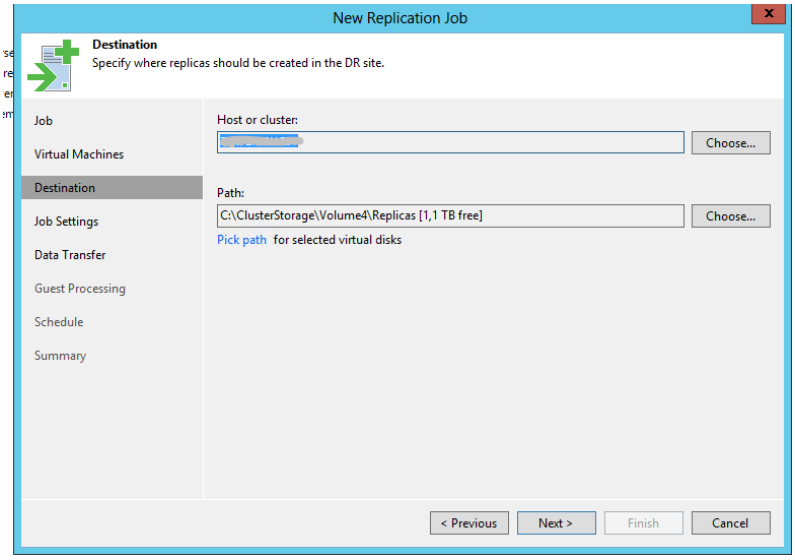
Details

Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
APP12	Success	03:33:40	03:36:09	100,0 GB	4,7 GB	284,9 MB	0:02:29	
APP01	Success	03:01:51	03:13:47	120,0 GB	8,2 GB	1,3 GB	0:11:56	
APP06	Success	02:55:34	03:01:50	127,0 GB	10,1 GB	1,6 GB	0:06:15	
APP09	Success	02:27:00	02:35:52	127,0 GB	7,8 GB	512,5 MB	0:08:52	
APP10	Success	02:35:58	02:55:29	258,7 GB	24,1 GB	4,4 GB	0:19:31	
APP03	Success	01:29:05	02:01:12	200,0 GB	12,6 GB	1,1 GB	0:32:07	
APP11	Success	03:13:53	03:33:36	200,0 GB	33,1 GB	3,1 GB	0:19:43	
DC01	Success	02:14:10	02:26:57	127,0 GB	12,8 GB	2,3 GB	0:12:47	
SP01	Success	02:01:15	02:14:03	100,0 GB	16,7 GB	2,2 GB	0:12:48	

Slika 21. prikazuje uspješan izvještaj o sigurnosnom kopiranju virtualnih servera koji pristiže na konfiguriranu email adresu. Na izvještaju je jasno vidljiva uspješnost zadatka, potrebno vrijeme za izvršenje, brzina prijenosa, ukupna veličina kopiranih podataka itd. Moguće je napraviti automatizaciju slanja izvještaja po svakom završetku radnog zadatka što omogućava administratorima dostupne informacije o stanju backupa bez da su logirani na aplikacijski sustav.

Na sličan način se može napraviti i replikacijski zadatak. „*Replication Job*“ služi za stvaranje potpune jednake replike odabranog virtualnog stroja. Nije moguće izraditi repliku fizičkog stroja. Prvo se unosi ime zadatka pod elementom „*Job*“. Zatim se kao i kod backup zadatka dodaje željeni virtualni stroj za replikaciju. Nakon toga se odabire host i putanja do mape na kojoj će se nalaziti replikacija stroja. U „*Job Settings*“ se definira naziv replike, repozitorij za meta podatke te pravila pohrane.

Slika 22. Novi zadatak za izradu replike



Pod „*Data Transfer*“ se izabire mod kopiranja. Opcije su „*on-host backup*“ i „*off-host backup*“ gdje se backup proxy server nalazi unutar infrastrukturi čime se možebitno opterećuje rad sustava, te u drugom slučaju gdje backup proxy podržava kopiranje i obradu izvana. „*Guest processing*“ pruža dodatnu mogućnost napredne obrade aplikacija. Zatim se odabire vrijeme i frekvencija izrade replike.

„*Tape Job*“ omogućuje izradu i pohranu sigurnosnih kopija u fizičkom obliku na vrpce. Moguće je napraviti kopije pojedinih datoteka ili mapa te čitave kopije virtualnih strojeva.

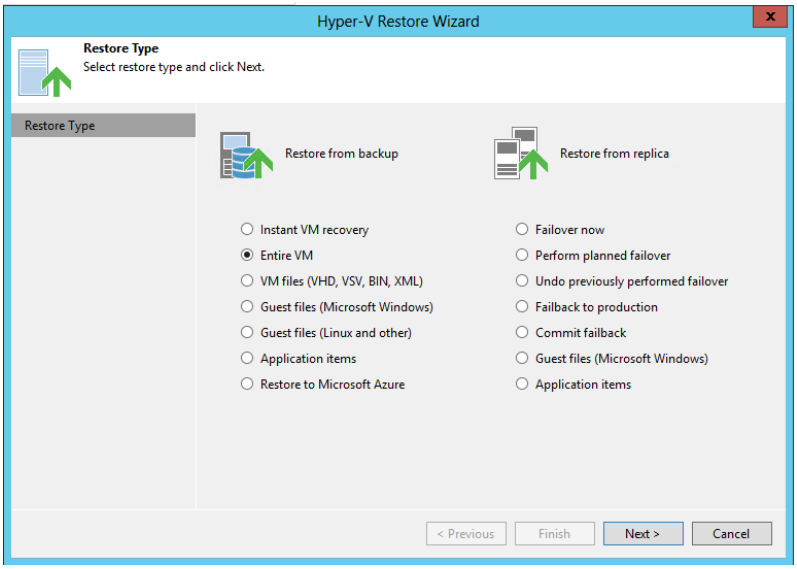
„*Backup Copy*“ se odnosi na izradu dodatne kopije na offsite lokaciji. To je vid dodatne sigurnosti u sklopu sigurnosnog pravila 3 - 2 – 1 koji nalaže da je:

- 3 – potrebno imati najmanje 3 kopije podataka, originalnu produkcijsku i barem dvije rezervne.
- 2 – potrebno koristiti barem dvije vrste medija za pohranu kopija, npr lokalno na disku i u oblaku.
- 1 – potrebno čuvati barem jednu kopiju na offsite lokaciji, bilo u oblaku ili na udaljenoj lokaciji.

„*Copy Job*“ je kao što sami naziv kaže odnosi na zadatak za izradu kopija datoteka.

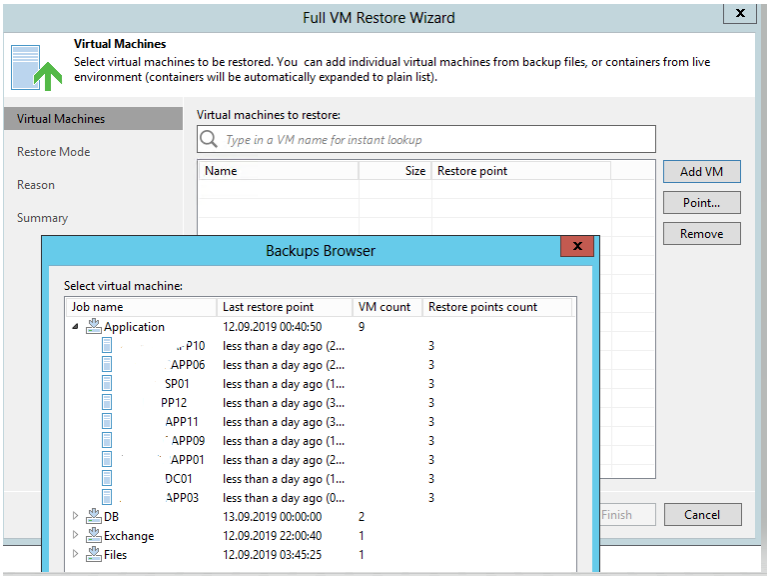
„*Restore*“ opcija je ključna funkcija unutar funkcionalnosti obnove u slučaju nepogode. Klikom na „*Restore*“ u izborniku otvara se novi prozor. Moguće je napraviti povrat iz sigurnosne kopije i iz replicirane kopije. Na slici su prikazani svi objekti koje je moguće povratiti. „*Restore from backup*“ omogućava povrat cijelih virtualnih strojeva, image datoteka, datoteka iz virtualnih strojeva i dijelova aplikacija.

