Nebojsa Jeremić[1]
Veljko Dmitrović[2]
Jovanka Jakovljević[3]
Nemanja Jakovljević[4]

PREGLEDNI RAD
UDK 005.33:005.591
DOI: 10.46793/Rev25111.107J
Primljen 30.06.2025.
Prihvaćen 23.08.2025.
Objavljen: 30.09.2025.

Testiranje otpornosti na rizik: kako definisati procedure

Apstrakt: *U današnjem sve složenijem i međusobno povezanijem svetu, organizacije i sistemi u različitim sektorima suočavaju se sa nivoima rizika bez presedana, u rasponu od finansijske nestabilnosti do ekoloških katastrofa i pretnji po sajber bezbednost. Kako učestalost i intenzitet ovih rizika rastu, postaje ključno ne samo da se identifikuju potencijalne ranjivosti, već i da se testira i izmeri otpornost sistema suočenih sa ovim izazovima. Otpornost na rizik se odnosi na sposobnost Sistema, bilo da se radi o organizaciji, infrastrukturi ili zajednici, da predvidi, apsorbuje, prilagodi se i oporavi od ometajućih događaja dok nastavi da efikasno funkcioniše. Predmet rada je analiza koncepta otpornosti na rizik, naglašavajući važnost testiranja okvira i metodologija za procenu robusnosti sistema u različitim scenarijima rizika. Kroz sveobuhvatno testiranje rizika, zainteresovane strane mogu bolje razumeti snage i slabosti svojih trenutnih strategija, omogućavajući im da donesu informisane odluke o upravljanju rizikom, ublažavanju i prilagođavanju. Glavni zaključak u radu je da interna revizija može u znacajnoj meri da doprinese da se poboljšaju sposobnosti organizacija za testiranje otpornosti na rizik tako što jesnije definisati dizajn i implementaciju internih procedura i internih kontrola, kao i tako sto ce da generise pravovremene i jasne rezultate testova otpornosti.*

Ključne reči: *interna revizija, interne kontrole, rizici, otpornost*

[1] Telekom Srbija. Srbija.
E-mail: nebojsaje@telekom.rs
ORCID iD: https://orcid.org/0009-0005-8622-3399

[2] Fakultet organizacionih nauka, Univerziteta u Beogradu. Srbija.
E-mail:
ORCID iD: https://orcid.org/ 0000-0001-8924-9758

[3] Centar za zaštitu odojčadi, dece i omladine, Beograd, Srbija.
E-mail: stefan.milojevic@educons.edu.rs
ORCID iD: https://orcid.org/009-0002-8175-1676

[3] Ekonomski fakultet Univerziteta u Beogradu, Srbija.
E-mail: jakovljevic.i.nemanja@gmail.com
ORCID iD: https://orcid.org/ 0009-0007-0198-1639

