LIDERSTVO I ZNAČAJ SISTEMSKOG PRISTUPA MENADŽMENTU RIZICIMA U POSLOVANJU

Mirko Gavrilović
Direktor sertifikacije i poslovnog unapređenja, SGS Beograd
Ivana Tepčević
Project Manager & Lead Auditor, SGS Beograd

Apstrakt

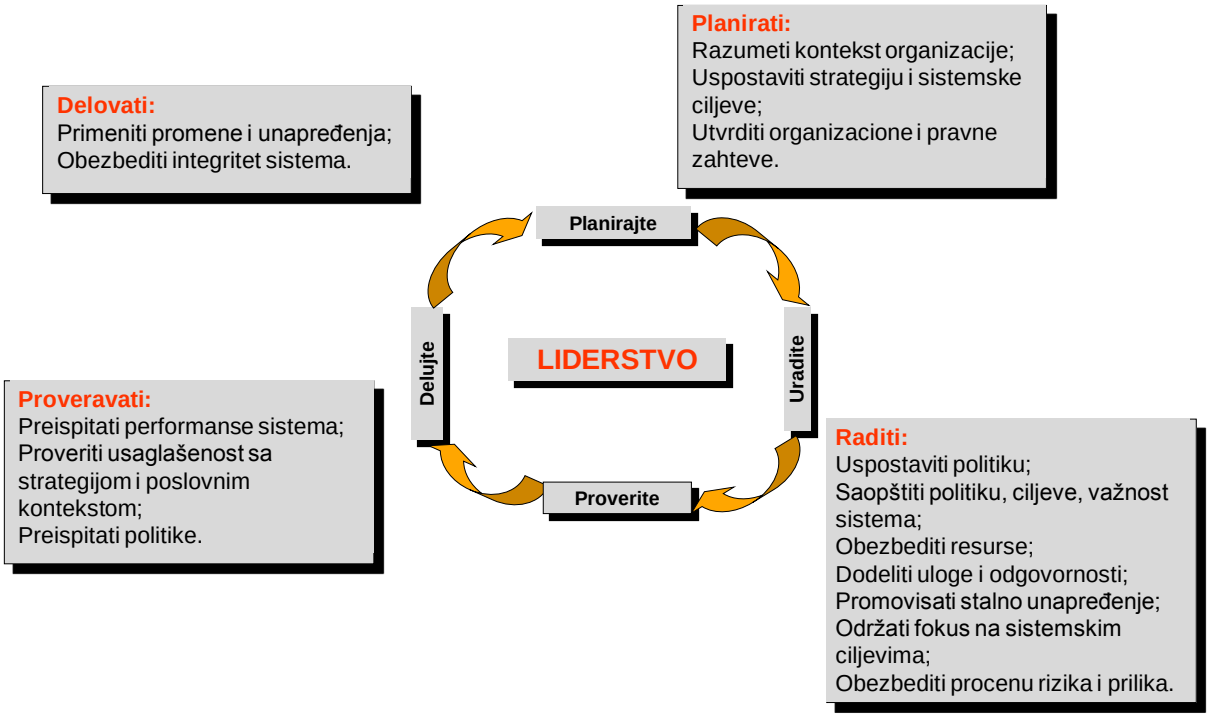
Dok požari, poplave i ostale vanredne situacije zauzimaju naslovne strane, skoro 90 procenata incidenata koji prete poslovanju su katastrofalni i ne prijavljuju se medijima, ali imaju razarajući uticaj na operativne sposobnosti organizacije. Menadžment se uglavnom tiče procesa, dok se liderstvo tiče ponašanja i atmosfere u organizaciji. Menadžment se oslanja na merljive veličine, kao što su efikasno planiranje ili upotreba organizacionih resursa. Umesto toga, liderstvo se oslanja na poverenje, inspiraciju, stav, sposobnost odlučivanja. Sve ovo je neophodno da bi se postigli ciljevi sistema menadžmenta, koji su u skladu sa strategijom organizacije i kontekstom u kojem organizacija posluje. Prema standardu ISO 9001:2015 liderstvo podrazumeva grupu ljudi koji upravljaju organizacijom na najvišem nivou i koji delegiraju ovlašćenja i obezbeđuju resurse u okviru organizacije, ali pre svega razumevajući poslovno okruženje i njegov uticaj na organizaciju. Neophodno je da budu identifikovani ključni rizici koji utiču na postizanje ciljeva, npr. zadovoljstvo klijenta. Svrha procesa procene rizika je da proceni verovatnoću i uticaj poznate pretnje na određenu funkcionalnost. One organizacije koje ne upravljaju kriznim situacijama jako dobro su upoznate sa padom svojih akcija na berzama, a čak i posle nekoliko godina još se nisu oporavile.