Slika 23. Povrat željenog objekta



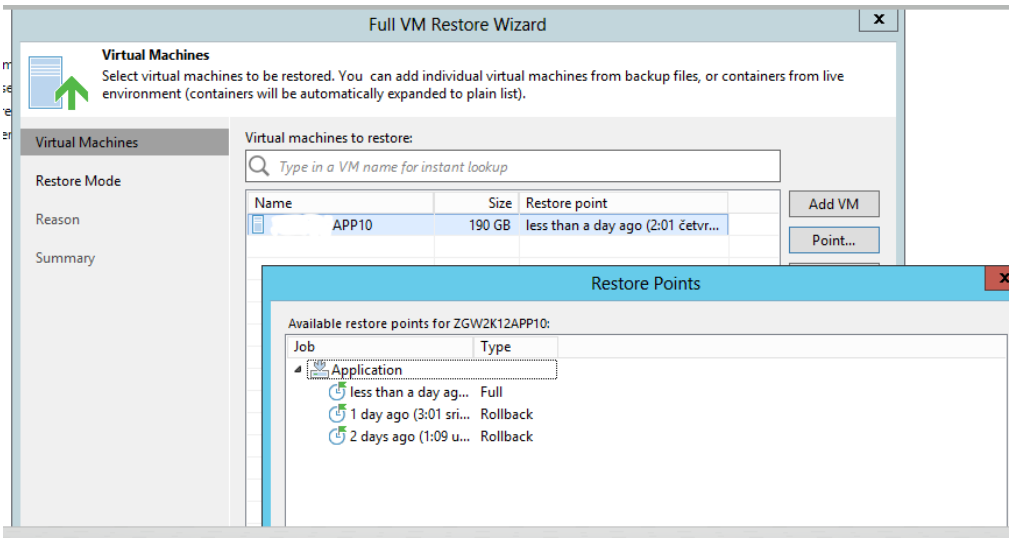
„*Restore from replica*“ omogućava povrat virtualnog stroja uživo bez ili uz minimalan ispad servisa koji su u operativnom statusu. Povrat iz replike nudi različite opcije kao što su „*Failover now*“ (instantno prebacivanje produkcije na repliku virtualnog stroja), „*perform planned failover*“ (planirano prebacivanje u slučaju više virtualnih strojeva) i druge. Odabirom povrata cijelog virtualnog stroja „*Entire VM*“ otvara se novi prozor.

Slika 24. Potpuni povrat virtualnog stroja



Klikom na „*Add VM*“ otvara se novi prozor gdje se odabiru željeni strojevi za povrat. Za ovaj slučaj odabrat ću aplikacijski server APP06 unutar repozitorija „*Application*“. Sljedeće možemo odabrati vremensku točku oporavka klikom na „*Point*“.

Slika 25. Odabir vremenske točke oporavka



Ponuđene su tri mogućnosti za ovaj slučaj: povrat stroja iz zadnje kopije, jučerašnje i kopije od prije dva dana. Odabirom jedne slijedi validacija sigurnosne kopije odabranog stroja. Ukoliko je uspješna, dalje se u postavkama odabire vrsta oporavka. Dvije su opcije „*Restore to the original location*“ (vraćanje odabranog stroja na originalnu lokaciju s prethodnim nazivom i postavkama) i „*Restore to a new location, or with different settings*“ (vraćanje stroja uz određene preinake). Nakon toga se upisuje razlog povrata odnosno obnove virtualnog stroja i pokreće zadatak.

Uz opisane funkcionalnosti Veeamovog softvera posebno bih istaknuo značajku „*SureBackup*“. Kao što je ukratko pojašnjeno prije, radi se o testiranju sigurnosnog kopiranja i provjere povrata podataka iz napravljenje kopije. Ova značajka omogućuje pokretanje kopiranog virtualnog stroja u izoliranom okruženju. Nakon pokretanja se vrše ispitivanja funkcionalnosti te se zatim po završetku kreira izvještaj o rezultatu testnog povrata. Ovime dakle možemo provjeriti uspješnost sustava za oporavak prije nego se katastrofa zaista dogodi.

5.3. Commvault Complete Backup and Recovery

Commvault je kompanija specijalizirana za izradu rješenja za sigurnost podataka i upravljanje informacijskih sustavima. Flagship proizvod kompanije je softver Commvault Complete Backup & Recovery, jedinstvena platforma za zaštitu podataka i upravljanje radnim okolinama lokalno i u oblaku. Ključne mogućnosti uključuju sigurnosno kopiranje podataka, snimke, replikaciju, arhivu, migraciju i zaštitu oblaka, detaljni oporavak, indeksiranje i pretraživanje sadržaja, oporavak od katastrofe i izvještavanje. Ove su značajke integrirane u podatkovnu platformu s jedinstvenom bazom kodova i na taj način pružaju učinkovitost u ukupnim troškovima i upravljanju. Commvault Complete Backup & Recovery je licencirani dio cjelokupne platforme Commvault, koja omogućava sveobuhvatnu zaštitu podataka i upravljanje podacima u podržanim sustavima, poslovnim aplikacijama, bazama podataka i virtualnim strojevima.

Osnovne funkcionalnosti programske platforme Commvault su:

Backup and Recovery - pruža učinkovito sigurnosno kopiranje i vraćanje podataka i podržava većinu operativnih sustava, baza podataka i aplikacija. Sustav za izradu sigurnosnih kopija koristi backup agente za međusobno povezivanje sustava datoteka i aplikacija za olakšavanje

prijenosa podataka iz produkcijskih sustava u zaštićeno rezervno okruženje. Izrada sigurnosnih kopija se vrši u pomoć backup agenata, softverskih modula koji se instaliraju na računala sa svrhom pristupa podacima i njihovom zaštitom.

OnePass and Archiving – korištenjem arhiviranja podataka može se zadržati, pohraniti, klasificirati i pristupiti informacijama prema njihovoj djelatnosti, sukladnosti ili dokaznoj vrijednosti s jednom metodom pristupa i očuvanja. OnePass predstavlja proces konvergiranja za sigurnosne kopije, arhive i izvještaje. Pomoću ove značajke je moguće riješiti probleme masovnih podataka i rastom spremnika emailova drastičnim smanjivanjem njihove veličine.

Virtual Machine Integration – omogućuje virtualizaciju najzahtjevnijih aplikacija i duboku integraciju u virtualnu infrastrukturu kako bi se pružila napredna mogućnost upravljanja podacima i automatizacija zaštite virtualnih strojeva.

Snapshot Management – tehnologija IntelliSnap automatizira stvaranje hardverskih kopija snimki u okruženjima pohrane podataka mnogih dobavljača. Također ima funkcionalnost kategoriziranja podatkovnih snimki kako bi se pojednostavio proces oporavka pojedinačnih datoteka.

Endpoint Solutions – osigurava siguran pristup podacima, sigurnost i zaštitu za uređaje krajnjih korisnika.

Security and Encryption – koriste se tehnologije enkripcije statičkih podataka i dinamičkih podataka te razne sigurnosne mjere kontrole pristupa.

Deduplication - značajka integrirane deduplikacije smanjuje sigurnosno kopiranje uz uštedu na skladišnim i mrežnim resursima prepoznavanjem i uklanjanjem duplikata blokova podataka tijekom izrade sigurnosnih kopija.

Reporting and Insight – alat za analitičko izvještavanje koji pruža pregled i razumijevanje svih operacija te dubok uvid u podatke, zauzeća procesa, karakteristike okoline, poslovnu inteligenciju za planiranje troškova i pojednostavljenu reviziju usklađenosti. Pregledi instrumentacije i nadzorne ploče pružaju sažetke i analitičke prikaze korištenja, stope uspjeha i mnoštva drugih parametara dizajniranih za pojednostavljenje upravljanja podacima, dok su povijesni podaci o operacijama dostupni za redovito izvještavanje o statusu, analizu trendova i usporedbu najboljih praksi za postizanje operativne izvrsnosti.

Search – intuitivno sučelje za pretraživanje, unos, kategorizaciju i preuzimanje podataka. Pružena je mogućnost indeksiranja i pretraživanja podataka u repozitorijima koji sadrže

elektronički pohranjene podatke kroz operativne sustave, arhive i medije pohranjene na centraliziranim korporativnim poslužiteljima, dijeljenim mapama i korisničkim računalima.

Analytics - softver pruža analizu podataka za pregled statističkih podataka, web analitiku za poboljšanje upotrebljivosti i sadržaja web mjesta ili aplikacije te priključke za prikupljanje podataka koji se nalaze u različitim spremištima podataka.