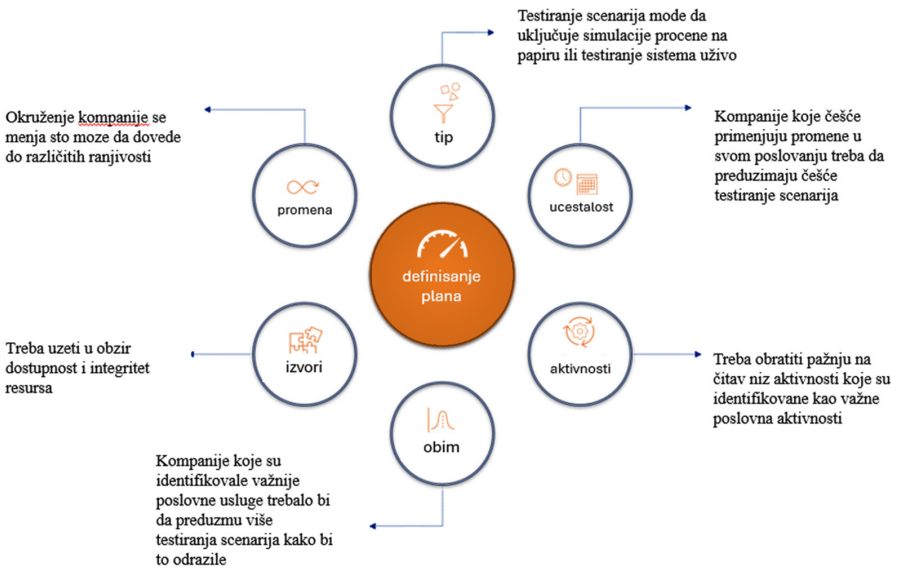
UVOD

Rastući izazovi, nadolazeće krize i nestabilnosti u sve složenijem i međusobno povezanom svetu, dovode do izrazitog pada sposobnosti sistema, organizacija i infrastruktura da izdrže i oporave se od neželjenih događaja. Ovakva situacija je postala kritičnija nego ikad. Testiranje otpornosti na rizik, sistematski proces za procenu sposobnosti entiteta da izdrži različite destabilizujuće sile, pojavilo se kao vitalna komponenta savremenih strategija upravljanja rizikom. Uprkos rastućoj važnosti, ostaje nedostatak standardizovanih procedura za efikasno sprovođenje takvih testova u različitim industrijama i kontekstima. Testiranje otpornosti na rizike je vrsta testiranja gde se interni sistem testira u odnosu na simulirane nepovoljne uslove, uključujući pregled internih aktivnosti i izvođenje internih kontrola (). Testiranje otpornosti se fokusira na testiranje softvera u odnosu na uobičajene probleme kao što su kvarovi hardvera ili sistema, prekidi mreže ili velika opterećenja saobraćaja. Testiranje otpornosti može pomoći da se testira sposobnost softvera da održi funkcionalnost ili da se oporavi od kvarova pre nego što se ove okolnosti naiđu u proizvodnji. Interna revizija treba da ima za cilj da proceni efektivnost aranžmana za operativnu otpornost njihove organizacije. Imajući to na umu, prvo treba da se definiše da li postoji dobra artikulacija i razumevanje šta operativna otpornost znači za organizaciju u kontekstu njihove specifične delatnosti, kao i personalnih osobenosti iskristalisanih kroz godine poslovanja. Ovo uključuje definisanje i identifikaciju poslovnih aktivnosti koje bi, u slučaju da dođe do pojave anomalija, mogle da utiču na kupce, dobavljače i druge zainteresovane strane, zajedno sa merama potrebnim da bi se obezbedilo da poslovanje ima kontinuitet i da bude profitabilno. Ovaj istraživački rad ima za cilj da istraži osnovne principe testiranja otpornosti na rizik i ponudi strukturirani okvir za definisanje robusnih, prilagodljivih procedura testiranja. Ispitujući postojeće metodologije, identifikujući praznine u praksi i predlažući proceduralni plan, ova studija nastoji da poboljša konzistentnost, pouzdanost i efikasnost procena otpornosti na rizik. Ishod će donosiocima odluka, inženjerima i stručnjacima za rizik pružiti uvide koji mogu da deluju kako bi ojačali svoje sisteme protiv očekivanih i nepredviđenih pretnji.

Uopšteno govoreći, u manje zrelom okruženju, veća je verovatnoća da će interna revizija uspeti da obezbediti vrednost usvajanjem pregleda i preporučivanjem obima svog rada i fokusiranjem svojih napora na procenu dizajna okvira. U organizacijama koje poseduju uhodane i temeljno uređene sisteme, funkcija interne revizije će imati jasniju verovatnoću da obezbedi osetnije veću sigurnost u domenu operativne efektivnosti. Interna revizija istovremeno treba da razmotri da li će proceniti operativnu otpornost kao samostalan pregled ili proceniti kako je otpornost koja je implementirana u okviru šireg, robusnijeg okvira. To znači dodavanje komponente otpornosti u delokrug pregleda u oblastima kao što su informacione tehnologije i sajber bezbednost, upravljanje lancem snabdevanja, kontinuitet poslovanja, oporavak od katastrofe i upravljanje operativnim rizikom. Interna revizija treba da formira sopstveni pogled na rizike koji bi mogli da umanje operativnu otpornost organizacije i/ili da izazovu operativnu nestabilnost kako bi se rukovodilo njenim obimom pregleda i programom testiranja. Ako je menadžment završio procenu zrelosti otpornosti, interna revizija treba da uporedi ove

rezultate sa sopstvenim pogledom na trenutnu poziciju. Mnoge organizacije razmatraju lekcije izvučene iz odgovora na krizu Covid-19 i suočavanja sa njom i to će obuhvatiti (direktno ili indirektno) elemente okvira otpornosti (3). Način na koje visoko strukturirani menadžment kompanije definiše ciljeve i preduzima napore kako bi realizovao određene unapred targetirane aktivnosti, može takođe da bude važan segment interesovanja za revizore. Međutim, česte i nove aktivnosti zakonodavnih vlasti i usvajanja i implementiranja novih propisa mogu jasno da rezultiraju rastom operativne otpornosti, osobito u slučajevima u kojima se manifestuje rizik od nezakonitog deljenja osetljivih informacija o klijentima. Na primer, prekid rada koji je Kraljevska banka Skotske imala 2012. nakon rutinske nadogradnje softvera koja je pošla naopako dovela je do kazne od 56 miliona funti, što je direktno posledično uticalo na brojne druge poslovne aktivnosti. Nedugo pre, pad Silicijumske doline banke i Prve republikanske banke u SAD je vratio sećanja na globalnu finansijsku krizu koja je počela 2007. godine, a analizirajući dokumentima koje su obelodanili regulatori, analitičari su došli obe banke su bile školski primeri lošeg upravljanja rizikom i nadzora. Osnovni uzrok kolapsa bio je nedostatak nadzora od strane funkcija upravljanja rizicima i regulatora sve većeg rizika sa kojim su se banke suočavale. Kao i u ranijoj finansijskoj krizi, neuspesi su pojačali potrebu za testiranjem na stres. Testovi stresa su vežbe koje finansijske institucije izvode da bi testirale svoju otpornost na nepovoljne ekonomske uslove. Testovi otpornosti na rizike sami po sebi nisu mogli da spasu banke, jer su oni samo jedan od nekoliko bitnih elemenata za oprezno upravljanje rizikom (12). Neuspeh banaka da se pripreme za promene kamatnih stopa rezultat je kombinacije nedostataka. Međutim, adekvatno testiranje na stres je moglo pomoći bankama da identifikuju rastuće rizike.