Svrha menadžmenta kontinuitetom poslovanja je da osigura organizaciji odgovor na katastrofu koja preti njenom opstanku. Cilj je da ojača žilavost organizacije, obezbeđujući joj da preživi gubitak operativnih sposobnosti. Sistem menadžmenta kontinuitetom poslovanja mora biti u vlasništvu organizacije i potpuno integrisani deo menadžment sistema u normalnim uslovima. Pošto žilavost organizacije zavisi kako od menadžmenta i operacija, tako i od tehnologije i geografskog položaja, onda ona mora biti razvijena kroz čitavu organizaciju – od najvišeg rukovodstva do operativaca na svim lokacijama. Upravljanje kontinuitetom poslovanja često uključuje i iznajmljivanje procesa i to sa dva aspekta, ispunjavanje zakonske regulative koja se odnosi na delatnost poslovanja organizacije i upotreba informacionih tehnologija (npr. cloud computing) u smislu replikacije kritičnih operacija.

ZAŠTO LIDERSTVO, A NE MENADŽMENT U ISO 9001:2015

Dodatni zahtev nove verzije standarda ISO 9001:2015 koji se odnosi na liderstvo obuhvata sledeće:

1. Sposobnost da se pokaže razumevanje poslovnog okruženja i kako ono utiče na strategiju organizacije. Potrebno je da sistemski ciljevi poslovanja budu usklađeni sa strategijom i postavljeni za sve relevantne nivoe u okviru organizacije. Organizacija mora da pokaže usaglašenost između sistemskih ciljeva i strateškog pravca koji je utvrdila.
2. Obezbeđivanje načina za identifikovanje značajnih, ključnih rizika koji mogu imati uticaj na postizaje sistemskih ciljeva, kao što je zadovoljstvo korisnika u slučaju ISO 9001.
3. Preispitivanje pristupa procesima menadžmenta i obezbeđivanje jasno definisanih odgovornosti i ovlašćenja za ove procese. Potrebno je da bude jasno identifikovano kako procesi doprinose postizanju sistemskih ciljeva i da bude utvrđeno koje su metode merenja.
4. Efektivnost kanala interne komunikacije treba da bude preispitana i politika treba da bude primenjena u okviru organizacije.
5. Procesi za upravljanje promenama i unapređenja u okviru organizacije treba da se preispitaju, a lideri treba da obezbede održivost efektivnosti sistema tokom unapređenja i organizacionih promena. Mnoge odgovornosti lidera su vrlo slične, dok se razlike odnose na specifičnosti koje karakterišu određeni standard.



Slika 1. Liderstvo u PDCA ciklusu

Liderstvo kao sposobnost da se motivišu ljudi ka zajedničkom cilju je važna veština u današnjem poslovnom svetu. Bez snažnog liderstva mnogi poslovi ne bi bili uspešni. Neke od najprepoznatljivijih osobina lidera su da motivišu na promenu i inspirišu zajedničku viziju, kao i da znaju kako da pridobiju ljude i usmere njihov rad na postizanje ciljeva, dobri lideri moraju biti samouvereni ljudi koji omogućavaju drugima da uspeju.

Menadžment se uglavnom tiče procesa, dok se liderstvo tiče ponašanja i atmosfere u organizaciji. Menadžment se oslanja na merljive veličine, kao što su efikasno planiranje ili upotreba organizacionih resursa. Umesto toga, liderstvo se oslanja na poverenje, inspiraciju, stav, sposobnost odlučivanja. Sve ovo je neophodno da bi se postigli ciljevi sistema menadžmenta, koji su u skladu sa strategijom organizacije i kontekstom u kojem organizacija posluje. Prema standardu ISO 9001:2015 liderstvo podrazumeva grupu ljudi koji upravljaju organizacijom na najvišem nivou i koji delegiraju ovlašćenja i obezbeđuju resurse u okviru organizacije, ali pre svega razumevajući poslovno okruženje i njegov uticaj na organizaciju.

