Nebojša Jeremić[1], Nemanja Jakovljević[2], Miloš Jeremić[3]

PREGLEDNI RAD
UDK: 657.6(497.11)
005.336
DOI: 10.56362/Rev2298053J

ULOGA INTERNE REVIZIJE U KONTINUITETU POSLOVANJA

UVOD

Upravljanje kontinuitetom poslovanja predstavlja suštinski kapacitet organizacije da održava svoje kritične, odnosno primarne poslovne usluge, kao i poslovne operacije i čitavu poslovnu infrastrukturu tako da su stalno dostupne i otporne na nastanak vanrednih okolnosti i situacija ili neprijateljskih događaja. Ovo zahteva uspostavljanje neophodnih okvira, politika, procedura i resursa za postizanje istih. Upravljanje oporavkom od katastrofe su akcije, procesi ili procedure koje usvaja organizacija da bi se efikasno oporavila od katastrofe ili neplaniranog prekida usluge u razumno definisanom periodu koji će imati minimalan uticaj na poslovanje i pružanje usluga. U nekim slučajevima, propisi i zakoni koji se primenjuju na određene industrije nalažu usvajanje mera koje će obezbediti kontinuitet osnovnih poslovnih usluga u slučaju poremećaja ili vanrednih situacija. Planovi oporavka od katastrofe su dokumentovane procedure oporavka od neprijateljskih događaja koji mogu da podrazumevaju i rutinska testiranja od strane zainteresovanih strana u pogledu njihove prikladnosti, izvodljivosti i otpornosti, kako bi se osiguralo da ostaju relevantni za poslovanje i efikasno oporavljaju date procese od katastrofe ili prekida usluge. Da bi se osigurala prikladnost i relevantnost sposobnosti organizacije za kontinuitet poslovanja i upravljanje oporavkom od katastrofe, svi procesi podložni predmetnom obuhvatu bi trebalo da budu predmet revizije, kako bi se zainteresovanim stranama pružila razumna sigurnost o njegovoj podobnosti za poslovanje. Brojni događaji širom sveta poput pandemije COVID-19, rata u Ukrajini i drugih, skreću pažnju na važnost i značaj kontinuiteta poslovanja. Naravno kako kontinuitet poslovanja postaje sve

REZIME

Cilj revizije kontinuiteta poslovanja je da se utvrde činjenične pojave radi odgovora na pitanje da li je plan kontinuiteta poslovanja delotvoran i da li je u skladu sa ciljevima organizacije. Predmet rada je ispitivanje važnosti i potrebe razmatranja kontinuiteta poslovanja na nivou entiteta, analiziranje sistema za upravljanje kontinuitetom poslovanja u regulatornom okviru Republike Srbije, odnosa funkcije interne revizije prema kontinuitetu poslovanja, razmatranje tehnika skeniranja u reviziji informacionih tehnologija posle katastrofa i analize kritičnih aplikacija informacionog sistema.

Ključne reči: interna revizija; kontinuitet poslovanja; rizici; katastrofe; oporavak.

[1] Viši interni revizor za finansije i računovodstvo, Telekom Srbija a.d. E-mail: nebojsaje@telekom.rs
[2] Student doktorskih studija Ekonomskog fakulteta Univerziteta u Beogradu. E-mail: jakovljevic.i.nemanja@gmail.com
[2] Diplomirani ekonomista i master pravnik. E-mail: milos.jeremic@rocketmail.com

značajniji, tako raste i želja za merenjem njegove efikasnosti, što dodatno ističe važnost funkcije interne revizije, koja, da bi ispunila ovu ulogu, mora da razume procese koji se odnose na kontinuitet poslovanja i da sprovodi redovne periodične revizorske angažmane na tu temu.

Rizici su po sopstvenoj prirodi nepredvidivi, a njihova jedina sigurna i prožimajuća karakteristika je da se pretnje i katastrofe povezane sa njima dešavaju uglavnom apsolutno nepredvidivo. Suštinski, svaki poslovni entitet koji posluje po tržišnom principu u skladu sa načelima konkurentnosti suočava se sa konstantnim svakodnevnim rizicima i pretnjama koji mogu da ugroze i naruše kontinuitet njegovog poslovanja. Brojni su primeri malih i velikih kompanija koje su nestale u relativno kratkom periodu jer su pretrpele neki neprijateljski sajber napad ili požar, poplavu i slično. Sa porastom popularnosti društvenih medija i sve većim oslanjanjem na informaciono-komunikacione tehnologije rizici po poslovanje su dobili osetniji uticaj u digitalnom obliku, a njihova neizvesnost i nepredvidivost je samim tim postala još veća. U tom kontekstu i reakcija na pojavu pretnji mora da bude brža i efikasnija, a funkcija interne revizije može značajno da doprinese tome. Revizija plana kontinuiteta poslovanja je suštinski formalizovana tehnika za procenu načina na koji se upravlja procesima koji su sastavni deo kontinuiteta poslovanja jednog poslovnog entiteta. Cilj ovakve vrste revizorskog angažmana je da se ispitaju i utvrde činjenične pojave kako bi se obezbedio tačan i jasan odgovor na pitanje da li je plan kontinuiteta poslovanja delotvoran i da li je u skladu sa ciljevima organizacije. Ona može da bude izvršena interno, od strane odeljenja interne revizije, i eksterno, uz pomoć nezavisne revizorske kompanije (4, 2). Njena ključna odrednica prilikom sprovođenja konkretnog revizorskog angažmana je njena objektivnost, koja je primarni ključ za razumevanje kontinuiteta poslovanja jednog poslovnog entiteta kao i za pregled i ažuriranje plana, što ukazuje na to da bi nezavisna revizorska kompanija mogla da bude pozvanija da realizuje reviziju kontinuiteta poslovanja. Međutim, višegodišnja praksa je pokazala suprotno jer odeljenja interne revizije uglavnom poseduju kapacitete da bolje razumeju organizacione procese, pa samim tim i proces planiranja kontinuiteta poslovanja (10, 6).