Slika 1: Ciljevi testiranja otpornosti na rizike



Izvor: Autori na osnovu (16) pristup dana 06.03.2025. godine u 14:57

Od finansijske krize, neke banke su uključile ili poboljšale stres testiranje u svoje procese upravljanja rizikom. Testovi su se pokazali posebno korisnim u pomaganju organizacijama da se kreću kroz makroekonomske neizvesnosti koje su rezultat globalne pandemije, inflacije i rasta kamatnih stopa. Kako je stresno testiranje postalo složenije i regulisano, interna revizija procenjuje aspekte kao što su način na koji se sprovode programi stres testova i njihove makroekonomske i poslovne hipoteze. Kako druge industrije uključuju testiranje stresa u svoje svakodnevne operacije rizika, one mogu naučiti lekcije iz bankarske industrije. Predmet rada je analiza koncepta otpornosti na rizik, naglašavajući važnost testiranja okvira i metodologija za procenu robusnosti sistema u različitim scenarijima rizika. Kroz sveobuhvatno testiranje rizika, zainteresovane strane mogu bolje razumeti snage i slabosti svojih trenutnih strategija, omogućavajući im da donesu informisane odluke o upravljanju rizikom, ublažavanju i prilagođavanju.

PLAN KONTINUITETA POSLOVANJA

Revizija plana kontinuiteta poslovanja, posmatrana sa aspekta strukturalnog definisanja, je zapravo ništa drugo do jedna visoko formalizovana procedura koja se primenjuje kako bi se procenio način na koji se upravlja procesima kontinuiteta poslovanja. Ona može da se izvršiti interno ili uz pomoć revizorske firme treće strane (10). To je u suštini definisan na način da pomogne kompanijama da identifikuju, spreče ili smanje rizike gde je to moguće, da se pripreme za rizike koji su izvan domena njihove kontrole i da promptno reaguju i da se oporave ako dođe do incidenta ili krize. Cilj planiranja kontinuiteta poslovanja je oporavak poslovanja u najkraćem vremenskom periodu, u situacijama kada dođe do narušavanja kontinuiteta poslovanja. Ovo planiranje doprinosi povećanju kompanijske otpornosti i nastavka poslovanja sa minimalnim prekidima.

Problemi kontinuiteta poslovanja za kompanije mogu da se manifestuju u različitim oblicima, često sa značajnim uticajem na poslovanje i poverenje klijenata. Nedavno je globalna pandemija postavila nove globalne izazove za bez presedana, kao što je potreba da kompanije brzo prebace značajan deo svoje operativne radne snage na aktivnosti na daljinu, odnosno rad od kuce, istovremeno upravljajući naglim porastom upotrebe digitalnog aktivnosti. Kontinuitet poslovanja je proaktivan proces dizajniran da osigura da organizacija može da nastavi da radi i pruža kritične usluge tokom i nakon ometajućeg događaja. Cilj kontinuiteta poslovanja je da se minimizira uticaj ovih poremećaja, obezbeđujući da organizacija može da održi osnovne funkcije i da se brzo vrati u normalno poslovanje. Planiranje kontinuiteta poslovanja osigurava da se kritične aktivnosti mogu nastaviti uprkos prekidima. Pouzdan pristup kompanijskim aktivnostima osigurava finansijsku stabilnost za sve zainteresovane strane i omogućava im da efikasno upravljaju svojim resursima i da izbegnu potencijalne neizvesnosti, kao i da donose pravovremene i jasne odluke (9). Ovo je od vitalnog značaja za održavanje nesmetanog funkcionisanja kompanijskog poslovanja na duže staze. Brojne kompanije rukuju osetljivim informacijama i upravljaju značajnim transakcijama. Bilo kakve nestabilnosti u tom domenu mogu

da naruše poverenje korisnika i da dovedu do značajnih finansijskih gubitaka. Istovremeno, brojni lokalni i globalni regulatorni organi i mandatorne organizacije obavezuju kompanije da imaju robusno upravljanje kontinuitetom poslovanja, uključujući planove i testiranje., dok svako nepoštovanje može dovesti do ozbiljnih kazni i gubitka kredibiliteta.