Commvault Backup Appliance – kombinacija softvera Commvault sa sustavom za pohranu kojima se omogućava jednostavnost upotrebe, skalabilnost, fleksibilnost i upravljanje sigurnosnim kopijama.

Replication - moguće je replicirati podatke s jednog računala na drugi u stvarnom vremenu što omogućava minimalni ispad sustava. Ukoliko padne sustav na produkcijskom poslužitelju, potrebno je jako kratko vrijeme za da se aktivira replika. Glavna značajka ove funkcionalnosti jest „*ContinousDataReplicator*“ (CDR) koji zapisuje sve log datoteke s izvornog na destinacijsko računalo.

Disaster Recovery - softver sadrži integriranu platformu za koja olakšava postupke oporavka i pojednostavljuje kontinuitet poslovanja. U sklopu ove funkcionalnosti uspostavljene su odgovarajuće strategije postupke oporavka u slučaju katastrofe:

- Integrirana deduplikacija u operacije zaštite podataka u svrhu smanjenja količine podataka koji se trebaju oporaviti ako dođe do katastrofe.
- Smanjivanje troškova oporavka od katastrofe i smanjenje vremena oporavka pomoću „*DASH Copy*“ za učinkovito i brzo kopiranje dupliciranih sigurnosnih kopija na rezervne lokacije ili na oblak.
- Integrirana replikacija produkcijskih podataka na rezervnu lokaciju.
- Integracija spremišta u oblaku za oporavak od katastrofe
- „*Virtualize Me*“ alat za brzo testiranje scenarija oporavka od katastrofe virtualne infrastrukture.
- „*Live Sync*“ mogućnost stvaranja i održavanja toplih web lokacija za oporavak virtualnih strojeva koji pokreću kritične poslovne aplikacije.

Cloud Services – skup rješenja za upravljanje i nadzor podataka u oblaku.

Solutions – jedinstvena kastomizirana platforma za upravljanje podacima.

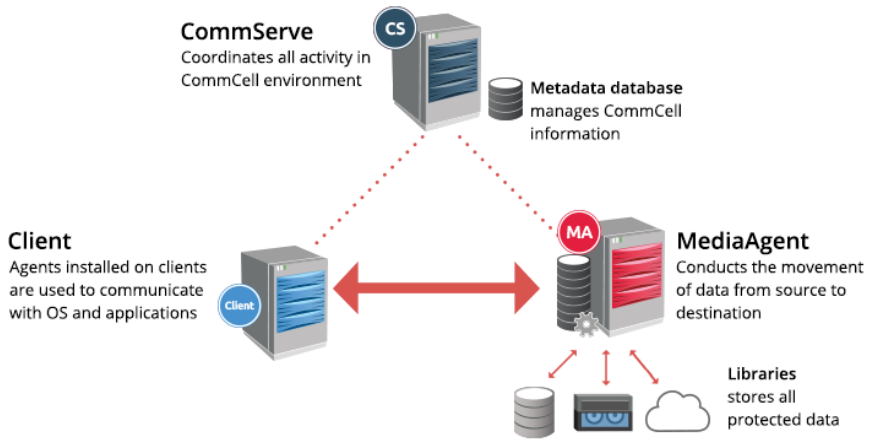
Poslužiteljsko okruženje aplikacije naziva se CommCell i sastoji se od logički grupiranih softverskih komponenti koji štite, premještaju, pohranjuju te upravljaju podacima i informacijama. CommCell okruženje se sastoji od jednog CommServe poslužitelja, jednog ili više MediaAgents te jednog ili više klijenata.

CommServe poslužitelj je središnja upravljačka komponenta CommCell okruženja koja koordinira i izvršava sve CommCell operacije, održavajući Microsoft SQL Server baze podataka koje sadrže svu konfiguraciju, sigurnost i operacijsku povijest okruženja.

MediaAgent je upravitelj prijenosa i distribucije podataka u CommCell okruženju. Omogućuje kretanje podataka uz visoke performanse i upravljanja knjižnicama za pohranu podataka.

Client je logičko grupiranje softverskih agenata instaliranih na računalima koji olakšavaju zaštitu, upravljanje i prijenose podataka povezanih s klijentom. Služi za komunikaciju s lokalnim operacijskim sustavom, aplikacijama i podacima.

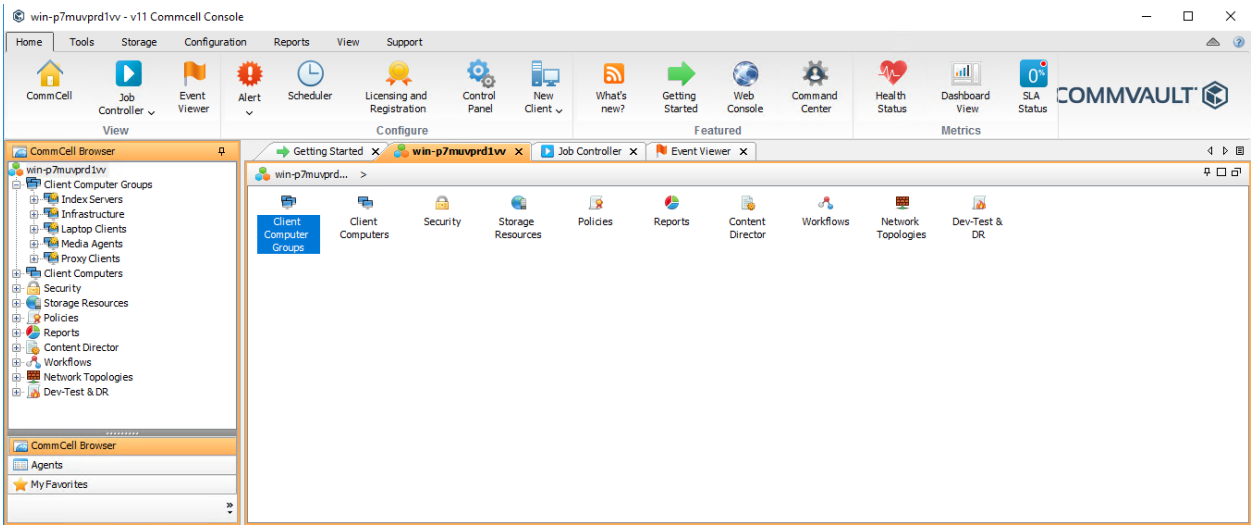
Slika 26. Glavne komponente CommCell okruženja



Izvor: commvault.com

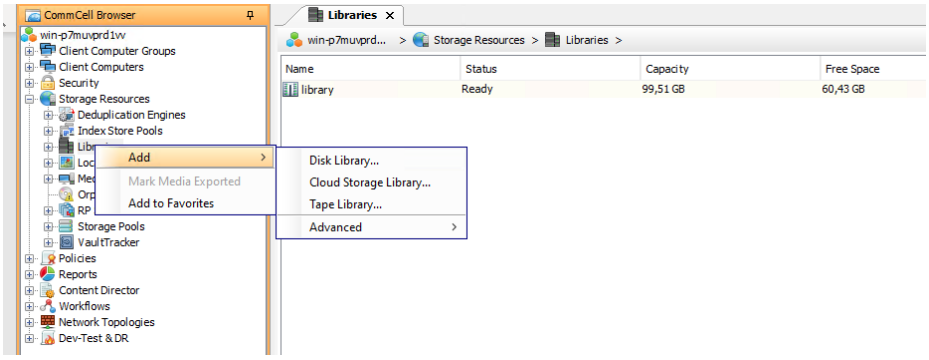
Na slici niže je prikazana početna stranica upravljačke konzole CommCell Console. To je centralno upravljačko korisničko sučelje za upravljanje CommCell okruženjem. Preko ovog sučelja se pokreću, kontroliraju, nadgledaju i upravljaju sve aktivnosti.