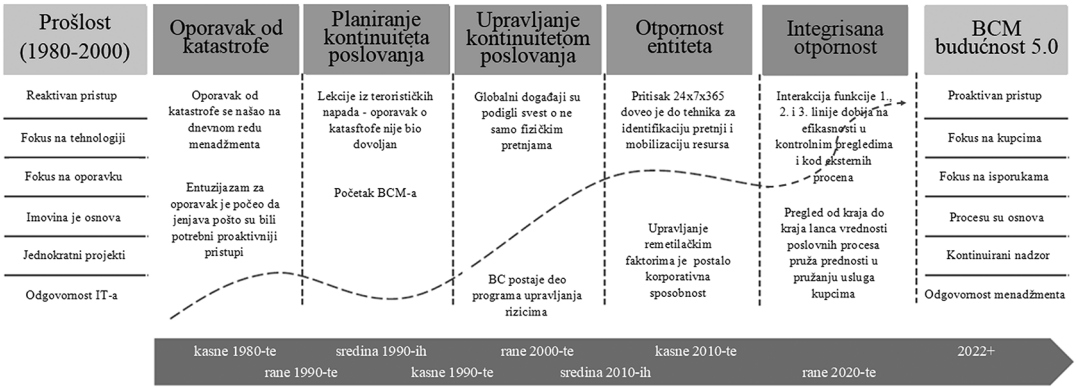
Iako kontinuitet poslovanja na mnogo načina može da bude složen i komplikovan, on zapravo nije tehnička ili naučna disciplina u poređenju sa kontrolom kvaliteta ili sa informacionom bezbednošću (14, 7). Revizorima su potrebne fiksne referentne tačke za poređenje, a to su standardi koji im obezbeđuju mapu rute koju treba da prate. Ovo im omogu-

ćava da provere proces, ali ne i efektivnost programa. Međutim, po svemu sudeći nedovoljan broj praktičara na polju konsultantskih usluga povezanih sa kontinuitetom poslovanja nema formalne revizorske veštine koje poseduju kolege u internoj reviziji i nema njihovu širinu pogleda i razmišljanja o poslovanju organizacije, što funkciju interne revizije pozicionira kao jednu od ključnih strana u sistemu kontinuiteta poslovanja unutar poslovnog entiteta. Da bi se postigao uspeh u reviziji programa kontinuiteta poslovanja, potrebno je i profesionalno poznavanje kontinuiteta poslovanja i posedovanja odgovarajuće veštine revizije. Predmet rada u nastavku je ispitivanje važnosti i potrebe razmatranja kontinuiteta poslovanja na nivou poslovnog entiteta, analiziranje sistema za upravljanje kontinuitetom poslovanja u regulatornom okviru Srbije, odnosa funkcije interne revizija prema kontinuitetu poslovanja, tehnika skeniranja u reviziji IT-ja posle katastrofa i analize kritičnih aplikacija informacionog sistema, što rezultuje izvođenjem važnih zaključaka o ulozi interne revizije u kontinuitetu poslovanja.

VAŽNOST I POTREBA KONTINUITETA POSLOVANJA

Iako postoji dosta literature koja govori o upravljanju zaštitom u slučaju katastrofa, i uprkos osvešćenosti o ovoj problematici, što je često, nažalost, bila posledica iskustva, mnoge organizacije još uvek nemaju razvijeno upravljanje zaštitom u slučaju katastrofa. S druge strane, današnje vreme pokazuje da se katastrofe događaju često i da dobra organizacija može znatno doprineti sigurnosti zaposlenih, usluga koje pružaju i zaštiti robe koju proizvode. Dostupni su primeri ustanova koje su pretrpele katastrofe poput potresa, poplava, požara, uništenja u ratovima i terorističkim napadima, a izveštaji o njihovim reakcijama i iskustvima dragocena su drugim privrednim subjektima jer im omogućavaju da unaprede svoje planove i zaštite organizaciju. Sistem za upravljanje kontinuitetom poslovanja organizaciono najčešće obuhvata najvažnije sektore organizacije: IT sektor, tehničko-proizvodni deo i finansije, a funkcionalno se odnosi na definisani skup IT/ICT servisa koje ove organizacione celine pružaju internim i eksternim korisnicima i poslovne procese koji su definisani u okviru *Business Continuity Management-a* (u daljem tekstu: BCM-a). *Business Continuity* evolucija je išla od reaktivne, usmerene na oporavak, do proaktivne i zasnovane na rizicima, kao što je prikazano na slici 1.

***Business Continuity** evolucija se razvijala od reaktivne, usmerene na oporavak, do proaktivne i zasnovane na rizicima.*



Izvor: Ilić, M (9, 9)

Slika 1. *Business Continuity* evolucija

Upravljanje kontinuitetom poslovanja je okvir za identifikaciju internih i eksternih rizika kojima je organizacija izložena. Cilj BCM-a je da obezbedi sposobnost organizacije da efektivno odgovori na pretnje kao što su prirodne katastrofe ili narušavanje, odnosno objavljivanje poverljivih podataka, i da zaštiti poslovne interese organizacije. Međunarodni standard ISO 22301, koji standardizuje aktivnosti u vezi sa kontinuitetom poslovanja, navodi i specifikuje zahteve za primenjivanje, održavanje i poboljšanje sistema menadžmenta radi zaštite, smanjenja verovatnoće dešavanja, pripreme za odgovor, odgovor i oporavak od poremećaja kada se oni pojave. Zahtevi specifikovani u ovom dokumentu su generički i predviđeni da budu primenljivi na sve organizacije ili njihove delove, bez obzira na vrstu, veličinu i prirodu kompanije. Obim primene ovih zahteva zavisi od okruženja u kojem organizacija radi, kao i njene kompleksnosti. Ovaj standard je primenljiv u organizacijama svih vrsta i veličina:

1. koje primenjuju, održavaju i poboljšavaju BCM;
2. koje teže da obezbeđuju usaglašenost sa iskazanom politikom kontinuiteta poslovanja;
3. kojima je potrebno da budu u stanju da nastave da isporučuju proizvode i usluge prema prihvatljivom, unapred definisanom kapacitetu, tokom poremećaja;
4. koje teže da unapređuju svoju otpornost putem efektivnog primenjivanja BCM-a.

Ovaj dokument može da se koristi za ocenu sposobnosti organizacije da ispunjava sopstvene potrebe i obaveze u vezi sa kontinuitetom poslovanja. Poimanje katastrofe obično je usmereno na razaranja nastala usled prirodnih pojava, poput poplava, požara, uragana i sl. No, u vremenu u ko-

jem zavisimo o novim tehnologijama, moguće su i nove katastrofe. Promene u energetskim sistemima, nestašica nafte i gasa koji dolaze iz Ruske Federacije i prekid dotoka električne energije ugrožavaju proizvodnju ili pružanje usluga, a, kada govorimo o struji, i mogućnost pružanja digitalnih usluga i pristupa različitima repozitorijumima, katalozima i slično, koji bez električne energije postaje nedostupan. Među eksternim stranama najznačajnije grupe su kupci, odnosno korisnici usluga. Toj kategoriji je najdragocenije da obezbedi:

1. ispunjenje dogovorenog nivoa usluga;
2. kvalitet usluga u skladu sa ponudom ili ugovorom;
3. identifikaciju potencijalnih tačaka za smanjenje uticaja;
4. procenu verovatnoće pojave događaja koji mogu izazvati krizne situacije;
5. poštovanje rokova;
6. bezbednost njihovih informacija u kriznim situacijama;
7. garanciju za pružanje usluga u kriznim situacijama;
8. brzo reagovanje u kriznim situacijama.