Revizija plana kontinuiteta poslovanja i njegove dokumentacije u odnosu na utvrđene standarde osigurava da je u skladu sa industrijskim praksama i kontrolama. Neka od pitanja kojima treba da se bave interni revizori prilikom razmatranja kontinuiteta poslovanja u kontekstu testiranja otpornosti kompanije na rizike mogu da budu, kako je menadžment razvio i implementirao planove za kontinuitet poslovanja koji su dizajnirani da održe pružanje usluge bilo u granicama tolerancije uticaja ili u okviru trenutnih organizacionih mogućnosti, odnosno da li je menadžment identifikovao i definisao važne poslovne usluge i artikulisao ishode potrebne za svaku od njih. Interni revizori treba da pregledaju programe obuke i podizanje svesti zaposlenih kako bi bili sigurni da su zaposleni upoznati sa svojim ulogama i odgovornostima u procesu planiranja i potencijalnog sprovođenja plana kontinuiteta poslovanja. Istovremeno treba obratiti pažnju da li je obezbeđena stalna obuka i da je efikasna u pripremi zaposlenih da pravovremeno odgovore na potencijalne neizvesnosti. Neophodno je i realizovati adekvatnu procenu kako kompanija upravlja rizicima trećih strana u vezi sa kontinuitetom poslovanja, uz sticanje dovoljno sigurnosti da dobavljači i drugi partneri imaju sopstvene snažne planove kontinuiteta poslovanja i da su oni usklađeni sa zahtevima institucije.

TESTIRANJE SCENARIJA

Testiranje scenarija je fundamentalni deo strategije operativne otpornosti organizacije. Operativna otpornost je osnovna sposobnost koja omogućava organizaciji da se prilagodi i napreduje na duge staze, čak i u uslovima koji se razvijaju. U kontekstu softvera, testiranje scenarija je mesto gde se simuliraju situacije iz stvarnog života kako bi se proverilo kako se određeni sistem ponaša u tim situacijama. Pomaže u identifikaciji i rešavanju potencijalnih problema i osigurava da softver radi ispravno u različitim praktičnim uslovima. U operativnoj otpornosti, testiranje scenarija je način da se vidi koliko će se dobro preduzeće ili organizacija nositi sa neočekivanim izazovima u situacijama iz stvarnog života. Pomaže im da se pripreme za poremećaje kao što su nestanci struje, sajber napadi ili prirodne katastrofe tako što testiraju kako će se njihove najvažnije poslovne usluge održati u tim scenarijima i da li su ove kritične operacije premašile prihvatljiv nivo tolerancije uticaja.

Važne poslovne usluge su osnovne funkcije na koje se kompanija oslanja da bi nastavila da radi. Ovo su kritične operacije bez kojih preduzeće ne može, a da ne rizikuje svoju sposobnost da pruži vrednost. Testiranje scenarija je sredstvo da se proveri kakav bi bio uticaj u realnom vremenu da je na bilo koju od ovih usluga uticao neočekivani događaj ili poremećaj za svaku važnu poslovnu uslugu, tolerancije uticaja moraju biti postavljene za maksimalno prihvatljiv nivo smetnji. Tolerancije udara određuju maksimalni nivo nestabilnosti koji se

može tolerisati. Stavljanjem ovih tolerancija uticaja na test, testiranje scenarija pomaže da se osigura da kompanija ne pređe na nivoe „nepodnošljive štete". Upravljanje kontinuitetom poslovanja uključuje sposobnost organizacije da održi operacije tokom neočekivanih kriza, služeći kao kratkoročna strategija odgovora na krizu. Dok se kontinuitet poslovanja bavi neposrednim izazovima, otpornost omogućava kontinuirano prilagođavanje i poboljšanje kako bi se održala korak sa dinamičnim poslovnim okruženjem. Testiranje scenarija je vitalna komponenta oba procesa, omogućavajući organizacijama da simuliraju i pripreme se za različite nepredviđene situacije i na duži i na kratak rok.

Testiranje je ključno za procenu tolerancije uticaja organizacije i utvrđivanje da li će njene strategije reagovanja na incidente omogućiti organizaciji da povrati poslovnu uslugu u okviru definisane tolerancije uticaja. Testiranje takođe daje organizaciji jasno razumevanje ozbiljnih, ali verovatnih scenarija koji mogu stvoriti maksimalan stres za poslovne usluge. Ozbiljni, ali verodostojni scenariji odnose se na situacije koje bi dovele do velikog uticaja i značajnih nestabilnosti, iako je malo verovatno da će se desiti . Organizacije treba da osiguraju da je njihov pristup testiranju i određivanju scenarija dobio odgovarajući izazov od strane višeg rukovodstva i da dobije njihovu podršku. Organizacije će morati da imaju okvir koji opisuje njihov pristup sprovođenju testova scenarija. Organizacije će posebno morati da razmotre kako su odredile svoje kriterijume za formulisanje ozbiljnih, ali verodostojnih testova specifičnih za usluge, uključujući faktore koji mogu da otežaju oporavak organizaciji (7). Kao deo svoje metodologije testiranja, organizacije takođe treba da razmotre dostupnost zaobilaznih rešenja i zamena.