Slika 27. Upravljačka konzola CommCell Console



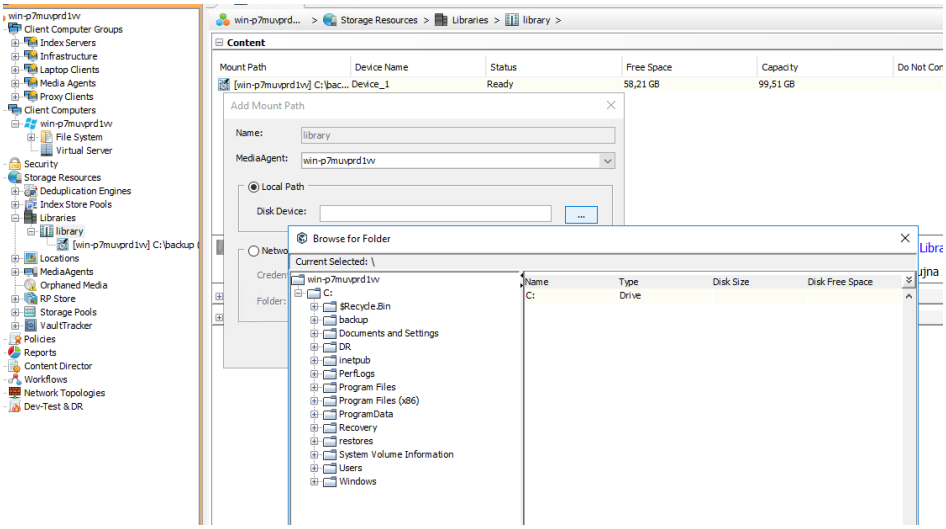
Za konfiguriranje sigurnosnog kopiranja prvo je potrebno dodati uređaj na koji će se pohranjivati kopirani objekti. U pretraživaču CommCell potrebno je kliknuti na „*Storage Resources*“, zatim desni klik na „*Libraries*“, pa „*Add*“ i odabrati željenu destinaciju pohrane. Moguće je izabrati između pohrane na disk, na traku te u oblaku.

Slika 28. Dodavanje knjižnice za pohranu podataka



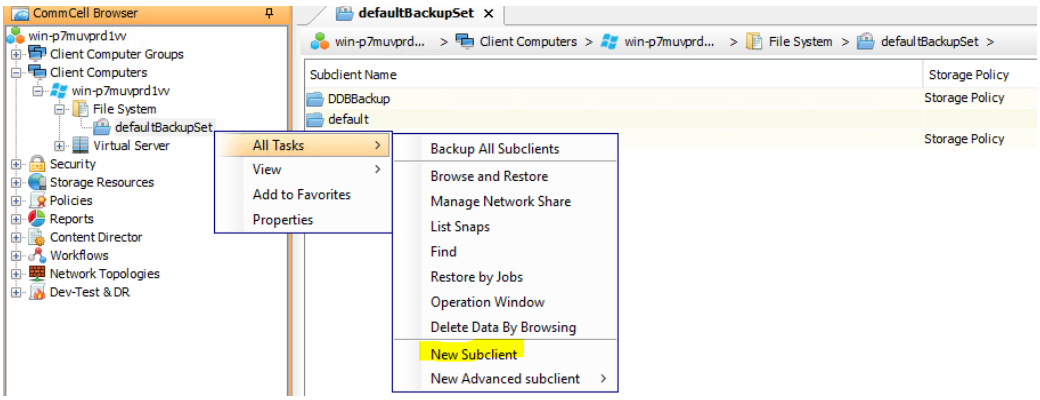
Klikom na *„Disk Library…“* otvara se novi prozor u kojem se konfiguriraju postavke knjižnice poput imena, MediaAgenta, te putanje do mape u koju će se spremati sigurnosne kopije. Moguće je odabrati disk na lokalnom serveru ili disk na serveru povezanim mrežom.

Slika 29. Konfiguriranje destinacijske mape za sigurnosne kopije



Nakon što je dodan disk za pohranu sigurnosnih kopija, slijedi kreiranje subclienta. To je logički spremnik u kojem je grupiran sadržaj sigurnosne kopije. Procedura stvaranja subclienta je sljedeća: (i) u CommCell pretraživaču proširiti „*Client Computers*“; (ii) zatim lokalnog klijenta „*win-p7muvprd1vv*“; (iii) pa „*File System*“; i (iv) desni klik na „*defaultBackupSet*“.

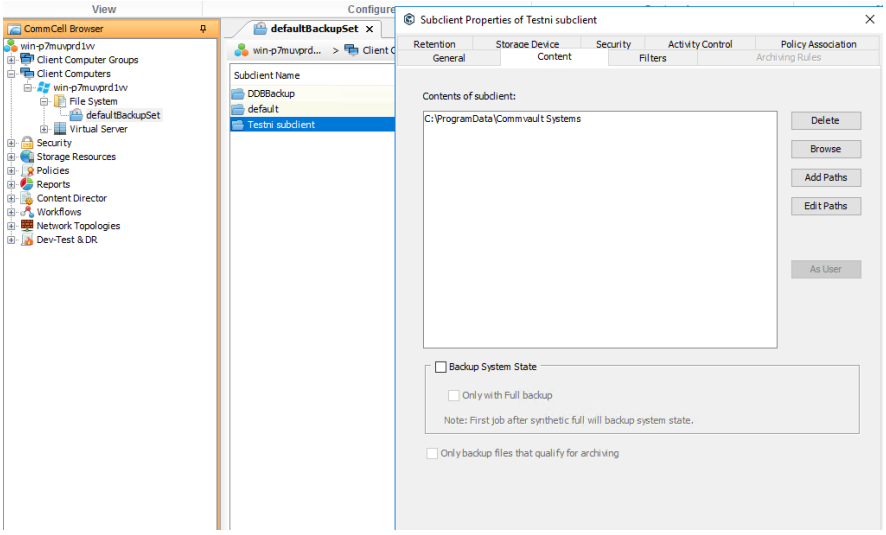
Slika 30. Kreiranje subclienta



Zatim je potrebno kliknuti na „*All Tasks*“ i u novom padajućem izborniku odabrati „*New Subclient*“. Nakon toga se otvara prozor za konfiguraciju postavki novog subclienta. U kartici „*Content*“ se odabire od kojeg sadržaja želimo napraviti sigurnosnu kopiju. Osim toga moguće je

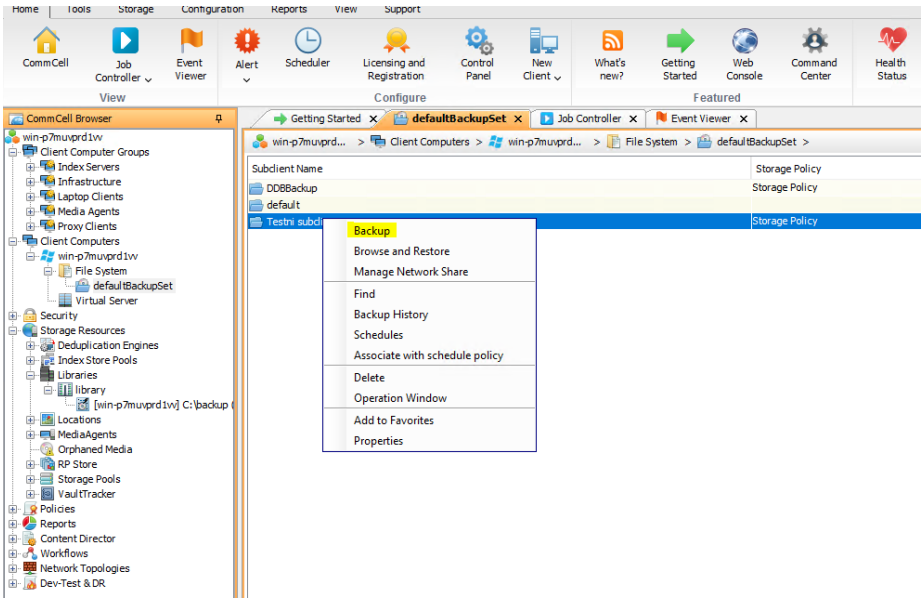
recimo urediti pravila kopiranja u kartici „*Retention*“, u kartici „*General*“ dati naziv subclientu, u kartici „*Storage Device*“ postaviti specifičnu destinaciju kopije i slično.

Slika 31. Postavke subclienta



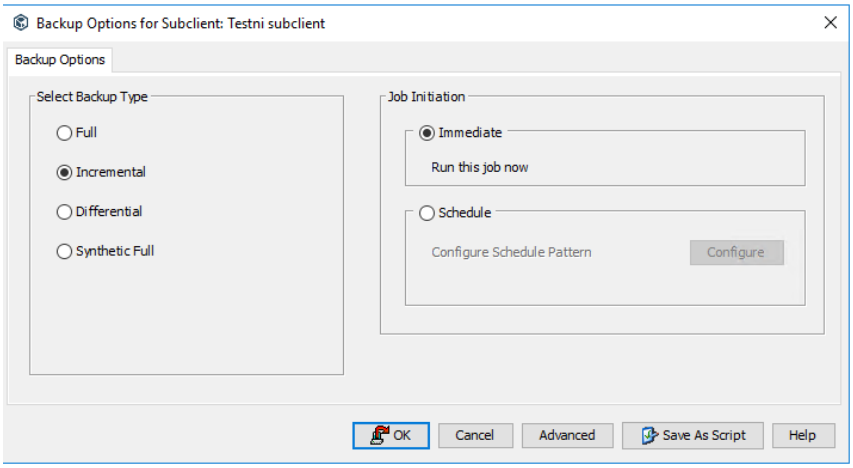
Nakon što je kreiran konfigurirano mjesto pohrane kopije i sadržaj za kopiranje, može se pokrenuti posao sigurnosnog kopiranja.