Potrebno je da najviše rukovodstvo pokaže liderstvo i posvećenost i to obezbeđujući:

- Politiku i ciljeve menadžment sistema usaglašene sa strategijom poslovanja i kontekstom organizacije, kontekst organizacije je nov zahtev u odnosu na važeću verziju standarda, a liderstvo mora da pokaže razumevanje poslovnog okruženja i njegov uticaj na poslovanje.
- Da politika bude saopštena, razumljiva i primenjena u okviru organizacije.
- Integraciju zahteva sistema menadžmenta u poslovnim procesima unapređujući procesni pristup poslovanju.
- Resurse neophodne za sistem menadžmenta.
- Sistem menadžmenta koji ostvaruje planirane rezultate.
- Uključivanje, usmeravanje i podrška osobama koje doprinose efektivnosti sistema menadžmenta.
- Promociju stalnog unapređenja i inovacija.
- Da su odgovornosti i ovlašćenja za određene menadžment uloge dodeljeni, saopšteni i shvaćeni unutar organizacije.
- Održivost integriteta sistema menadžmenta kada se promene planiraju i implementiraju.

Neki od navedenih zadataka će biti i delegirani, ali odgovornost liderstva je da obezbedi da se one planiraju, implementiraju i ostvare. Lideri uspostavljaju svrhu i strategiju organizacije. Oni kreiraju i održavaju interno okruženje gde su ljudi potpuno posvećeni postizanju organizacionih ciljeva.

Primena principa liderstva omogućava da ljudi razumeju ciljeve organizacije i da su motivisani da ih dosegnu, da procene aktivnosti, usaglase i implementiraju na jedinstven način, da se potpuno izbegne nedostatak komunikacije između nivoa organzacije, da imaju jasnu viziju budućnosti organizacije, da dele iste vrednosti i etičke norme na svim nivoima organizacije, da se uspostavi poverenje i eliminiše strah, da se obezbede ljudima resursi za rad, obuke i sloboda da rade u okviru svojih odgovornosti i ovlašćenja, da su ljudi inspirisani, ohrabreni i da se njihov doprinos prepoznaje.

Ka ostvarivanju ciljeva put nije pravolinijski i bez prepreka. Ove prepreke mogu biti predvidive ili potpuno iznenađujuće. Efekat nesigurnosti koje ovi neplanirani događaji mogu imati na ostvarivanje ciljeva zove se rizik u poslovanju.

CILJEVI I RIZICI U POSLOVANJU

Standard ISO 31000:2009 Upravljanje rizicima – principi i smernice i ISO Guide 73:2009 jasno definišu svaki termin definicije rizika – efekat nesigurnosti prilikom ostvarivanja ciljeva i to:

- **Efekat** kao devijaciju od očekivanog i koji može biti pozitivan ili negativan.
- **Nesigurnost** kao stanje, delimičan nedostatak informacija koje se odnose na neplanirane događaje, njihove posledice ili verovatnoću da se dese.
- **Ciljevi** mogu imati različite aspekte (kao što su finansijski, bezbednosti i zdravlja na radu, životne sredine) i mogu se odrediti na različitim nivoima (strateški, organizacioni, projektni, procesni, operativni, itd.).

Kombinacija verovatnoće da se događaj desi i njegove posledice je rizik. Proces procene rizika određuje verovatnoću i uticaj različitih pretnji koje mogu da uzrokuju prekid poslovanja ili imaju značajne posledice na ekonomske performanse. Utvrđivanjem prioriteta, moguće je primeniti mere za smanjenje verovatnoće ili smanjenje uticaja pretnji.

Organizacije svih tipova i veličina suočavaju se sa internim i eksternim faktorima i uticajima koji dovode do nesigurnosti kad se ide ka ciljevima. Učinak koje ove nesigurnosti imaju na organizacione ciljeve je poslovni rizik koji se izražava u posledicama po organizaciju i to u vidu:

- Ekonomskih performansi (prihod,rashod, profit);
- Profesionalne reputacije;
- Uticaja na bezbednosti ljudi, životnu sredinu i društvo.

Sve organizacione aktivnosti u procesima uključuju rizik koji je potrebno da bude identifikovan od strane svih učesnika u procesima, da bude procenjen, tretiran i ponovo procenjen. Takođe je važno da rezidualni rizik bude kontinuirano praćen i preispitivan u planiranim intervalima vremena. ISO 31000 detaljno opisuje sistemski i logički proces upravljanja rizicima. Dok sve organizacije upravljaju rizicima do nekog nivoa, ISO 31000 uspostavlja određen broj principa i preporučuje da organizacije razviju, implementiraju i stalno unapređuju proces upravljanja rizicima čiji je cilj da bude integrisan u sve procese organizacije i da se rizicima upravlja na sistemski način, primenom jedinstvene metodologije za procenu rizika, jedinstvene strategije za tretman rizika i jasnom podelom odgovornosti i ovašćenja u sistemu upravljanja rizicima.