Organizacije treba da testiraju niz scenarija, uključujući one u kojima predviđaju da će premašiti svoju toleranciju uticaja. Razumevanje okolnosti u kojima je nemoguće ostati u granicama tolerancije uticaja pružiće korisne informacije organizaciji. Odbori i više rukovodstvo će morati da procene da li je neodržavanje tolerancije uticaja u određenim scenarijima prihvatljivo i moraće da budu u stanju da objasne svoje obrazloženje regulatorima. Vežbe su uobičajena metoda testiranja ozbiljnih, ali verovatnih scenarija. Program vežbanja treba da kombinuje i najavljene i nenajavljene metode vežbanja. Jedan od glavnih nedostataka najavljenih vežbi je to što ne testiraju stanje stalne pripravnosti i sposobnost brzog reagovanja timova za kontinuitet poslovanja i kriznog menadžmenta. Metoda nenajavljenog vežbanja je veoma važna i ne koristi se toliko često koliko bi trebalo da bude u mnogim organizacijama. Incidenti se dešavaju bez upozorenja. Kompanije bi trebalo da stave veći akcenat na nenajavljene vežbe za testiranje stalne spremnosti timova i njihove sposobnosti da reaguju na iznenađujuću najavu vežbe.

ODGOVORI NA INCIDENTE

Organizacija koja je otporna po svojoj suštini i pojavi, poseduje široke operativne raspoložive kapacitete da predvidi, izbegne, pripremi i prilagodi se različitom spektru nestabilnosti i rastućim izazovima koji bi mogli potencijalno da se realizuju, odnosno

ostvare kao postepena promena u okruženju organizacije. Organizacija je sposobna da se prilagodi u izazovnim vremenima, sposobna je da se 'odskoči' i sposobna je da izađe iz situacije jača i sve snalažljivija. Suštinska definicija otpornosti, kao univerzalne kategorija koja je široko primenljiva u poslovnom svetu zapravo glasi da je otpornost direktna, suštinska sposobnost organizacije da održi ili povrati dinamički stabilno stanje, koje joj omogućava da nastavi sa radom nakon veće nestabilnosti i/ili u prisustvu kontinuirano dinamičnog i izazovnog okruženja. Organizaciona otpornost kao koncept se smatra dvostrukim jer se tiče i pojedinca unutar organizacije i same organizacije (5). Široko korišćen i referentni model za organizacionu otpornost je model otpornosti riblje kosti. U njemu je definisan specifičan opseg sposobnosti koje otporna organizacija poseduje, uključujući relevantne aktivnosti koje organizacija treba da izvrši kako bi dalje poboljšala svoju otpornost. Pored ovih sposobnosti i aktivnosti, brojne druge specifične karakteristike svojstvene otpornoj organizaciji.

Aktivnosti kao što su upravljanje kontinuitetom poslovanja i upravljanje krizama koje se tiču rukovanja krizama, uključujući upravljanje vanrednim situacijama, izuzetno su važne za organizacije koje rade u nerutinskim okruženjima kao što su krize i generalno se smatraju važnim faktorima koji doprinose otpornosti organizacije. BCM je proces strateškog upravljanja koji se koristi za identifikaciju potencijalnih pretnji organizaciji i obezbeđuje sistematski proces za ublažavanje efekata kriza, incidenata i prekida tvrde da je stepen u kome je organizacija dovoljno primenio BCM direktno povezan sa otpornošću te organizacije (14).

DIGITALIZACIJA

U sadašnjem digitalnom dobu, sajber bezbednost je fundamentalni aspekt organizacionog integriteta i prevazilazi jednostavna, tradicionalna pitanja informacionih sistema i praktičnog rada sa njima u svim sferama organizacionog poslovanja. Imajući na umu da pretnje po osnovu sajber bezbednosti uvek evoluiraju, organizacije moraju da upravljaju ovim rizicima proaktivno i reaktivno. U tom kontekstu funkcija interne revizije igra ključnu ulogu kao strateški saveznik u jačanju sajber otpornosti organizacije. Funkcija interne revizije obezbeđuje usklađenost sa korporativnim ciljevima povezujući operativne rizike sajber bezbednosti sa dugoročnim ciljevima. Korišćenjem tehnika kao što su ISO 27005 i NIST-ov okvir za sajber bezbednost, revizori pronalaze opasnosti i slabosti u rasponu od ransomvare-a i malvera do najrazličitijih tipova insajderskih pretnji. Jedan primer je identifikacija zastarelih konfiguracija zaštitnog zida koje su podložne napadima SKL import-a, u kojima zlonamerne SKL datoteke koriste napadači za modifikovanje baza podataka. Ovo skreće pažnju na određenu bezbednosnu ranjivost i naglašava neophodnost strateškog usklađivanja sajber bezbednosti. Dosledna kontrola sajber opasnosti je zagarantovana efikasnim upravljanjem sajber bezbednošću. Interni revizori procenjuju upravljačke strukture sa naglaskom na uloge, odgovornosti