Slika 32. Pokretanje sigurnosnog kopiranja



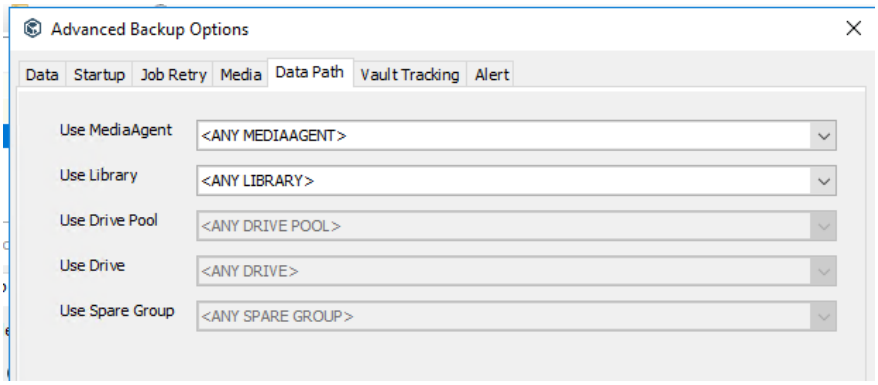
Desnim klikom miša na kreirani subclient, u ovom slučaju „*Testni subclient*“, otvara se padajući izbornik u kojem treba odabrati „*Backup*“. Zatim se otvara novi prozor u kojem se odabire vrsta sigurnosne kopije i postavlja vrijeme izvršavanja zadatka. Moguće je birati između 4 vrste backupa: „*Full*“ (potpuni backup), „*Incremential*“ (backup samo promijenjenih podataka od zadnjeg backupa), „*Differential*“ (slično inkrementalnom) i „*Synthetic Full*“ (konsolidiranje potpunog i inkrementalnog backupa).

Slika 33. Odabir vrste backupa



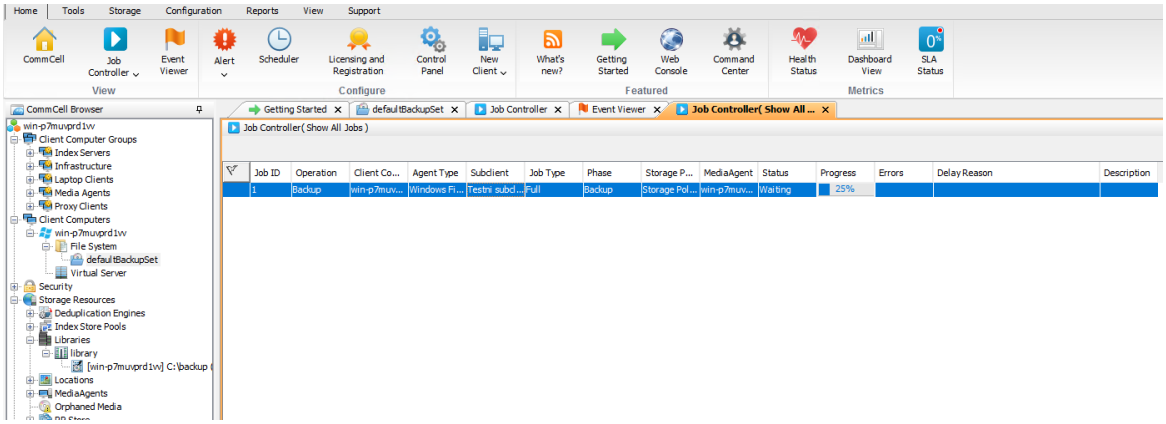
Također je moguće odrediti vrijeme izvršavanja zadatka sigurnosnog kopiranja. Klikom na „*Advanced*“ moguće je konfigurirati dodatne postavke sigurnosnog kopiranja. Tako se može promijeniti MediaAgent i knjižnica za pohranu kopije.

Slika 34. Dodatna konfiguracija backupa



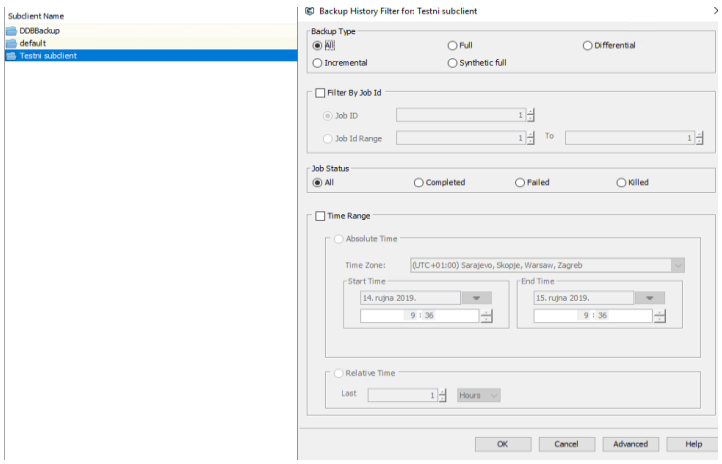
Ukoliko smo postavili da je vrijeme izvršavanja zadatka „*Immediate*“, klikom na „*OK*“ pokreće se zadatak. Moguće je pratiti izvršavanje zadatka ukoliko kliknemo na „*Job Controller*“ na gornjoj izbornoj traci na konzoli.

Slika 35. Praćenje backup joba



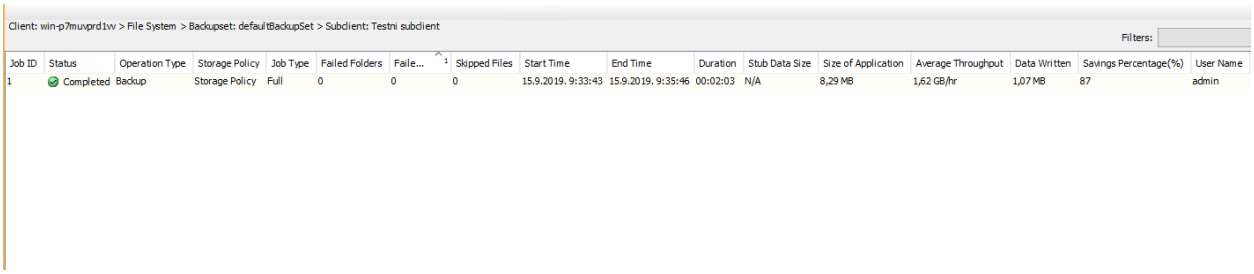
Odabirom „*Job Controller*“ otvara se nova kartica u kojoj je prikazana vrsta operacije, klijent, vrsta agenta, subclient, podvrsta operacije, stanje zadatka i drugi detalji o zadatku.
Također je moguće vidjeti povijest o izvršenim backup poslovima. Potrebno je stisnuti desnim klikom miša na subclienta kojem se želi vidjeti povijest izvršenja backupa te zatim u padajućem izbornika odabrati „*Backup History*“. Tada se otvara novi prozor u kojem se mogu filtrirati prošli backupi na temelju vrste backupa i krajnjeg statusa.

Slika 36. Prikaz povijesti backupa



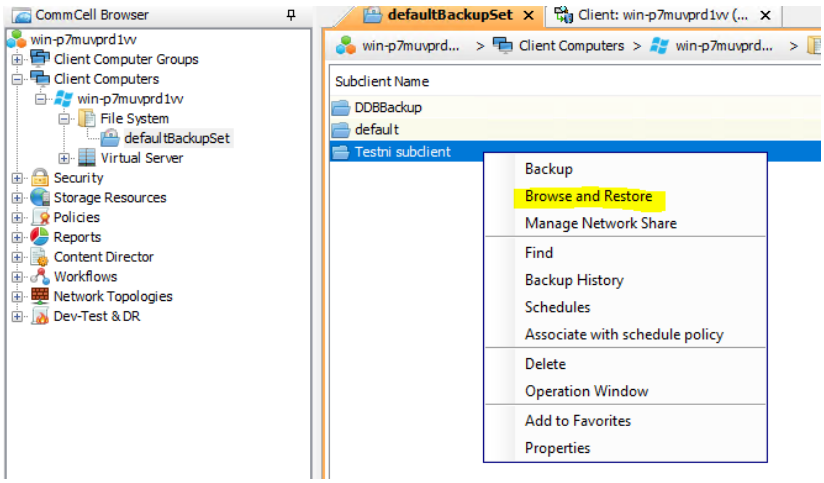
Niže je prikazan pregled izvršenih backup zadataka. Ovo daje mnoge informacije o poslu sigurnosnog kopiranja poput vrste, pogrešaka tijekom kopiranja, početnog i završnog vremena, trajanja, veličine sigurnosne kopije itd.