RIZICI I KONTINUITET POSLOVANJA

Procena rizika ima ozbiljne mane prilikom procene katastrofalnih rizika po operacije, i to iz sledećih razloga:

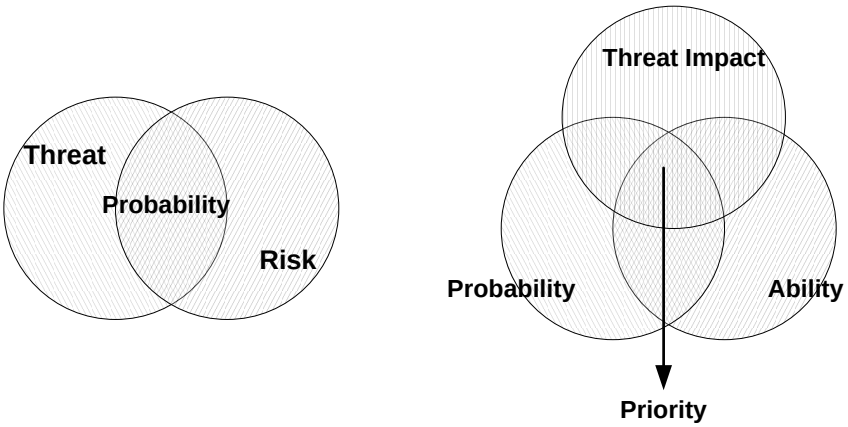
- Nemoguće je identifikovati sve pretnje.
- Procena verovatnoće je „procena“ i bazira se na iskustvenim i istorijskim informacijama koje ponekad mogu biti netačne.
- Posledice nisu precizno određene (visok, srednji, nizak) i menjaju se tokom vremena u različitoj meri.
- Opsezi rizika i uticaja često prenaglašavaju uticaj manje bitnih događaja.

Procenom rizika se može utvrditi neprihvatljiva vrednost rizika koja je poznata kao „slaba tačka prekida“. U najranijoj fazi procene rizika ovo treba da se istakne menadžmentu na najvišem nivou zajedno sa predlogom rešenja za tretiranje ovako visokog rizika. Odluka da se smanji, prenese ili prihvati ovakav rizik mora biti strateška, formalno dokumentovana i doneta od strane liderstva.

Analiza uticaja na poslovanje treba da bude završena pre procene rizika kako bi bile poznate kritične aktivnosti tj. kritične funkcije na koje procena rizika treba da se fokusira.

Svrha procene rizika je da:

- Identifikuje interne i eksterne pretnje koje mogu da prouzrokuju poremećaj ili prekid poslovanja
- Proceni verovatnoću da se pretnje ostvare kao i njihov uticaj na poslovanje
- Izlista pretnje po prioritetima prema unapred utvrđenoj formuli i
- Saopšti program mera za upravljanje rizicima kao i akcioni plan



Slika 2. Koncept procene rizika

- Rizik = Uticaj pretnje x Verovatnoća pretnje
- Prioritet = Rizik x Sposobnost da se kontroliše rizik
- Prihvatljiv rizik ili tolerancija rizika

Na ovaj način se određuje prioritet pretnji koje je najlakše kontrolisati, kao argumenti koji određuju najbolji povrat na investiciju u vidu vremena ili novca. Međutim, ovako su izostavljeni mnogi eksterni uticaji.

U drugim modelima procene rizika, procenjeni rizik se prvo ispita kao da nema implementiranih mera, a onda se ponovo ispita sa postojećim merama i sa poželjnim merama koje još nisu primenjene. Ovaj drugi korak služi da istakne probleme koji se odnose na pretpostavke o rizicima iz okruženja. To pokazuje da efektivnost mera mora uvek biti preispitana, a onda odgovarajuće korigovana ili unapređena.

Ako, posle preduzimanja drugog koraka, organizacija odluči da ne želi da unapredi postojeće mere – možda zbog povećanja troškova – onda menadžer rizika i menadžer za kontinuitet poslovanja moraju biti svesni ove činenice i uzeti je u obzir u svom pristupu riziku i kontinuitetu poslovanja.

Prihvatljiv rizik ili tolerancija rizika (nivo prihvatljivog rizika) je visina rizika koju je organizacija spremna da prihvati, da kontinuirano prati i preispituje nivo aktivnosti koje preduzima kako bi držala pod kontrolom identifikovane pretnje.