Druga veoma značajna grupa su dobavljači i ostali poslovni partneri čije interese možemo sažeti u korist poslovne saradnje, kontinuiteta u saradnji, pridržavanja utvrđenih ugovornih obaveza i uzajamne pomoći u kriznim situacijama. Društvena zajednica (lokalna i šira, u smislu države) pre svega je zainteresovana za poštovanje zakonske regulative, bezbednost i zaštitu imovine, zaštitu životne sredine, bezbednost i zdravlje zaposlenih i radno angažovanih, društveno odgovorno ponašanje i, u nekom širem smislu, pomoć u prevazilaženju sličnih budućih kriznih situacija. Među internim stranama najznačajnije grupe su korporativni organi, u smislu skupština akcionara, izvršni i nadzorni odbori akcionarskih društava i sami zaposleni. Tako je rukovodstvu i vlasnicima, tj. akcionarima, najvažnije:

Društvena zajednica pre svega je zainteresovana za poštovanje zakonske regulative, bezbednost i zaštitu imovine, zaštitu životne sredine, bezbednost i zdravlje zaposlenih i društveno odgovorno ponašanje.

1. pridržavanje zakona i propisanih pravila o radu;
2. očuvanje i unapređenje imidža i brenda kompanije;
3. stvaranje konkurentske prednosti;
4. povećanje otpornosti društva na događaje koji izazivaju poremećaj u poslovanju;
5. smanjenje zakonske i finansijske izloženosti, kao i direktnih i indirektnih troškova poremećaja u poslovanju;
6. obezbeđivanje poverenja zainteresovanih strana;
7. sposobnost društva da posluje uspešno i poboljšavanje sposobnosti društva da poslovanje ostane efektivno tokom poremećaja;
8. efektivno i efikasno proaktivno upravljanje rizicima uz razmatranje operativnih ranjivosti;

9. stalno unapređenje sistema upravljanja kontinuitetom poslovanja;
10. smanjenje štete u kriznim situacijama i ponašanje u skladu sa korporativnom kulturom;
11. kvalitetni i bezbedni uslovi rada.

Zaposleni su najznačajnija interna zainteresovana strana, a najčešće predstavljaju najveću enigmu, jer negativno iskustvo u nekim slučajeva nije značajno promenilo njihovu praksu upravljanja zaštitom u okolnostima katastrofa, kao ni upravljanja zaštitom uopšte. To se može povezati s poimanjem zaštite kao tehničkog pitanja, postupka koji zahteva velika finansijska ulaganja i dodatno vreme i posebne veštine osoblja, što nije uvek lako ostvarivo. No, može se povezati i s psihološkim činiocima, pri čemu su proživljena iskustva u nekim slučajevima ostavila osećaj nemoći i nedostatak potrebe da osoblje bude spremno da reaguje u slučajevima katastrofe. Dakle, zaposlenima i drugim radno angažovanim licima (npr. preko lizinga radne snage) najvažniji su:

1. bezbednost i zaštita zdravlja na radu;
2. kvalitetni radni uslovi;
3. poštovanje privatnosti u kriznim situacijama;
4. jasne i nedvosmislene informacije u kriznim situacijama;
5. motivisanost za ispunjenje obaveza u kriznim situacijama.

Naime, pažnju treba usmeriti na snažnu psihološku komponentu prisutnu u upravljanju zaštitom u slučaju katastrofa. Stoga je spremnost zaposlenih na primerene reakcije i njihova sposobnost da se nose s kriznim stanjima nešto čemu treba posvetiti izrazitu pažnju. Da bi revizori uspešno razumeli svoju ulogu u obezbeđivanju kontinuiteta poslovanja, važno je da razumeju analizu uticaja na poslovanje (u daljem tekstu: BIA – Business Impact Analysis). Navedena analiza se odnosi na proces određivanja kritičnosti poslovnih aktivnosti i potrebnih resursa kako bi se obezbedila operativna otpornost i kontinuitet poslovanja tokom i nakon prekida poslovanja. BIA kvantifikuje uticaje poremećaja na pružanje usluga, rizike po pružanje usluga i ciljeve vremena oporavka (u daljem tekstu: RTO – Recovery, Time, Objective) i ciljeve tačke oporavka (u daljem tekstu: RPO – Recovery, Point, Objective). Ovi ciljevi za oporavak se zatim koriste za razvoj strategija, rešenja i planova, identifikaciju poslovnih procesa koji podržavaju pružanje usluga i proizvoda, procenu uticaja nedostupnosti svakog poslovnog procesa nezavisno od njegovog izvora, prikupljanje po-

Spremnost zaposlenih na primerene reakcije i njihova sposobnost da se nose s kriznim stanjima je nešto čemu treba posvetiti izrazitu pažnju.

dataka o finansijskim i nefinansijskim gubicima u slučaju da poslovni proces nije dostupan, identifikaciju prioritetnih vremenskih okvira za nastavak aktivnosti na unapred definisanom nivou usluge u obliku ciljanog vremena oporavka, identifikaciju zavisnosti procesa i potrebnih resursa. Vremenski cilj oporavka (RTO) se koristi za definisanje vremena do kada mere ublažavanja (npr. plan kontinuiteta poslovanja) moraju biti završene, kako bi se izbegao negativan efekat nedostupnosti procesa.

Dakle, trebalo bi da revizori, ukoliko bi sa informatičarima simulirali nastanak vanrednog događaja, u revizorskom programu jasno popišu i testiraju najznačajnije aktivnosti pre RTO-a. To je trenutak do kojeg treba da se završe procedure oporavka i da se uspostavi i pokrene minimalni nivo usluge. S druge strane, revizori moraju da u slučaju RPO-a imaju u vidu međunarodni standard interne revizije 2600 – Izveštavanje o prihvaćenom riziku, koji zahteva od izvršnog rukovodioca revizije da kada zaključi da je rukovodstvo prihvatilo nivo rizika koji može biti neprihvatljiv za organizaciju, on/ona mora da raspravi to pitanje s višim rukovodstvom, zato što je cilj tačke oporavka (RPO) maksimalni podnošljivi period u kome podaci mogu biti izgubljeni usled prekida poslovanja, a sve preko toga je neprihvatljiv rizik za kompaniju.

SISTEM ZA UPRAVLJANJE KONTINUITETOM POSLOVANJA U REGULATORNOM OKVIRU REPUBLIKE SRBIJE

BCM ne obuhvata granice samostalnog subjekta, nije ni ogranak, niti na bilo koji način funkcioniše kao samostalna celina, već je deo poslovnog okruženja kompanije. Iako se pomenute granice u kojima važe principi kontinuiteta poslovanja odnose samo na neke organizacione celine, uz dobro uspostavljen integrisani sistem upravljanja mogle bi se primenjivati i u ostalim organizacionim celinama kompanije. Resursi koji se koriste iz drugih delova kompanije koji nisu u opsegu BCM-a nemaju status eksterne strane, već se posmatraju kao interni, pošto funkcionišu u okviru iste organizacije. Uz izvesna ograničenja, ovo važi za dokumentaciju, infrastrukturu, rukovodstvo i određene pomoćne funkcije. BCM povezuje politiku i ciljeve kontinuiteta poslovanja, sveukupnu strategiju upravljanja kontinuitetom poslovanja i upravljanje rizicima, uključujući kriterijume i prihvatljiv nivo rizika i identifikovane potencijalne uticaje na kontinuitet poslovanja.