Slika 37. Povijesni pregled backup zadataka



Operacija povrata podataka „*Restore*“ druga je ključna funkcionalnost ove aplikacije. Za izvršenje povrata sigurnosno kopiranih podataka potrebno kao i kod backupiranja otvoriti padajući izbornik na željeni subclient koji želimo povratiti i zatim odabrati „*Browse and Restore*“.

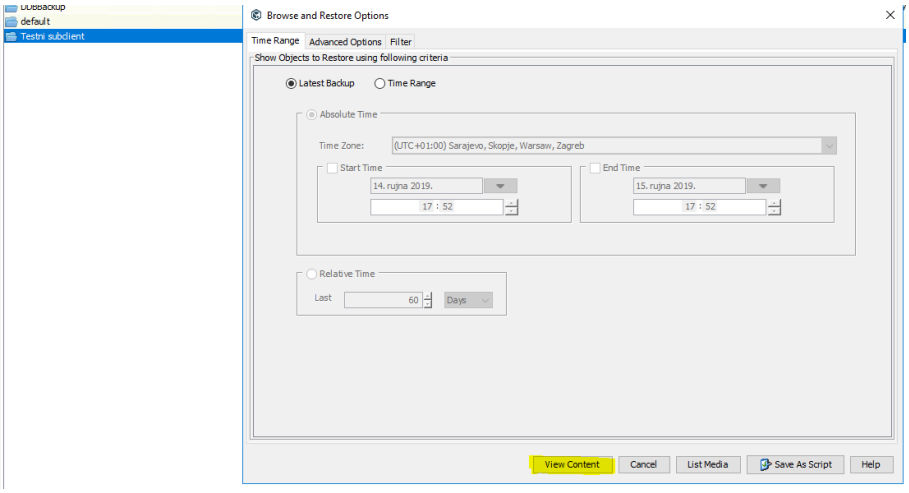
Slika 38. Pokretanje povrata podataka



Nakon toga se otvara novi prozor gdje se odabiru postavke povrata. Klikom na „*View Content*“ mogu se vidjeti sigurnosne kopije unutar odabranog subclienta i odabrati željene za povrat. U postavkama je moguće odabrati vremensku točku povrata i to posljednji backup te prošle

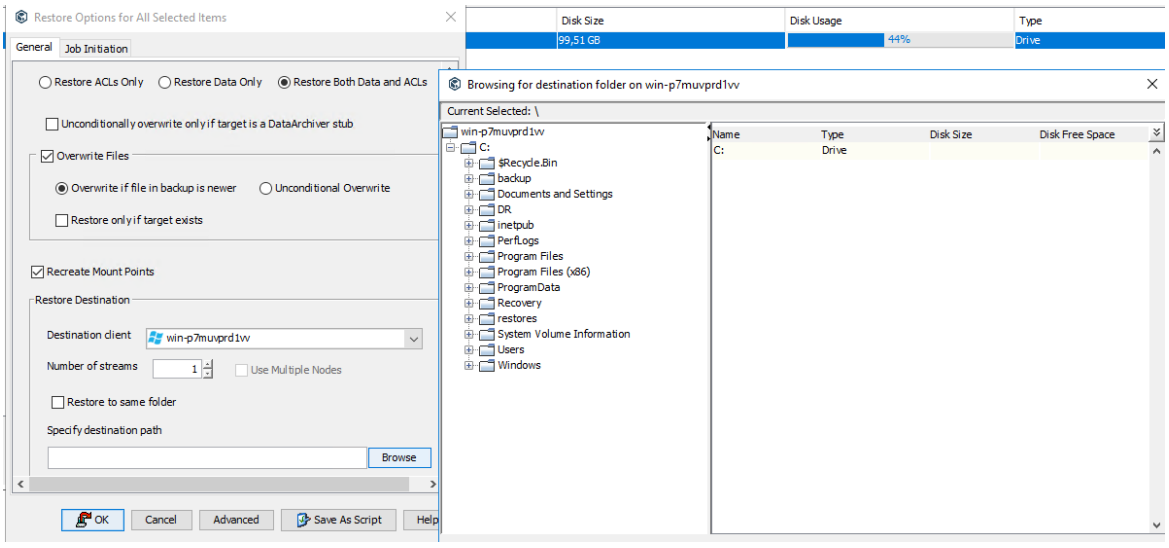
backupe odabirom relativne (npr. zadnja 3 dana) i apsolutne vremenske točke (npr. od 13.9. – 15.9.2019.).

Slika 39. Odabir vremenske točke i sadržaja za povrat



Moguće je odabrati povrat samo kontrolnih lista, povrat podataka i oboje. Dodatna opcija je pisanje preko već postojećih datoteka („*Overwrite Files*“). Pod „*Restore Destination*“ se odabire klijent na koji želimo povratiti sigurnosnu kopiju podataka. Klikom na „*Browse*“ otvara se novi prozor i odabire mapa u koju želimo spremiti podatke.

Slika 40. Postavke povrata podataka



Pod karticom „*Job Initiation*“ se konfigurira vrijeme izvršavanja zadatka povrata. Također kao i kod backupa, moguće je konfigurirati dodatne postavke klikom na „*Advanced*“. Odabirom „OK“ pokreće se posao povrata podataka. Poslovi koji se trenutno vrše mogu se vidjeti unutar opcije „*Job Controller*“ kao što prikazano prije. Također se povijest povrata može vidjeti kao i kod backupa, klikom na željeni subclient i zatim „*Restore History*“

5.4. Usporedba Veema i Commvaulta

U nastavku će biti prikazana komparacija značajki koje sadrže dvije aplikacije te ću se zatim osvrnuti na osobno korisničko iskustvo korištenja aplikacija

Tablica 7. Usporedba značajki unutar funkcionalnosti izrade sigurnosne kopije

Karakteristike	**Veeam Backup and Replication**	**Commvault Complete Backup and Recovery**
Izrada kopije fizičke, virtualne i okoline u oblaku	√√	√√
Izrada kopije u snimku	√√	√√
Izrada kopije na fizičke trake	√√	√√
Testiranje backupa i povrata	√√	√√
Središnja upravljača konzola za upravljanje	√√	√√
Application aware proccesing	√√	√√
Deduplikacija i kompresija podataka	√√	√√
Jedinstveni repozitorij za upravljanje kopijama lokalno i u oblaku	√√	√√
Izrada kopije i spremanje offsite na oblak	√√	√√
Arhiviranje podataka		√√

Može se uočiti da obje aplikacije imaju gotovo podjednake mogućnosti unutar sustava izrade sigurnosnih kopija, što i objašnjava zašto su lideri na tržištu tog segmenta. Jedina dodatna mogućnost koji nudi Commvaultov softver u odnosu na Veeamov jest postupak arhiviranja i pohrane podataka.

Tablica 8. Usporedba značajki replikacije

Karakteristike	Veeam Backup and Replication	Commvault Complete Backup and Recovery
Replikacija onsite	√√	√√
Replikacija offsite	√√	
Testiranje i verifikacija replike za povrat	√√	
Povrat replike i prebacivanje servisa s minimalnim prekidom	√√	√√

Prema tablici usporedbe značajki replikacije, Veeamov softver nudi više funkcionalnosti za repliciranje podataka i strojeva. Omogućena je izrada i pohrana replike offsite na lokaciju van infrastrukture organizacije. Također je moguće napraviti testiranje i verifikaciju povrata repliciranog virtualnog stroja u operativno stanje.