Procena rizika obuhvata sledeće pretpostavke:

- Sve realne pretnje mogu biti identifikovane.
- Tačna i primenljiva statistika za procenu verovatnoće pojavljivanja je na raspolaganju.
- Pretnje koje je lakše kontrolisati (ljudstvo ili zgrade) moraju biti nižeg prioriteta nego one koje nisu podložne uticaju (vremenski uslovi).
- Korišćenje numeričkih opsega gde se dodeljuje numerička vrednost uticaju tj. adekvatno kvantifikuje važnost određene imovine (ugled, postrojenje, itd.).
- Korišćenje numeričkog opsega (1, 2, 3, ...) predstavlja realnu vezu između različitih uticaja i verovatnoća.

Ključni koraci u proceni rizika su:

1. Razvoj adekvatnog mernog sistema za uticaje i verovatnoće.
2. Lista pretnji za najkritičnije poslovne procese određene iz analize uticaja na poslovanje.
3. Procena uticaja pretnje na organizaciju koristeći numerički merni sistem.
4. Određivanje verovatnoće ili učestanosti pojavljivanja pretnje i izračunavanje njene vrednosti u skladu sa mernim sistemom.
5. Izračunavanje rizika kombinovanjem rezultata dobijenih za posledicu i verovatnoću svake pretnje u skladu sa prihvaćenom formulom.
6. Opciono, kreiranje liste prioriteta rizika prema formuli koja uključuje meru sposobnosti da se kontroliše određena pretnja.
7. Dobijanje odobrenja od rukovodstva za listu prioriteta rizika.
8. Preispitivanje postojećih strategija upravljanja rizicima, sa postojećim merama za postupanje sa rizicima.

Razmotriti odgovarajuće mere za:

- Transfer rizika — (kroz osiguranje)
- Prihvatanje rizika — (tamo gde je posledica tj. verovatnoća niska)
- Smanjenje rizika — (kroz primenu novih mera, kontrola)
- Izbegavanje rizika — (uklanjajući uzroke rizika ili izvore pretnji)

Neophodno je obezbediti da planirane mere za postupanje sa rizikom ne povećavaju druge rizike. Na primer, iznajmljivanje (outsourcing) neke aktivnosti može da smanji neke vrste rizika, ali da poveća druge. Takođe je važno dobiti odobrenje od rukovodstva tj. menadžera za rizike ili menadžera za kontinuitet poslovanja za primenu mera za postupanje sa rizicima u smislu budžeta, vremena, odgovornosti (akcioni plan).

Rezultat procesa procene rizika obuhvata sledeće:

- Slabe tačke prekida u poslovanju
- Listu prioriteta pretnji za organizaciju ili određene procese koji su analizirani
- Strategiju upravljanja rizicima i akcioni plan za postupanje sa rizicima
- Prihvatanje identifikovanih rizika koji neće biti tretirani.

Procena rizika treba da se uradi onako kako je definisano u strategiji upravljanja rizicima na nivou organizacije. Preispitivanje procene rizika treba da se radi na godišnjem nivou za kritične procese ili češće ukoliko dođe do značajnih promena kako unutar organizacije tako i spolja, u okruženju.

Mada su to komplementarne discipline, fokus i metode kontinuiteta poslovanja se razlikuju u odnosu na metode upravljanja rizicima.

Upravljanje kontinuitetom poslovanja je holistički proces upravljanja kojim se identifikuju potencijalni uticaji koji ugrožavaju organizaciju i kojim se obezbeđuje okvir za razvoj otpornosti i sposobnosti za efektivan odgovor koji štiti interese ključnih aktera, ugled i brend, kao i aktivnosti koje prave novu vrednost.
Proces procene rizika kojim se identifikuju i procenjuju poznate pretnje je jedan od zahteva standarda ISO 22301. „Šta ako“ scenario daje odgovore na sledeća pitanja:

- Šta se može dogoditi i zašto?
- Koje su moguće posledice?
- Koja je verovatnoća da se posledice stvore?
- Da li postoje već primenjene mere koje smanjuju posledice ili redukuju verovatnoću dešavanja incidenta?