BCM se do izvesne mere posmatra kao deo sistema za upravljanje incidentima uspostavljenog u društvu. Zakonski i regulatorni okvir u kome posluje društvo nameće određene zahteve u pogledu kontinuiteta poslovanja. Ovi zahtevi su prvenstveno sadržani u Zakonu o smanjenju rizika od katastrofa i upravljanju vanrednim situacijama (26, 1), Zakonu o kritičnoj infrastrukturi (25, 1), Zakonu o elektronskim komunikacijama (23, 1), Zakonu o zaštiti podataka o ličnosti (27, 1), Zakonu o informacionoj bezbednosti (24, 1), Odluci o minimalnim standardima upravljanja informacionim sistemom finansijske institucije (18, 1), Pravilniku o uslovima upravljanja informaciono-komunikacionim sistemom pružaoca usluga povezanih s digitalnim tokenima (15, 1) i Odluci o uslovima upravljanja informaciono-komunikacionim sistemom pružaoca usluga povezanih s virtuelnim valutama (10, 1). Socijalni i kulturološki aspekt informaciono-komunikacionih tehnologija postaje sve važniji za BCM, jer evoluciju tehnologija i servisa ne prati adekvatno i promena svesti korisnika, pa slaba percepcija bezbednosti informacija unosi dodatne rizike po kontinuitet poslovanja. Tehnološko okruženje u kojem funkcionišu srpske kompanije i uspostavljeni ISU karakterišu stalna unapređenja servisa i brza promena tehnologija uz pomoć kojih servisi funkcionišu. Treba imati u vidu i način upotrebe interneta u privredi Srbije:

Socijalni i kulturološki aspekt informaciono-komunikacionih tehnologija postaje sve važniji za BCM, jer evoluciju tehnologija i servisa ne prati adekvatno i promena svesti korisnika.

- u Republici Srbiji 100% preduzeća ima internet priključak;
- u 36,0% preduzeća od 1% do 24% zaposlenih lica koristi internet;
- u 35,7% preduzeća od 75% do 100% zaposlenih koristi internet.

Zbog čega je važan osvrt na upotrebu interneta? Pandemija bolesti COVID-19, izazvana koronavirusom, ima veliki uticaj na kontinuitet poslovanja. S jedne strane, poslovni procesi i pružanje servisa obavljaju se u izmenjenim uslovima ili u smanjenom obimu, a s druge strane, korišćenje nekih servisa (pre svega interneta) u kompanijama se značajno povećava, čime se povećava rizik od preopterećenja pojedinih sistema ili nedovoljnog kvaliteta servisa koji se pružaju korisnicima. Praćenje trendova na tržištu i na polju tehnologija zahteva odgovarajuće finansijske i kadrovske resurse kako bi se išlo u korak sa dinamičnim tehnološkim okruženjem, kao i konstantan rad na ispunjenju zahtevanog nivoa kvaliteta pružanja usluga ili servisa krajnjem korisniku. Pa tako veb-sajt poseduje 84,4% srpskih preduzeća, što čini povećanje od 0,8% u odnosu na 2019. i povećanje od 1,8% u od-

nosu na 2018. godinu. Kada pogledamo strukturu preduzeća prema veličini, dobijamo sledeće rezultate:

- 99,0% velikih preduzeća poseduje veb-sajt;
- 89,1% srednjih preduzeća poseduje veb-sajt;
- 82,8% malih preduzeća poseduje veb-sajt.

Ipak, Strategiji razvoja informacionog društva i informacione bezbednosti u Republici Srbiji za period od 2021. do 2026. godine (19, 16) usluge *cloud* servisa putem interneta plaća svega 18,6% srpskih preduzeća. Vezu digitalizacije i kontinuiteta poslovanja treba višeslojno posmatrati. S jedne strane, aktuelna pandemija je uticala kao svojevrsni „filter" koji je iznedrio mnoge kompanije, ali i grane privrede, i doprineo sveopštoj globalizaciji i digitalizaciji celokupnog društva. Primer za to su svi poslovi i sve delatnosti koje su bazirane na internet tehnologijama, poput elektronske prodaje, dostave hrane, obrazovanja posredstvom onlajn alata i platformi, kao i bilo koji drugi poslovi koji se mogu efikasno obavljati putem interneta (8, 1). S druge strane, nepovoljna ekonomska situacija u kojoj posluju srpske kompanije zahteva smanjenje izdataka i postizanje rezultata uz ograničene finansijske resurse. S treće strane, sve su veći zahtevi tržišta da se servisi i proizvodi kompanija koji se pružaju kupcima isporučuju i u vreme vanrednih ili kriznih situacija.

Tržište radne snage u Srbiji, kao i u svetu, karakteriše povećana potražnja za IKT stručnjacima kao posledica brzog razvoja IKT sektora. U uslovima u kojima posluje kompanija, i zbog sve većih poslovnih potreba u ovoj oblasti, fluktuacija ljudskih resursa u srpskim kompanijama je relativno velika. Taj problem je prepoznat i u navedenoj Strategiji razvoja informacionih tehnologija, gde se navodi da 20,9% preduzeća zapošljava IKT stručnjake, 55,7% je imalo slobodna radna mesta za IKT stručnjake, a čak 77,1% preduzeća koristi eksterne dobavljače za obavljanje IKT funkcija. Nemogućnost da se zadrže ili dodatno motivišu zaposleni, čije su kvalifikacije i kompetencije u ovoj oblasti sve traženije, predstavlja jedan od najznačajnijih rizika sa kojim se kompanije suočavaju u poslednjih nekoliko godina. Istovremeno se nameće pitanje toga ko će zaposlenima usađivati organizacionu kulturu važnosti BCM-a zarad kompletne saradnje na poslovima obezbeđivanja poslovnog procesa i ujedno opstanka kompanije na tržištu. Neke kompanije koje grade imidž društveno odgovornih kompanija, angažovane su u realizaciji mera propisanih od strane nadležnih tela za vanredne situacije (npr. omogućavanje interneta u privremenim bolnicama), zbog čega su zaposleni telko (telco) kompanija dopunski angažovani, a u nekim slučajevima i izloženi

većem riziku od zaražavanja. Takođe, aktuelne klimatske i geopolitičke promene dodatno utiču na aktuelnost kontinuiteta poslovanja u telko kompanijama.