Tablica 9. Usporedba značajki oporavka

Karakteristike	Veeam Backup and Replication	Commvault Complete Backup and Recovery
Povrat datoteka, aplikacija i operacijskih sustava	√√	√√
Instant povrat stroja iz kopije uz RTO 2 minute	√√	
Prenosivost kopije na oblak i povrat iz oblaka	√√	√√
Povrat s dodatnim sigurnosnim mjerama	√√	√√
Povrat iz AD-a, Exchangea i Sharepointa	√√	√√
Povrat baza MS SQL i Oracle SQL Servera	√√	√√
Povrat iz snimke	√√	√√
Povrat baza MySQL, PostgreSQL, SAP, DB2		√√
Održavanje tople lokacije za oporavak VM-ova		√√

Tablica 8. nudi pregled mogućnosti aplikacije kod oporavka podataka, aplikacija i računala. Obje aplikacije imaju mogućnost povrata podatkovnog sustava i aplikacija, povrata iz oblaka, povrata specifičnih objekata poput email servera Exchange, platforme Sharepoint i Active Directoryja. Prednost aplikacije Veeam je što ima mogućnost instant povrata virtualnih strojeva

uz veoma kratak RTO od samo 2 minute. Dok s druge strane aplikacija Commvault pruža širi opseg sustava za upravljanje bazama podataka koje može oporaviti poput MySQL, PostgreSQL i DB2. Također moguće je konfigurirati „*Warm site*“ za brzi povrat virtualnih strojeva uz minimalan ispad.

Što se osobnog korisničkog iskustva u korištenju ovih aplikacija, prednost bi dao aplikaciji Veeam Backup and Recovery zbog više razloga. Prvo lošije iskustvo s aplikacijom Commvault je bilo pokretanje aplikacije nakon instalacije. Čak i za besplatnu verziju je potrebno prvo konfigurirati certifikate unutar web poslužitelja, zatim preko web sučelja se registrirati i tek onda je bilo moguće pokrenuti aplikaciju. I tu je također bilo problema jer se aplikacija ponekad ne želi pokrenuti jer teško održava sesiju sa serverom na kojem je hostirana. Veeamova aplikacija je imala poprilično jednostavno i brzo iskustvo instalacije i inicijalnog pokretanja. Zatim korisničko sučelje Veeamove aplikacije je veoma intuitivno, pregledno i jednostavno za snalaženje, dok rješenje Commvault ima malo zastario izgled i nepreglednu konzolu za upravljanje. Sljedeća veća razlika u korisničkom iskustvu jest proces izrade sigurnosne kopije i izrade zadatka za oporavak. U aplikaciji Commvault prvo je potrebno kreirati i konfigurirati knjižnicu pohrane odnosno mjesto pohrane za kopije te nakon toga odrediti sadržaj koji želimo backupirati. Zatim slijedi izrada kopije na način odaberemo objekt u kojem se nalazi sadržaj za kopiranje. Kod Veeama je ovaj proces puno jednostavniji jer izbacuje prva dva nepotrebna koraka pošto se željeni sadržaj backupa i destinacija pohrane konfigurira „u hodu“. Ujedno aplikacija Veeam unutar svog sučelja nudi dodatna pojašnjena mogućnosti. Također velika prednost Veeamu je dostupan opširni korisnički vodič koji se može preuzeti na njihovoj web stranici. Vodič ima čak 1100 stranica i nudi detaljan uvid u sve mogućnosti aplikacije i upute za rad. Commvault ima internetsku dokumentaciju, no uz jako malo pomoćnih uputa za aplikaciju.

6. ZAKLJUČAK

Planiranje kontinuiteta poslovanja je kompleksan i složen proces koji zahtijeva napore svih jedinica organizacije s potencijalno upitnim rezultatima. Ukoliko je organizacija velika i složena, trošak uspostave neprekidnosti poslovanja može doseći ogromne brojke. Na prvi pogled može biti jednostavnije ne činiti ništa po tom pitanju i samo se nadati da organizacija neće doživjeti katastrofalni događaj. No, krize i neželjeni događaji su neizbježni u današnjem vremena i samo je pitanje vremena kada će i koliko snažno pogoditi organizaciju. Zato je nužno planirati poslovni kontinuitet i prilagoditi ga veličini, budžetu i drugim ograničenjima. Također upravljanje kontinuitetom poslovanja ne donosi samo neprekidnost poslovnih operacija te brz i efikasan oporavak od poremećaja. Ovaj kružni proces zapravo daje duboki uvid u poslovne procese i njihove slabe točke, te omogućava bolje razumijevanje organizacije, njenih unutarnjih i vanjskih prijetnji, te svakodnevnih rizika.

Može se reći da sveobuhvatan i kvalitetan plan kontinuiteta poslovanja čini konkurentsku prednost organizacije. Organizacije s implementiranim planovima mogu iskoristiti poremećaje na razini industrije za ostvarivanje većeg tržišnog udjela, jačanje ugleda i imidža u javnosti, među interesno utjecajnim skupinama i iskazati se kao subjekt koji efikasno i efektivno upravlja svim poslovnim izazovima, posebice krizama. Ovaj rad daje jedan takav okvir.

U skladu s predmetom rada predstavljene su aplikacije koje podupiru koncept upravljanja kontinuiteta poslovanja i oporavka od katastrofalnih događaja. Poznata je činjenica da nijedan informacijski sustav nije 100% siguran, pa tako ni procesi, aplikacije i podaci unutar organizacijske infrastrukture. Zato je nužno implementirati softverska rješenja za upravljanje sigurnosnim kopijama, replikacijama i oporavkom od nepogode kako bi se uspješno ovladavali poremećaji u poslovanju jednom kada se jave.

POPIS LITERATURE

1. Barnes, J. C. (2001) *A Guide to Business Continuity Planning*. Chichester: John Wiley & Sons, Ltd.
2. Bates, W. i Von Opstal, D. (2007) *Five for the Future*. Washington, D.C.: Council on Competitivenes. [online]. Dostupno na: http://quoniam.info/competitive-intelligence/PDF/ebooks/Five_Final_8858COC.pdf
3. CARNet CERT (2010) Upravljanje kontinuitetom poslovnih procesa [online] www.cis.hr. Dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-15-307.pdf
4. Commvault [online]. www.commwault.com. Dostupno na https://www.commvault.com/
5. De Guise, P. (2008) *Enterpise Systems Backup and Recovery: A Corporate Insurance Policy*. Boca Raton, FL: CRC Press.
6. *Disaster Recovery Plan (DRP)* [online]. Techopedia.com. Dostupno na: https://www.techopedia.com/definition/1074/disaster-recovery-plan-drp
7. Fulmer, K. L. (2005) *Business Continuity Planning: A Step-by-Step Guide with Planning Forms, Third Edition*. Brookfield, CT: Rothstein Associates Inc.
8. Gallagher, M. (2003) *Business Continuity Management: How to Protect Your Company from Danger*. Harlow: Pearson Education Limited.
9. Hiles, A. (2007*) The Definitive Handbook of Business Continuity Management.* Chichester: John Wiley & Sons, Ltd.
10. *Introduction to Business Continuity* [online]. Thebci.org. Dostupno na: https://www.thebci.org/knowledge/introduction-to-business-continuity.html
11. Marinović, D. (2017) *Uspostava neprekinutosti poslovanja, temeljem analize utjecaja na poslovanje*. Završni specijalistički rad. Zagreb: Fakultet strojarstva i brodogradnje
12. NIST Special Publication 800-12, Revision 1 (2017) *An Introduction to Information Security*. Gaithersburg, Maryland: National Institute of Standards and Technology. [online]. Dostupno na: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf
13. NIST Special Publication 800-34, Revision 1 (2010) *Contigency Planning Guide for Federal Information Systems*. Gaithersburg, Maryland: National Institute of Standards and Technology.

[online]. Dostupno na: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

14. NIST Special Publication 800-39 (2011) *Managing Information Security Risk*. Gaithersburg, Maryland: National Institute of Standards and Technology. [online]. Dostupno na: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf
15. Omar, A., Alijani, D. i Roosevelt, M. (2011) Information Technology Disaster Recovery Plan: Case Study. *Academy of Strategic Management Journal*, 10 (2), str. 127-142
16. Panian, Ž. i Strugar, I. (2013) *Informatizacija poslovanja*. Zagreb: Ekonomski fakultet.
17. Panian, Ž., Spremić, M. i suradnici (2007) *Korporativno upravljanje i revizija informacijskih sustava*. Zagreb: Zgombić i partneri.
18. Parsons, D. (2010) Organizational Resilience. *The Australian Journal of Emergency Management*, 25 (2), str. 18-20
19. Partio, A. (2017) *Data center Disaster Recovery & Major Incident Management*. Master's Thesis in Information and Communications Technology. Lahti: University of Applied Sciences.
20. Ransome, J. F. i Rittinghouse, J. W. (2005) *Business Continuity and Disaster Recovery for InfoSec Managers*. Burlington, MA: Elsevier Digital Press.
21. Reuvid, J. (2005) *The Secure Online Business Handbook: e-commerce, IT functionality & business continuity*. London i Sterling, VA: Kogan Page Limited.
22. Snedaker, S. (2007) *Business Continuity & Disaster Recovery for IT Professionals.* Burlington, MA: Syngress Publishing.
23. Spremić, M. (2017) *Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije*. Zagreb: Ekonomski fakultet.
24. Tijan, E., Kos., S. i Ogrizović, D. (2009) Disaster recovery and business continuity in port community systems. *Pomorstvo*, 23 (1), str. 243-260
25. Tomić Rotim, S. i Komnenić, V. (2017) Kako pripremiti sveobuhvatan plan kontinuiteta poslovanja? U: I. Nađ, ur. *Zbornik radova 10. Međunarodne znanstveno-stručne konferencije: Dani kriznog upravljanja. 24-26 studeni 2017, Terme Tuhelj, Hrvatska*. Velika Gorica: Veleučilište Velika Gorica, str. 475-489.
26. Udovičić, A., Kadlec, Ž. (2013) Analiza rizika upravljanja poduzećem. *Praktični menadžment*, 4(1), str. 50-60