i usklađenost sa politikom u poređenju sa standardima kao što su COBIT ili ISO/IEC 27001. Procena da li je strategija sajber bezbednosti kompanije dobro saopštena u celoj organizaciji i sadrži odredbe za česte revizije kao odgovor na nove pretnje, takav je primer nultog dana. Kroz testiranje planova reagovanja na incidente zasnovano na scenarijima, funkcija interne revizije procenjuje spremnost organizacije da se nosi sa sajber incidentima. Sa druge strane, ispitivanje protokola za identifikaciju incidenata, analizu, zadržavanje, iskorenjivanje i oporavak je deo toga. Kao opipljiva ilustracija može poslužiti stona vežba koja oponaša napad phishing-a koji rezultira eksfiltracijom podataka. Ovo daje trenutnu povratnu informaciju radi poboljšanja taktike odgovora i testira odgovor organizacije u realnom vremenu. Taktike sajber bezbednosti treba da se menjaju zajedno sa sajber pretnjama (13). Da bi odbranu organizacije bila ažurna, interna revizija je neophodna. Ovo uključuje procenu upotrebe naprednih tehnologija za prediktivne procene pretnji, kao što su mašinsko učenje i veštačka inteligencija. Ovo pomaže u proceni upotrebe sistema za upravljanje događajima i bezbednosno-obaveštajnih sistema zasnovanih na veštačkoj inteligenciji koji ispituju trendove pretnji i predviđaju moguća kršenja pre nego što se dogode.

Da bi sama procena spremnosti organizacije za sajber bezbednost bila i praktično realizovana, interni revizori koriste niz tehničkih instrumenata i metodologija, pre svega oni koriste alate kao što su Kualis ili Nessus. Oni pronalaze nedostatke sistema pre nego što ih napadači iskoriste. Pored toga, upotrebljavaju i alate za testiranje penetracije kao što su Metasploit ili Kali Linux se koriste za testiranje koliko je otporna mrežna odbrana na simulirane napade. Zamislite situaciju u kojoj interna revizija utvrdi da mreža kompanije nije pravilno segmentirana. Ovo poslednje bi moglo dozvoliti napadaču da napreduje po različitim osnova istovremeno izbegavajući različite odbrambene tehnike. Implementacijom segmentacije mreže koristeći VLAN (virtuelne lokalne mreže) u skladu sa sugestijom revizije, organizacija može drastično smanjiti površinu napada (1). Revizija koja otkriva da su članovi osoblja nenamerno koristili oštećenu SaaS uslugu treće strane, dovodeći podatke u opasnost, je još jedan primer. Kao rezultat revizije, mogu da budu postavljene značajno strožije smernice za upravljanje dobavljačima i može da bude preporučeno sprovođenje detaljne analize bezbednosnih procedura trećih strana. Ovo može u pojedinim situacijama i da obuhvata rutinske revizije i bezbednosne procene svih spoljnih dobavljača. Funkcija interne revizije je ključni partner za sajber bezbednost u digitalnom dobu (8). Interna revizija osigurava da mere sajber bezbednosti budu jake i dinamično povezane sa promenljivim pretnjama i ciljevima kompanije kroz temeljne procene rizika, preglede menadžmenta, procene kontrole, provere usklađenosti i tekuće prilagođavanje. Interna revizija može da planira snažnu odbranu kombinovanjem tehničkog znanja sa temeljnim razumevanjem strateškog cilja organizacije. Ovo čuva poverenje zainteresovanih strana, garantuje usklađenost sa propisima i štiti digitalnu imovinu. Put ka otpornosti na sajber bezbednost je u toku, a interna revizija je u prvom planu, vodeći organizacije sa stručnošću, predviđanjem i nepokolebljivom budućnošću (2).

ZAKLJUČAK

U brzo promenljivom i neizvesnom makroekonomskom okruženju, testiranje na stres će nastaviti da igra ključnu ulogu u organizacijama i biće pod nadzorom regulatora. Rizici koji se pojavljuju kao što su klimatske promene, sajber kriminal i prekid lanca snabdevanja će primorati više industrija da usvoje alate za testiranje stresa u svoje strateško planiranje i procese upravljanja rizikom. Ukoliko se osvrnemo na razmotreno pitanje kontinuiteta poslovanja u kontekstu testiranja otpornosti na rizike, za lica angažovana na poslovima interne revizije, obezbeđivanje adekvatnog, odnosno odgovarajućeg upravljanja kontinuitetom poslovanja nije samo regulatorni zahtev već kritična komponenta strategije upravljanja rizicima organizacije. Dobro razvijen i redovno testiran plan kontinuiteta poslovanja poboljšava operativnu otpornost, održava poverenje kupaca i obezbeđuje usklađenost sa regulatornim zahtevima (11). Fokusirajući se na ključne komponente kao što su procena rizika, strategija oporavka, obuke i komunikacije, interni revizori mogu da zauzmu ključnu ulogu u zaštiti svojih organizacija od potencijalnih nestabilnosti i obezbeđivanju brzog oporavka kada dođe do krize.