REVIZIJA I KONTINUITET POSLOVANJA

Iz svega navedenog nameće se zaključak da kontinuitet poslovanja predstavlja više od formulisanog i napisanog plana za slučaj katastrofe, te se odnosi i na šira pitanja upravljanja kao što su finansije, procena rizika i edukacija zaposlenih. Revizori pre svega moraju da razumeju proces, od toga da upravljanje zaštitom u slučaju katastrofa (u literaturi se često navodi i engl. disaster management), predstavlja unapred planiranu organizaciju zaposlenih, sredstava i aktivnosti kako bi se predvideli potencijalni izvori katastrofa (u slučajevima gde je to moguće) i pokušalo sprečiti da do njih dođe, te kako bi se moglo primereno reagovati u određenim okolnostima i time osigurati efikasna zaštita zaposlenih, objekata, proizvoda i usluga. Plan mera zaštite u slučaju katastrofa je jasan i koncizan dokument u kojem su navedene preventivne i pripremne mere kako bi se smanjio mogući rizik, a takođe propisuje postupke reakcije i oporavka tokom i nakon katastrofe. To u velikoj meri olakšava i formulisanje revizorskog programa, jer nema „apstraktnih" delova koji neretko zamagljuju pojedine procese i otežavaju revizorske angažmane.

Plan mera zaštite u slučaju katastrofa je jasan i koncizan dokument u kojem su navedene preventivne i pripremne mere kako bi se smanjio mogući rizik.

Faze u planiranju mera zaštite predstavljaju aktivnosti grupisane u barem nekoliko faza, a to su: procena ugroženosti, preventivne mere, mere pripravnosti, spasavanje građe i saniranje posledica. Samim tim bi revizori koji učestvuju u BCM reviziji trebalo da testiraju BCM planove, procedure i dokumentaciju organizacije. Testiranjem adekvatnosti kontrola bi se procenila usklađenost sa specifikacijama, standardima, ugovornim sporazumima ili drugim kriterijumima poput:

- da li je informacioni sistem deo BCM;
- da li su zahtevi informacionog sistema jasno i u potpunosti definisani od strane menadžmenta;
- da li je u održavanju i testiranju informacionog sistema obezbeđena ažurnost;
- da li se promene u informacionom sistemu kreću „u koraku" s promenama u poslovanju;
- da li je završena sveobuhvatna analiza uticaja na poslovanje;
- da li su regulisani odnosi sa dobavljačima u slučaju kašnjenja u dostavi repromaterijala;

- da li se redovno ažuriraju ugovori;
- da li se *backup* podataka nalazi na istoj lokaciji kao i produkcioni podaci.

Skladištenje podataka, odnosno sve komponente na koje se vrši *backup* podataka, trebalo bi da se ne nalaze u data centru gde je i sedište preduzeća, tj. organizacije. Data centar se može definisati kao mesto u kom su smešteni računarski sistemi, sistemi za skladištenje podataka i telekomunikaciona oprema. Data centri uključuju i sisteme za napajanje, sisteme za *backup* napajanja (baterije, agregate), protivpožarne sisteme, sisteme za održavanje uslova radne okoline i bezbednosne sisteme, i omogućavaju smeštaj i funkcionisanje IT infrastrukture. Osnovna namena data centara je da obezbede rad aplikacija i operativnih baza podataka neophodnih za funkcionisanje preduzeća.

TEHNIKE SKENIRANJA U REVIZIJI IT-JA POSLE KATASTROFA

Kod BCM-a važno je sagledati i kakve su kontrole uspostavljene za sajber rizike. Naime, u slučaju većih katastrofa i vanrednih situacija, „preživeli" zaposleni će biti upućeni da rade iz domova, i time se nameće masovno prihvatanje digitalne tehnologije. Primera radi, tokom pandemije su pravi *bum* doživeli servisi za audio i video prenos signala poput *Zoom-a*, *Webex-a*, ali i društvenih medija kao što su *Facebook*, *Instagram* i *YouTube*. Neka istraživanja (2, 9) potvrđuju da su kompanije koje su preusmerile svoje usluge ili poslovanje, u meri u kojoj je to bilo moguće, na ove elektronske servise, doživele porast profita tokom pandemije, bez rizika po obustavljanje proizvodnog procesa. U tom smislu, revizori bi trebalo da obuhvate proveru nadzora aplikacija za udaljeni pristup i njihovo testiranje. Istovremeno, potrebno je proveriti i kako su HR rukovodioci vršili „kampanje podizanja svesti" o posebnim uslovima društvenog života zaposlenih tokom pandemije i koje su mere preduzete za pomoć zaposlenima u slučaju poteškoća u radu sa elektronskim servisima. Ukoliko se katastrofa već desila, revizori primenom specijalizovanih softverskih alata mogu automatizovano skenirati IT sistem da utvrde posledice. Naravno, tehnika skeniranja i mimo BCM-a, tj. u mirnodopskim uslovima, primenljiva je na testove različitih kontrola u različitim procesima, sistemima i tehnologijama. Njihova osnovna karakteristika je velika brzina izvođenja. Zbog svoje brzine, testovi u kojima se primenjuju ove tehni-

Revizori bi trebalo da obuhvate proveru nadzora aplikacija za udaljeni pristup i njihovo testiranje.

ke mogu se izvoditi na čitavoj populaciji i sa većim brojem ponavljanja, što znači da uzimanje uzoraka nije potrebno. Pored toga, manuelni rad revizora i interakcija sa ljudskim faktorom na strani klijenta revizije svedeni su na minimum, čime se uvećava pouzdanost testova i objektivnost rezultata. Sve ovo zajedno utiče na veliko umanjenje revizorskog rizika, a posebno rizika detekcije, budući da je rizik uzorkovanja potpuno isključen.

Skeniranje je slanje automatski generisanog niza paketa (TCP segmenta, UDP i IP datagrama ili ethernet okvira) koji su u skladu sa jednim ili više mrežnih protokola, a u kojima se programski menjaju izabrani parametri. U zavisnosti od tipa skeniranja, parametri koje menjamo mogu da budu IP adresa (polazna i odredišna), MAC adresa, UDP ili TCP port, TTL (eng. Time to Live), flegovi (eng. Flags - „zastavice" su bitovi u TCP segmentu kojima se označavaju faze u konekciji i razmeni podataka – URG, ACK, PSH, RST, SYN i FIN), redni brojevi (eng. sequence numbers), itd. U opštem slučaju, moguća je manipulacija sadržajem bilo kojeg kontrolnog polja u protokolu, uključujući i vrednosti koje nisu u skladu sa definicijom protokola; bilo u sintaksnom, bilo u semantičkom pogledu. Skeniranja se mogu vršiti u okviru svih vrsta mrežnih protokola. Najčešće su to TCP/UDP, ARP i ICMP, dok se u specifičnim skeniranjima, kao što su skeniranja aplikacija, koriste pripadajući aplikativni protokoli. Na primer, kod testova veb-aplikacija koriste se protokoli HTTP ili HTTPS (TCP portovi 80 i 443), koji su karakteristični za ovaj tip aplikacija. Nešto ređe skeniraju se protokoli DNS i SNMP, dok se kod baza podataka skeniranja prilagođavaju portu i aplikativnom protokolu koji je karakterističan za svaku konkretnu DBMS implementaciju. U pogledu sistema i tehnologija, njihova primena nema nikakvih ograničenja, dok je u pogledu procesa primena ovih tehnika najčešća u planiranju, implementaciji i održavanju sistema informatičke bezbednosti i u procesima kao što su upravljanje konfiguracijama i izmenama (eng. Configuration and Change Management), upravljanje slabostima (eng. Vulnerability Management), održavanje softvera i upravljanje softverskim korekcijama (eng. Patch Management).