27. Valenčić, D., Ćavar, I. i Lebinac, V. (2012) Provedba oporavka od katastrofe u računalstvu u oblaku. *Zbornik radova 5. Međunarodne konferencije: Dani kriznog upravljanja. 24-25 svibnja 2012, Velika* Gorica*, Hrvatska*. Veleučilište Velika Gorica, str. 674-692
28. Varga, M., Strugar, I., Pejić Bach, M., Srića, V., Spremić, M., Bosilj Vukšić, V., Ćurko, K., Vlahović, N., Milanović Glavan, Lj., Zoroja, J. i Jaković B. (2016) *Informacijski sustavi u poslovanju*. Zagreb: Ekonomski fakultet
29. Vašak, J. (2017) *Analysis of Backup for Small and Medium-sized Enterprises (SME) in the Czech Republic*. Master's thesis. Prague: Faculty of Information Technology.
30. Veeam [online]. www.veeam.com. Dostupno na: https://www.veeam.com/
31. Wallace, M. i Webber, L. (2004) *The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities and Assets*. New York, NY: AMACO

POPIS SLIKA

Slika 1. Ciklus poslovnog kontinuiteta

Slika 2. Interdisciplinarni proces upravljanja kontinuitetom poslovanja

Slika 3. Ciklus upravljanja kontinuitetom poslovanja

Slika 4. Elementi plana kontinuiteta poslovanja i plana oporavka od katastrofe

Slika 5. Dijelovi upravljanja kontinuitetom poslovanja

Slika 6. Koraci u planiranju poslovnog kontinuiteta

Slika 7. Vrste prirodnih katastrofa

Slika 8. Ciklus upravljanja rizicima

Slika 9. Proces upravljanja rizicima

Slika 10. Pregled procesa upravljanja rizicima

Slika 11. Matrica vrednovanja rizika

Slika 12. Prikaz zadnje faze u procjeni rizika

Slika 13. BIA dijagram

Slika 14. Faze procesa oporavka

U ovoj fazi upravljanja kontinuitetom poslovanja aktivnosti su povezane, kao što je prikazano na slici poviše. Ukoliko se provodi ispitivanje plana, tada se u jednu ruku i uvježbava zaposlenike u slučaju neželjenog događaj a zatim se rezultatom testiranja dolazi do eventualnih slabijih područja plana koje je potrebno revidirati i prilagoditi.

Slika 15. Veza između uvježbavanja, testiranja i revizije

Slika 16. Proces održavanja i ažuriranja plana

Slika 17. Prikaz upravljačke konzole Veeam Backup and Recovery aplikacije

Slika 18. Odabir objekta za sigurnosno kopiranje

Slika 19. Novi zadatak za izradu sigurnosne kopije

Slika 20. Primjer izvršenog zadatka sigurnosnog kopiranja

Slika 21. Primjer izvještaja o uspješno provedenom backupu

Slika 22. Novi zadatak za izradu replike

Slika 23. Povrat željenog objekta
Slika 24. Potpuni povrat virtualnog stroja
Slika 25. Odabir vremenske točke oporavka
Slika 26. Glavne komponente CommCell okruženja
Slika 27. Upravljačka konzola CommCell Console
Slika 28. Dodavanje knjižnice za pohranu podataka
Slika 29. Konfiguriranje destinacijske mape za sigurnosne kopije
Slika 30. Kreiranje subclienta
Slika 31. Postavke subclienta
Slika 32. Pokretanje sigurnosnog kopiranja
Slika 33. Odabir vrste backupa
Slika 34. Dodatna konfiguracija backupa
Slika 35. Praćenje backup joba
Slika 36. Prikaz povijesti backupa
Slika 37. Povijesni pregled backup zadataka
Slika 38. Pokretanje povrata podataka
Slika 39. Odabir vremenske točke i sadržaja za povrat
Slika 40. Postavke povrata podataka

POPIS TABLICA

Tablica 1. Vrste planova unutar procesa upravljanja kontinuitetom poslovanja
Tablica 2. Vrste kontrolnih mjera
Tablica 3. Izvori rizika
Tablica 4. Tri osnovne stavke analize utjecaja na poslovanje
Tablica 5. Kategorije testne provjere plana
Tablica 6. Usporedba vrsta sigurnosnih kopija
Tablica 7. Usporedba značajki unutar funkcionalnosti izrade sigurnosne kopije
Tablica 8. Usporedba značajki replikacije
Tablica 9. Usporedba značajki oporavka

ŽIVOTOPIS

europass Životopis

OSOBNE INFORMACIJE

Radić Ivan

Sokolgradska 73, 10000 Zagreb (Hrvatska)

(+385) 99 402 7166

ivanradic0401@gmail.com

RADNO ISKUSTVO

01/09/2018–danas — Junior sistem inženjer

IN2, Zagreb (Hrvatska)

- Održavanje informatičke infrastrukture Windows okruženja
- prijedlog i implementacija infrastrukturnih rješenja
- dokumentiranje informacijskih sustava
- komunikacija s korisnicima i rješavanje problema

01/05/2018–01/09/2018 — Praktikant

IN2, Zagreb (Hrvatska)

IT helpdesk

Administracija informacijskog sustava

01/06/2011–01/10/2016 — Studentski poslovi

- sezonski ljetni poslovi u turizmu i ugostiteljstvu

01/07/2008–01/09/2011 — Prakse u hotelima i turističkim agencijama

Dubrovnik (Hrvatska)

- Ljetne prakse na recepcijama hotela s 5 zvjezdica i u turističkim agencijama

OBRAZOVANJE I OSPOSOBLJAVANJE

01/10/2018–danas — Magistar ekonomije

Ekonomski fakultet, Zagreb (Hrvatska)

01/10/2012–01/07/2018 — Sveučilišni prvostupnik ekonomije

Ekonomski fakultet, Zagreb (Hrvatska)

01/09/2008–01/06/2012

Turistička i ugostiteljska škola Dubrovnik, Dubrovnik (Hrvatska)

OSOBNE VJEŠTINE

Materinski jezik: hrvatski

Strani jezici

RAZUMIJEVANJE		GOVOR		PISANJE
Slušanje	Čitanje	Govorna interakcija	Govorna produkcija	

engleski	C2	C2	B2	B2	C1
njemački	A2	A2	A2	A2	A2
talijanski	A2	A2	A2	A2	A2

Stupnjevi: A1 i A2: Početnik - B1 i B2: Samostalni korisnik - C1 i C2: Iskusni korisnik
Zajednički europski referentni okvir za jezike

Komunikacijske vještine

Vrsne komunikacijske vještine stečene kroz dugogodišnje iskustvo na sezonskim poslovima u turizmu i ugostiteljstvu, te kroz upravljanje privatnim obiteljskim smještajnim jedinicama

Organizacijske / rukoviteljske vještine

Vještine organiziranja sam stekao kroz obrazovanje (vođenje timova kolega), radno iskustvo i vođenje obiteljskog biznisa

Digitalne vještine

SAMOPROCJENA				
Obrada informacija	Komunikacija	Stvaranje sadržaja	Sigurnost	Rješavanje problema
Iskusni korisnik	Iskusni korisnik	Samostalni korisnik	Iskusni korisnik	Iskusni korisnik

Digitalne vještine - Tablica za samoprocjenu

- MS Office - izvrsno poznavanje
- Windows tehnologije - napredno znanje
- Linux - osnovno znanje
- Veeam - napredno znanje
- Routing & Switching (Cisco)
- Administracija MS SQL - osnovno znanje
- Virtualna rješenja (Hyper-V i VMware) - napredno znanje

Vozačka dozvola

B