Testiranje scenarija je ključni deo operativne otpornosti. On gradi i demonstrira sposobnost da se reaguje i oporavi u okviru unapred definisanih nivoa tolerancije na udar. Mora se identifikovati niz ekstremnih, ali verovatnih scenarija šoka koji utiču na resurse potrebne za pružanje važne poslovne usluge koja se testira. To može uključivati stvari kao što su prirodne katastrofe, pandemije, društveni nemiri, sukobi, sajber napadi ili infrastrukturni problemi. Ove scenarije treba testirati da bi se utvrdilo da li će tolerancije na udar biti ispunjene. Jedini način na koji organizacija može da proceni svoju sposobnost da ostane u granicama tolerancije uticaja u ozbiljnim, ali verovatnim scenarijima poremećaja za svaku od svojih poslovnih usluga je kroz dobro razvijenu metodologiju testiranja scenarija. Testiranje scenarija omogućava firmama da steknu sveobuhvatno razumevanje otpornosti svojih važnih poslovnih usluga i da identifikuju oblasti u kojima treba preduzeti akciju da bi se otklonile ranjivosti kako bi se vremenom izgradila otpornost. Razumevanje ozbiljnih, ali verovatnih scenarija u kojima organizacija nije u stanju da ostane u granicama tolerancije uticaja koje je postavila, jednako je važno kao i razumevanje slučajeva u kojima organizacija može da ispuni svoje tolerancije. Odbor će takođe možda morati da se angažuje kako bi utvrdio da li su potrebna dodatna ulaganja za rešavanje nalaza iz scenarija u kojima bi organizacije prekršile svoje tolerancije uticaja. Odbor poseduje pristup operativne otpornosti u organizaciji i igra ključnu ulogu (15). Testiranje scenarija identifikuje slabosti, razotkriva ranjivosti i pruža uvide koje samo teorijsko planiranje ne može. Simulacijom scenarija iz stvarnog sveta, organizacija stiče iz prve ruke razumevanje kako će se ponašati u vremenima krize.

Testiranje otpornosti na rizik iz perspektive interne revizije je kritična funkcija u obezbeđivanju da su organizacije spremne da se snalaze i da se oporave od različitih rizika (4). Ovo istraživanje je naglasilo evoluirajući ulogu internih revizora u proceni i poboljšanju otpornosti organizacija primenom različitih metodologija, okvira i alata testiranja.

Angažovanjem u sveobuhvatnim procenama rizika, analizama scenarija i testovima na stres, interni revizori su sastavni deo identifikovanja ranjivosti, poboljšanja organizacione spremnosti i podrške dugoročnoj održivosti. Nalazi ove studije naglašavaju važnost usvajanja proaktivnog, sistematskog pristupa testiranju otpornosti na rizik. Međutim, on takođe priznaje izazove sa kojima se interna revizija suočava, uključujući složenost okruženja rizika koji se stalno menja, ograničenja resursa i ograničenja podataka. Uprkos ovim izazovima, istraživanje pokazuje da korišćenjem najboljih praksi, podsticanjem saradnje među odeljenjima i stalnim unapređenjem metodologija revizije, funkcije interne revizije mogu značajno doprineti jačanju otpornosti na rizik. Ovaj rad ne samo da pruža dragocen uvid u metodologije koje koriste interni revizori, već nudi i praktične preporuke za poboljšanje napora u testiranju otpornosti. Buduća istraživanja bi trebalo da nastave da istražuju dinamičnu prirodu otpornosti na rizik, posebno pošto nove tehnologije i globalni poremećaji preoblikuju okruženje rizika. Na kraju, pošto se organizacije suočavaju sa sve većom neizvesnošću, interna revizija će ostati ključni igrač u očuvanju njihove sposobnosti da izdrže i oporave se od negativnih događaja, obezbeđujući i kratkoročnu prilagodljivost i dugoročni uspeh. Kako testiranje otpornosti na rizike postaje sve složenije, interna revizija bi trebalo da prati iterativni, višegodišnji pristup kako bi se u potpunosti pokrio životni ciklus ovih programa. Glavni zaključak u radu je da interna revizija može u značajnoj meri da doprinese da se poboljšaju sposobnosti organizacija za testiranje otpornosti na rizik tako što jasnije definisati dizajn i implementaciju internih procedura i internih kontrola, kao i tako sto će da generise pravovremene i jasne rezultate testova otpornosti.