Preporučeni alati mogu da budu:

- Nessus (komercijalni *vulnerability scanner* opšte namene),
- OpenVAS (open source *vulnerability scanner* opšte namene),
- ZAP – Zed Attack Proxy (*open source vulnerability scanner* za veb-aplikacije),

- Burp Suite (komercijalni vulnerability scanner za veb-aplikacije),
- Retina, Nexpose, Acunetix, Netsparker (komercijalni skeneri različite namene).

Otkrivanje i ocena slabosti (ranjivosti) je automatski postupak kojim se identifikuju slabosti mrežnih servisa, aplikacija ili kompletnih informacionih sistema (1, 4). U zavisnosti od alata koji se koristi, ovaj postupak takođe pruža ocenu otkrivenih slabosti prema stepenu rizika i daje praktična uputstva za njihovo otklanjanje sa prioritetima korektivnih aktivnosti. Tehnike skeniranja koje se koriste u ovom postupku predstavljaju kombinaciju prethodno nabrojanih tehnika za skeniranje i drugih složenijih automatskih postupaka (eng. fingerprinting, versioning, vulnerability scanning). Alati su znatno kompleksniji od onih za prethodno nabrojane tehnike skeniranja, imaju grafičke korisničke interfejse i raspolažu desetinama politika za različite tipove skeniranja i desetinama hiljada *plug-in* modula, od kojih je svaki specijalizovan za pojedinu ranjivost. Pored alata opšte namene, postoje i alati specijalizovani za slabosti veb-aplikacija, slabosti baza podataka, enkripcionih protokola, pristupa *wireless* mrežama i drugo. Tipične primene mogu da obuhvataju polja koja se odnose na suštinske testove kontrola informatičke bezbednosti, fokusirane testove slabosti, testove adekvatnosti i efektivnosti generalnih i aplikativnih kontrola, sticanje uverenja o stanju informatičke bezbednosti sistema u radu i sticanje uverenja o servisnom statusu softvera u informacionim sistemima.

Otkrivanje i ocena slabosti (ranjivosti) je automatski postupak kojim se identifikuju slabosti mrežnih servisa, aplikacija ili kompletnih informacionih sistema.

KRITIČNE APLIKACIJE INFORMACIONOG SISTEMA

Kontrole u oblasti informatičkih rizika najčešće se dele na opšte (eng. General Level Controls) i aplikativne kontrole (eng. Application Level Controls). Opšte ili generalne kontrole se odnose na širi kontekst – zajedničke su i istovetne za celu organizaciju ili neki njen obiman i složen sastavni deo. Aplikativne kontrole se odnose na specifičnosti pojedinih sistema ili njihovih delova, što znači da te kontrole u nekim svojim detaljima i pojedinostima odstupaju od opštih kontrola. Sve kontrole su podložne reviziji i, kao takve, one moraju biti dobro shvaćene od strane revizora. Revizor mora razumeti njihov smisao, njihove ciljeve i specifične rizike na koje se te kontrole odnose. Kontrole za neprekidnost poslo-

vanja (eng. Contingency Planning Controls) pružaju razumno uverenje da planovi za neprekidnost poslovanja štite informacione resurse u slučaju neplaniranih prekida i obezbeđuju brz oporavak kritičnih procesa nakon takvog prekida, odnosno da obezbeđuju efektivno:

- ocenjivanje stepena kritičnosti i osetljivosti operacija;
- identifikovanje resursa neophodnih za podršku poslovnim operacijama;
- postupanje u cilju sprečavanja i minimizovanja potencijalne štete i trajanja prekida;
- planiranje neprekidnosti, odnosno donošenje plana o neprekidnosti;
- periodično testiranje plana za neprekidnost poslovanja;
- adaptaciju (izmene) plana za neprekidnost poslovanja u skladu sa rezultatima testova.

Operativna rezervna lokacija mora biti pokrivena ugovorima, i to tako što bi ključni hardver trebalo da bude pokriven ugovorima o održavanju. Revizori mogu da sprovedu brzu „zdravstvenu proveru", pregledajući planove i intervjuišući ključne aktere. Složeniji i duži revizorski angažmani pomeraju fokus i testove u revizorskom angažmanu na sledeće aspekte:

- donošenje odluka u vanrednim situacijama i operativnu koordinaciju;
- bezbednosnu podršku i pomoć;
- kriznu komunikaciju;
- sistemski odgovor na različite scenarije vanrednih situacija i katastrofa;
- oporavak informacionih sistema;
- uspostavljanje i održavanje kontinuiteta poslovanja, tj. ključnih funkcija organizacije.

Naravno da, slično drugim revizijama, vrsta i obim revizorskog angažmana zavise od rizika, zahteva za uveravanjem rukovodstva i dostupnih resursa revizije. Rukovodiocima revizije uvek stoji na raspolaganju mogućnost da angažuju i spoljne specijalističke resurse. To je praksa koju i standardi dozvoljavaju ukoliko nema kolektivnog znanja. Revizori bi mogli da učestvuju kao „formalni posmatrači" u takvim angažmanima. Ipak, poželjno je da to bude zajednički poduhvat sa eksternim konsultantom, jer čak i tada nema prepreka da pregledaju dokumentaciju, programe i procene njegovu sveobuhvatnost i potpunost. Prilikom obavljanja revizije interni revizor je dužan da primenom pune profesionalne pažnje identifikuje prevare, pogrešne radnje, greške, propuste, nee-

fikasnosti i neadekvatne kontrole koje prate uspostavljanje i održavanje kontinuiteta poslovanja. Sledeće aspekte generalno vredi razmotriti prilikom ove vrste revizije:

- *Celokupno upravljanje programima*
  1. Kako se upravlja programima?
  2. Da li im se daju odgovarajući strateški pravci i investicije?
  3. Da li organizacija stavlja dovoljan naglasak na kontinuitet poslovanja?
- *Identifikacija ključnih rizika*
  1. Da li su identifikovani rizici po infrastrukturu poslovanja?
  2. Da li je rukovodstvo utvrdilo smernice za daljinsko upravljanje sistemima i proizvodnjom?
  3. Da li su mapirane tačke koje su kritične u proizvodnji?
- *Organizaciona struktura i odgovornost*
  1. Da li su uključeni odgovarajući i zainteresovani stejkholderi?
  2. Da li se dovoljno interesuju za programe kroz angažovanje i akciju?
  3. Ko je odgovoran za njihov uspeh ili neuspeh?