	Upravljanje rizicima	Upravljanje kontinuitetom poslovanja
Ključni metod	Analiza rizika	Analiza uticaja na poslovanje
Ključni parametri	Uticaj i verovatnoća	Uticaj i vreme
Tip incidenta	Svi tipovi događaja – mada obično segmentirani	Događaji koji uzrokuju značajne prekide poslovanja
Veličina događaja	Svih veličina (troškova) – mada obično segmentirani	Bitni za strateško planiranje: samo incidenti koji ugrožavaju opstanak biznisa
Obim	Fokus na upravljanje rizicima važnih za ključne poslovne ciljeve	Fokus na upravljanju incidentima nezavisno od ključnih kompetencija biznisa
Intenzitet	Od postepenog do iznenadnog	Iznenadni događaji

Tabela 1. Poređenje upravljanja rizikom i upravljanja kontinuitetom poslovanja

Proces menadžmenta kontinuitetom poslovanja je vlasništvo menadžmenta i mora biti integrisan potpuno u organizaciju kao sastavni deo menadžment sistema. Ovaj proces ima za cilj da razvije i unapredi otpornost organizacije.

Adekvatan plan kontinuiteta poslovanja neće samo zadovoljiti specifične zahteve, već će dati odgovore na poslovne rizike i doprineti podizanju svesti o ukupnim rizicima koji prete poslovanju jedne organizacije.

KAKO U KRIZNIM SITUACIJAMA ODRŽATI KRITIČNE OPERACIJE?

„To se nama neće desiti“, „ Uhvatićemo se u koštac – to uvek radimo“, „Previše smo jaki, da bismo propali“ i „Mi nismo meta terorista“ su najčešći odgovori od strane biznisa kada ih pitate zašto su slabo pripremljeni za slučaj katastrofe. Drugi veruju da će im osiguravajuće kompanije platiti svu štetu. Većina veruje da nemaju vremena za pripremu nečega što se nikad njima neće desiti. Sve ovo su primeri pogrešne procene jer su baš ovakve organizacije žrtve katastrofa.

Dok bombe, požari i poplave zauzimaju naslovne strane, skoro 90 procenata incidenata koji prete poslovanju su katastrofalni i ne prijavljuju se medijima, ali imaju razarajući uticaj na operativne sposobnosti organizacije. Mnoge situacije su van kontrole organizacije i one su najčešće prepuštene na milost i nemilost hitnih službi i dobavljača koji definišu rokove tokom prekida.

Nedavna istraživanja su pokazala da organizacije koje budžetiraju najviše na rizike, sisteme kontinuiteta poslovanja i održivost su najprofitabilnije u svojoj delatnosti – što dovodi do zaključka da je ulaganje u smanjenje rizika investicija, a ne trošak. One organizacije koje su odlučile da ne upravljaju kriznim situacijama jako dobro su upoznate sa padom svoje vrednosti na berzama, a čak i posle nekoliko godina još se nisu oporavile.

Standard ISO 22301:2012 Sistemi menadžmenta kontinuitetom poslovanja – Zahtevi – definiše zahteve koje kada jedna organizacija ispuni, ona praktično dobija organizaciju u vanrednim, kriznim situacijama. Glavna svrha sistema kontinuiteta je da osigura organizaciji adekvatan odgovor na katastrofu koja ugrožava njen opstanak. Neke organizacije imaju čak zakonske obaveze koje se odnose na kontinuitet poslovanja ili upravljanje rizicima kao deo korporativnog upravljanja.

PDCA model se primenjuje na procese upravljanja kontinuitetom poslovanja. Planiranje uključuje uspostavljanje politike kontinuiteta poslovanja, ciljeva, utvrđivanje procesa i procedura adekvatnih za sistem kontinuiteta. Implementacija obuhvata upravljanje procesima i operacijama i primenu uspostavljenog sistema kako bi se ispunili postavljeni ciljevi. Paralelno sa primenom procesa provere vrši se praćenje i preispitivanje pokazatelja procesa u odnosu na uspostavljene kriterijume (standard, politike, ciljeve, procedure) kako bi se sistem unapredio ili ispravile neusaglašenosti preduzimanjem korektivnih mera. Ponovnim razmatranjem predmeta primene, politika i ciljeva kontinuiteta poslovanja, kao i rezultata preispitivanja od strane najvišeg rukovodstva sistem kontinuiteta se održava i kontinuirano poboljšava.

Za organizaciju koja je na više lokacija, neophodno je definisati maksimalnu geografsku udaljenost katastrofe tj. do koje mere će doći do gubitka resursa neohodnih za preživljavanje organizacije. Na primer, zemljotres u jednoj državi neće dovesti do prekida operacija u filijali koja je u nekoj drugoj državi koju nije pogodio zemljotres, ali do koje mere će uticati na kontinuitet poslovanja to se mora proceniti.