Literatura

1. Barrio, G., A. (2023). Risk: Testing Risk Resilience. Internal Audit Magazine. https://internalauditor.theiia.org/en/articles/2023/october/risk-testing-risk-resilience/
2. Ehiagwina, D., U., Akintayo, J., Kolapo, O., O. & Akinloye, O., A. (2024.) The role of internal audit function in enhancing risk management. https://doi.org/10.70382/hijbems.v06i7.012
3. Erarslan, I., Orcanli, K. (2024). MONITORING ACTIVITY IN THE RISK-ORIENTED INTERNAL AUDIT: A MODEL PROPOSAL. Denetişim. https://doi.org/10.58348/denetisim.1537295
4. Jakovljević, N., Dmitrović, V. (2024). AI and Internal Audit, Reporting Transformation. Conference: 43rd International Conference on Organizational Science Development https://doi.org/10.18690/um.fov.3.2024.27
5. Jeremić, N., Jakovljević, N. (2023). The role of internal auditors in preventing financial fraud in the Republic of Serbia. Trendovi u poslovanju 11(2):63-72. https://doi.org/10.5937/trendpos2302063J
6. Jeremić, N., Jakovljević, N., Jeremić, M. (2022). The role of internal auditing in business continuity. Revizor, 25(97-98), 53–71. https://doi.org/10.56362/Rev2298053J
7. Jeremić, N., Jeremić, M., Jakovljević, N. (2021). Agility of internal audit. Revizor. 24, (95-96), 57-76, https://doi.org/10.5937/Rev2196057J
8. Jeremić, N., Jeremić, M., Jakovljević, N. (2023). The role of audit in preventing financial frauds. Revizor 26(104):63-72. https://doi.org/10.56362/Rev23104063J
9. Jullianeth, L. & Fitriany, F. (2024). The Role of Internal Audit in Enhancing Risk Awareness at PT X. Eduvest - Journal Of Universal Studies 4(9):8341-8350. https://doi.org/10.59188/eduvest.v4i9.3787

10. Kovalev, N. (2025). Budgetary Risk and the Role by Internal Financial Audit in it is Management. Auditor 10(11):22-31. https://doi.org/10.12737/1998-0701-2024-10-11-22-31
11. Kurniawan, T., Bukit, R., B. & Erwin, K. (2023). The Factors Influencing the Risk Based Internal Audit in Improving the Effectiveness of Internal Audit. International Journal of Social Science and Business 7(4):1030-1041. https://doi.org/10.23887/ijssb.v7i4.51371
12. Udoh, O., R. (2024). Enhancing Internal Audit Efficiency for Effective Risk Management and Corporate Governance Frameworks. International Journal of Research Publication and Reviews 5(12):3646-3659. https://doi.org/10.55248/gengpi.5.1224.250122
13. Vakhorina, M. (2025). Internal Audit As a Key Management Tool: Goal Setting, Assessment and Risk Management. Scientific Research and Development Economics 13(1):18-22. https://doi.org/10.12737/2587-9111-2025-13-1-18-22
14. Van Maaren, I. (2022). A reference model for auditing organisational resilience. Maandblad voor Accountancy en Bedrijfseconomie 96(7/8): 201-211. https://doi.org/10.5117/mab.96.89573
15. Waulandari, P., P., Sudarma, M., Prihatiningtias, Y. & W., Baridwan, Z. (2025). Embracing resilience in a dynamic work environment: coping mechanisms of internal auditors in public higher education. Cogent Business & Management. https://doi.org/10.1080/23311975.2025.2473037
16. XCINA Consulting, Operational Resilience: Scenario Testing. Operational Resilience: Scenario Testing | Whitepaper.

Risk Resilience Testing: How to Define Procedures

Summary: In today's increasingly complex and interconnected world, organizations and systems across sectors face unprecedented levels of risk, ranging from financial instability to environmental disasters and cyber security threats. As the frequency and intensity of these risks grow, it becomes critical not only to identify potential vulnerabilities, but also to test and measure the resilience of systems in the face of these challenges. Risk resilience refers to the ability of a System, whether it is an organization, infrastructure or community, to anticipate, absorb, adapt and recover from disruptive events while continuing to function effectively. The subject of the paper is the analysis of the concept of risk resistance, emphasizing the importance of testing frameworks and methodologies for assessing system robustness in different risk scenarios. Through comprehensive risk testing, stakeholders can better understand the strengths and weaknesses of their current strategies, enabling them to make informed decisions about risk management, mitigation and adaptation. The main conclusion of the paper is that internal audit can significantly contribute to improving the ability of organizations to test resistance to risk by more clearly defining the design and implementation of internal procedures and internal controls, as well as by generating timely and clear results of resistance tests.

Keywords: internal audit, internal controls, risks, resilience.