Naime, u slučaju da su već mapirane tačke koje su se pokazale neuspešnim u prvim danima nekog ranije vanrednog događaja, razmatra se da li su kreirani novi planovi reagovanja (koji uključuju postupke, raspodele zaposlenih, alate i sredstva za rad), kao i pripreme za kašnjenja u lancu snabdevanja. Tako neki od najčešćih nalaza mogu da obuhvataju zahteve za obnavljanjem posvećenosti upravljanju programom kontinuiteta poslovanja, jer je primećeno da se procesi, procedure i mehanizmi retko testiraju, pregledaju i ažuriraju, da nisu definisani zahtevi za obuku zaposlenih sa odgovornostima, nisu ažurirana interna dokumenta, i drugo.

Primećeno je da se procesi, procedure i mehanizmi retko testiraju, pregledaju i ažuriraju, da nisu definisani zahtevi za obuku zaposlenih sa odgovornostima, nisu ažurirana interna dokumenta, i drugo.

ZAKLJUČAK

Okolnosti nameću informacionu pismenost revizorima kao neophodnost za upravljanje izazovima revizorskog angažmana (12, 1). Upravo je rukovodstvo klijenata revizije, za koje se podrazumeva da je savladalo IT i ICT izazove procesa kojim upravlja, stvorilo uslove u kojima omogućuje da upravo oni budu podrška u donošenju odluka, odnosno u delotvornom i efikasnom ostvarenju poslovnih ciljeva. Kako rizici predstavljaju sveprisutni faktor neizvesnosti

u poslovanju, oni bez izuzetaka moraju biti uzeti u razmatranje kada govorimo o realizaciji ciljeva, pri čemu kapitalni strateški cilj bilo koje organizacije predstavlja upravo uspostavljanje adekvatne organizacione otpornosti na vanredne događaje i katastrofe. Upravljanje kontinuitetom poslovanja predstavlja napredni sistematski pristup u procesu ostvarenja kompanijske otpornosti. Revizori mogu biti dragoceni saveznik rukovodstvu jer testiranjem adekvatnosti internih kontrola omogućuju rukovodstvu da preventivno identifikuje potencijalne slabosti koje mogu dovesti do neuspeha u uspostavi kontinuiteta poslovanja.

Revizija kontinuiteta poslovanja treba da podrži napore korporativne otpornosti i kritične poslovne funkcije. Interna revizija kontinuiteta poslovanja treba da definiše rizike ili pretnje po uspeh plana kontinuiteta poslovanja i da testira postojeće kontrole da bi se utvrdilo da li su ti rizici prihvatljivi (3, 5). Ona treba da potvrdi plan kontinuiteta poslovanja organizacije i da obezbedi da svi njegovi procesi funkcionišu ispravno. Zadatak revizije je da ispita učinak aktivnosti u planu i osigura da procesi kontinuiteta poslovanja i oporavka od katastrofe ispunjavaju organizacione standarde. Takođe bi trebalo da skrene pažnju na svako održavanje ili ažuriranje koje treba izvršiti, ako postoje jasni nedostaci (5, 4). Ona istovremeno treba i da kvantifikuje efekat slabosti plana i ponudi preporuke za poboljšanje plana kontinuiteta poslovanja. Tehnologija i pretnje se stalno menjaju, a revizija plana kontinuiteta poslovanja je još jedan korak koji treba preduzeti da bi se osiguralo da je plan ažuran i da neće propasti ako se suoči sa katastrofom. Kada su u pitanju procesi koji se odnose na kontinuitet poslovanja, neko opšte, neformalno pravilo bi moglo da glasi da što više testiranja se sprovodi, to je bolje. Iako organizacija može pokušati da ublaži i izbegne potencijalne rizike, veličina i obim potencijalnih pretnji, kao što su sajber napadi i prirodne katastrofe, često su nepredvidivi (7, 2). Što više poslova na prevenciji, pripremi i planiranju organizacija može da uradi, to je bolje. Napori za upravljanje kontinuitetom poslovanja su potkrepljeni obavljanjem revizije, koja daje povratne informacije o tome šta funkcioniše u planu i šta treba poboljšati. Sveobuhvatna revizija BCP-a pruža objektivne povratne informacije koje mogu poboljšati plan kontinuiteta poslovanja uz aktivne izmene i ažuriranja. Uzimajući u obzir opštu najbolju praksu u industriji i očekivanja menadžmenta, dovoljnost i uspeh plana za kontinuitet poslovanja može se utvrditi temeljnom revizijom (19, 1).

Tako se tokom planiranja i sprovođenja revizije kontinuiteta poslovanja pojedina pitanja mogu nametnuti kao naroči-

to bitna za kvalitet samog učinka revizorskog angažmana, a to su poverljivost, redovnost i jasnost. Pitanje poverljivosti je veoma važno jer, iako je neophodno obaveštavati zainteresovane strane o nalazima revizije kontinuiteta poslovanja, ranjivosti kompanije ne bi trebalo da budu lako dostupne van organizacije. Kako se sajber napadi povećavaju i bezbednost informacija postaje kritična, rezultati revizije treba da budu adekvatno zaštićeni (18, 10). Samo redovne i periodične revizije kontinuiteta poslovanja mogu da pruže zahtevani učinak. Planiranje kontinuiteta poslovanja nije jednokratna procedura, to je proces koji je je kontinuiran. Plan kontinuiteta poslovanja mora da se ažurira onoliko često koliko organizacija prolazi kroz promene. Godišnje ažuriranje može biti pravilo za neke organizacije, ali učestalost može da se razlikuje, pa se tako, da bi se održao integritet plana i revizorskog izveštaja, oni moraju redovno ažurirati kako bi odražavali promene, a to znači sprovođenje redovnih i periodičnih revizija kontinuiteta poslovanja. Prilikom obavljanja ove vrste revizorskog angažmana, revizorski tim treba da bude jasan i nedvosmislen u pogledu zahteva plana kontinuiteta poslovanja. Izveštaji kao što su analiza uticaja na poslovanje (BIA) i procena rizika treba da budu ažurni (14, 1). Ako plan mora ispuniti bilo koje standarde usklađenosti, ti parametri moraju biti uključeni u reviziju, a sama revizija mora da pokaže nepristrasne rezultate, posebno ako se sprovodi interno.

Revizija upravljanja kontinuitetom poslovanja neizbežno dovodi do preispitivanja kvaliteta donošenja odluka i komunikacije najviših rukovodilaca.