Ovde je nekoliko osnovnih pitanja koja bi trebalo razmotriti za svaku aktivnost:

- U okviru kog vremenskog perioda se ova aktivnost mora povratiti?
- Na kojim lokacijama se ova aktivnost preduzima?
- Koji su uticaji na aktivnost, na primer periodi najvećeg intenziteta, najvećeg pritiska, izveštavanja, najveća iskorišćenost resursa, itd.?
- Koja je posledica ukoliko se aktivnost uopšte ne nastavi?
- Koliko organizacija može da traje bez ove aktivnosti?
- Da li postoji alternativa ovoj aktivnosti? Koja?

Rezultati analize uticaja na poslovanje su:

1. Maksimalni period prekida koji se može tolerisati, kao i priroda posledice na svaku aktivnost
2. Ciljna tačka oporavka tj. tačka do koje informacije moraju biti oporavljene tako da omogućavaju izvršavanje aktivnosti kada se uspostave.

Najbolja praksa preporučuje da se analiza uticaja na poslovanje preispituje najmanje jednom godišnje ili češće u slučaju značajnih promena u poslovanju, značajnih promena u internim biznis procesima, lokacijama, tehnologiji ili značajnim promenama u eksternom poslovnom okruženju – kao što je tržište ili regulativa.

Sistem menadžmenta kontinuitetom poslovanja doprinosi znatno većoj otpornosti organizacije i društva da preživi, ukoliko izgubi delimično ili potpuno svoje operativne sposobnosti u smislu gubitka ljudi, opreme, infrastrukture. Otpornost organizacije zavisi kako od menadžmenta tako i od operacija, tehnologije i geografskog položaja, i samim tim mora biti razvijana kroz čitavu organizaciju – od najvišeg rukovodstva do operative i celokupnog lanca snabdevanja. Pokretači jačanja otpornosti organizacije su najviše rukovodstvo (liderstvo) i klijenti, kao i svi oni koji zavise od organizacije na neki način. Pored finansijskih gubitaka izazvanih katastrofom, najznačajnije posledice koje organizacija može da ima, tiču se gubitka ugleda ili gubitka poverenja da rukovodstvo nije u stanju da upravlja organizacijom u kriznim situacijama. Suprotno, dobro upravljanje u kriznim situacijama može povećati ugled organizacije i najvišeg rukovodstva.

ZAKONSKI OKVIR ZA UPRAVLJANJE RIZICIMA

Jedan od benefita implementacije ISO standarda koji se odnose na sisteme menadžmenta je usaglašenost sa zakonskim zahtevima i ostalom regulativom, kako lokalno, u zemlji u kojoj se posluje, tako i šire, poštujući međunarodne direktive.

Standard ISO 31000 koji pruža okvir za dobru praksu upravljanja rizicima korišćen je prilikom pripreme Priručnika za upravljanje rizikom i procenu rizika u javnom sektoru od strane Ministarstva finansija i privrede. Ovaj Priručnik definiše koncept rizika i opisuje način na koji se rizik može identifikovati, proceniti i tretirati, pratiti i preispitivati. Postupanje u skladu sa Priručnikom ima za posledicu kreiranje registra rizika.

Na osnovu Zakona o budžetskom sistemu 2013. godine je donet Pravilnik kojim je definisano da „upravljanje rizicima obuhvata identifikaciju, procenu i kontrolu nad neplaniranim događajima i situacijama koje mogu imati suprotan efekat na ostvarivanje ciljeva korisnika javnih sredstava sa zadatkom da pruži razumno uveravanje da će ti ciljevi biti ostvareni.“ Rizik je definisan kao „mogućnost nastanka događaja čija bi se posledica mogla odraziti na postizanje ciljeva privrednog subjekta,“ što je praktično preuzeta definicija iz ISO 31000:2009. Vrednost rizika se izražava kao proizvod posledice iskazane novčanom vrednošću i verovatnoćom nastanka događaja. Na ovaj način se dobija vrednost rizika izražena u novčanom iznosu, na osnovu čega najviši menadžment može da donese odluku o nivou prihvatljivog rizika i može planirati budžet za rizike na godišnjem nivou. Ovaj Pravilnik opisuje proces upravljanja rizicima po fazama i način na koji se organizuje sistem upravljanja rizicima u javnom preduzeću. Takođe, definiše i strategiju upravljanja rizikom kao normativni akt.