Detaljnost i složenost revizije kontinuiteta poslovanja može da varira i da se kreće od krajnje jednostavne do veoma složene, u zavisnosti od zahteva i potreba zainteresovanih strana. Sa porastom detaljnosti i složenosti ovakve vrste revizije, rastu i njeni značaj i učinkovitost. Jedan poslovni entitet bi mogao da bude samo zainteresovan da izvrši neposredan opšti pregled i da testira plan kontinuiteta poslovanja u domenu generalnih odrednica, međutim, rezultati takve vrste revizije kontinuiteta poslovanja mogu da budu manjeg značaja (13, 2). S druge strane, neka poslovna organizacija se može odlučiti na sprovođenje detaljnijeg pregleda plana kontinuiteta poslovanja sa pratećim testiranjima otpornosti na napade, simulacijama neprijateljskih napada i katastrofa, što bi sigurno predstavljalo osetno veći trošak, ali bi i rezultiralo daleko značajnijim nalazima, čijim blagovremenim izvršenjem može da se postigne značajan učinak na polju unapređenja poslovnih procesa u domenu kontinuiteta poslovanja i sveukupne otpornosti poslovnog entiteta. Revizija upravljanja kontinuitetom poslovanja neizbežno dovodi do preispitivanja kvaliteta donošenja odluka i komunikacije najviših rukovodilaca (15, 1). Odbor i najviše rukovodstvo poslovnog entiteta mogu

da budu skloni precenjivanju sopstvenih sposobnosti za reagovanje na pretnje, a funkcija interne revizije im može pomoći na više načina. Interna revizija može da odredi fokus rukovodstva poslovnog entiteta i da ga poveže sa pitanjima otpornosti organizacije na pretnje (11, 1). Fokus na pretnje podrazumeva procenu verovatnoće i uticaja nastanka stvarno rizičnih događaja, poput ekstremnih vremenskih prilika, pandemija, terorizma, poplava, transportnih prepreka, požara i drugo. Uključivanjem kriznih vežbi na najvišem nivou, kao deo njihove definicije efikasnog upravljanja rizikom i otpornošću, i simulacijama neprijateljskih napada i katastrofa tokom sprovođenja revizorskog angažmana - povećava se i spremnost organizacije da reaguje na stvarne pretnje.

LITERATURA

1. Ashrafi, R., Haitham, A. (2022). A framework for IS/IT disaster recovery planning. International Journal of Business Continuity and Risk Management. 12 (1), 1-21.
2. Askeland, T., Flage, R., Guikema, S., D. (2021). Assessing the risk reducing effect of measures against intelligent attacks: review and discussion of some common approaches. International Journal of Business Continuity and Risk Management. 11 (1), 25-51.
3. Balkaran, L., Mark, J., E. (2022). Red flag risks. For many corporate mishaps, there were plenty of warning signs. Internal Auditor. 89 (2), 58-64.
4. Dushie, D. (2019). Business Continuity Planning: An Empirical Study of Factors that Hinder Effective Disaster Preparedness of Businesses. Journal of Economics and Sustainable Development. 5 (27), 185-191, 2014.
5. Fani, S., Subriadi, A., Business Continuity Plan: Examining of Multi-Usable Framework. Procedia Computer Science. 161, 275-282.
6. Federal information system controls audit manual (FISCAM). United States Government Accountability Office (2009). https://www.gao.gov/assets/gao-09-232g.pdf
7. Ha, K. (2019). Examining a research boundary within natural disaster management: qualitative case study. International Journal of Business Continuity and Risk Management. 9 (4), 298-311.
8. Hodge, B. (2021). An understanding of technology, third parties, and the human factor of security is vital to protecting the organization. Internal Auditor. 88 (4), 24-31.
9. Ilić, M. (2021). Business Continuity Management, UIRS webinar, Beograd.
10. Jain, P., Pasman, H., J., Mannan, M., S. (2020) Process system resilience: from risk management to business continuity and sustainability. International Journal of Business Continuity and Risk Management. 10 (1), 47-66.
11. Jakovljević, N., Jakovljević, J. (2021). The impact of the Covid-19 global pandemic on the responsibility of auditors. Finansije. 92-113.
12. Jeremić, N., Jeremić, M., & Jakovljević, N. (2021).Agilnost interne revizije. Revizor. 24, (95-96), 57-76.
13. Kall, V., L. (2022). Risk. The Test of Time In an age of digital transformation, legacy systems quickly become outdated. Internal Auditor. 89 (2), 25-29.

14. Lenning, J., Gremyr, I. (2017). Making internal audits business-relevant. Total Quality Management and Business Excellence 28(3). 1-16.
15. Međunarodni standard ISO 22301. Institut za standardizaciju Srbije objavljen SRPS EN ISO 22301:2020 60.60.
16. Odluka o minimalnim standardima upravljanja informacionim sistemom finansijske institucije (Sl. glasnik RS br. 23/13, 113/13, 2/17, 88/19, 37/21).
17. Odluka o uslovima upravljanja informaciono-komunikacionim sistemom pružaoca usluga povezanih s virtuelnim valutama (Sl. glasnik RS br. 49/21).
18. Pravilnik o uslovima upravljanja informaciono-komunikacionim sistemom pružaoca usluga povezanih s digitalnim tokenima (Sl. glasnik RS br. 69/21).
19. Rimmer-Hollyman, G., Oliver, M. (2022). Risky business. Internal audit can take a 5-step approach to providing assurance over an organization's risk management culture. Internal Auditor. 89 (2), 52-58.
20. Sambo, F., Bankole, F., O. (2016). A Normative Process Model for ICT Business Continuity Plan for Disaster Event in Small, Medium and Large Enterprises. International Journal of Electrical and Computer Engineering. 6 (5): 2425–2431.
21. Strategija razvoja informacionog društva i informacione bezbednosti u Republici Srbiji za period od 2021. do 2026. godine (Sl. glasnik RS br. 86/21).
22. Venclova, K., Urbancova, H., Vydrova, H. (2013). Advantages and Disadvantages of Business Continuity Management. International Journal of Industrial and Systems Engineering 7:4, 2013.
23. Zakon o elektronskim komunikacijama (Sl. glasnik RS br. 44/10, 60/13 - US, 62/14, 95/18 - dr. zakon).
24. Zakon o informacionoj bezbednosti (Sl. glasnik RS br. 6/16, 94/17, 77/19).
25. Zakon o kritičnoj infrastrukturi (Sl. glasnik RS br. 87/18).
26. Zakon o smanjenju rizika od katastrofa i upravljanju vanrednim situacijama (Sl. glasnik RS br. 87/18).
27. Zakon o zaštiti podataka o ličnosti (Sl. glasnik RS, br. 87/2018).

Rad primljen: 12.4.2022 • Prihvaćen: 19.5.2022.

THE ROLE OF INTERNAL AUDITING IN BUSINESS CONTINUITY

SUMMARY

The goal of auditing business continuity is to establish factual phenomena and to answer the question of whether the business continuity plan is effective and in line with the goals of the organization. The subject of the paper is examining the importance and need to consider business continuity at the entity level, analyzing the business continuity management system in the Republic of Serbia regulatory framework, the relationship of internal audit to business continuity, scanning techniques in information technology audit after disasters and analysis of critical information system applications.

Keywords: internal audit; business continuity; risks; disasters; recovery.