Zakon o javnim preduzećima uvodi termin politika upravljanja rizicima i određuje da je Komisija za reviziju odgovorna za pripremu i sprovođenje ove politike. Ova Komisija to radi na osnovu ocene procesa upravljanja rizicima koja se sprovodi najmanje jednom godišnje, kao i na osnovu analize upravljanja glavnim rizicima, i načina na koji su uticali na poslovanje i stvaranje vrednosti. Istovremeno Komisija mora raspolagati informacijama o ključnim rizicima koji utiču na strategiju organizacije. Sadržaj strategije nije definisan propisima, međutim elementi strategije mogu biti

određeni na osnovu međunarodnih standarda interne kontrole, kao i ISO standarda koji sadrže zahtev za implementacijom procesa upravljanja rizicima u oblasti na koju se standard odnosi.

Zakonom o vanrednim situacijama „uređuju se delovanje, proglašavanje i upravljanje vanrednim situacijama – sistem zaštite i spasavanja ljudi, materijalnih i kulturnih dobara i životne sredine od elementarnih nepogoda, tehničko-tehnoloških nesreća - udesa i katastrofa, posledica terorizma, ratnih i drugih većih nesreća." Vanredna situacija je definisana kao stanje kada rizici i posledice nepredviđenih događaja su takvog obima i intenziteta po ljude, životnu sredinu i materijalna dobra da ih nije moguče otkloniti tekućim kontrolama, zbog čega je potrebno primeniti dodatne mere za smanjivanje ili otklanjanje rizika i posledice. Ovaj Zakon definiše obaveze za identifikaciju vanrednih situacija, procenu rizika, primenu preventivnih mera za sprečavanje i smanjenje posledica, definisanje planova reagovanja u vanrednim situacijama, uvežbavanje planova, stalne obuke i unapređenja.

U februaru 2016. godine stupio je na snagu Zakon o informacionoj bezbednosti, kojim se uređuju kontrole za upravljanje informacionom bezbednošću, odgovornosti i ovlašćenja i nadležni organi za praćenje primene ovog Zakona. Ovim Zakonom je predviđeno osnivanje Nacionalnog centra za prevenciju bezbednosnih rizika u informaciono-komunikacionim sistemima (nacionalni CERT), za koji je nadležna Regulatorna agencija za elektronske komunikacije i poštanske usluge.

Evropska komisija (EC) je 2013. godine predložila direktivu koja se tiče mera kojima se osigurava visok nivo mrežne i informacione bezbednosti u Evropskoj Uniji (EU). Dve godine kasnije Parlament se saglasio sa nacrtom Direktive za mrežnu i informacionu bezbednost (NIS Directive). Ova Direktiva oblikuje zakonske mere za unapređenje nivoa bezbednosti u EU i to:

- Povećanjem sposobnosti i resursa namenjenih bezbednosti informacija u digitalnoj formi kod svih članica;
- Jačanjem saradnje na temu bezbednosti informacija između svih članica;
- Obezbeđivanjem dobro razvijene prakse upravljanja rizicima u ključnim sektorima (kao što su energija, transport, bankarstvo i zdravstvo).

Implementacijom NIS direktiva dobijaju sve zainteresovane strane – građani, vlade, kompanije – koji će imati mogućnost da se oslone na bezbednije digitalne mreže i infrastrukturu da bi pružili svoje usluge u lokalnim zemljama i preko granice.

Sve aktivnosti koje uređuje NIS direktiva su podržane od Evropske agencije za mrežnu i informacionu bezbednost (ENISA), kao i evropskog CERT-a. Kako bi se pomoglo malim i srednjim kompanijama da se uhvate u koštac sa rizicima informacione bezbednosti, definisane su smernice i online NIS platforma u vidu portala za razmenu znanja i dobre prakse. Nedavno je osnovan i Centar za evropski sajber kriminal koji je osnovao Europol i koji bi trebalo da deluje kao centralna tačka za borbu protiv sajber kriminala u EU.

U poslednje dve godine aktivnosti po pitanju bezbednosti informacija su vrlo intenzivne između EU i SAD u smislu osnivanja zajedničkih organizacija i donošenja regulative koja uređuje bezbednost informacija u biznisu, zaštitu ličnih podataka građana i lakše detektovanje rizika i pretnji u digitalnom okruženju primenom pre svega tehnoloških rešenja i podizanjem svesti kod svih učesnika na tržištu.

KOJA TEHNOLOGIJA OBEZBEĐUJE KONTINUITET POSLOVANJA?

Identifikujući unapred potencijalne uticaje iznenadnih katastrofa na poslovanje, moguće je pripremiti odgovor i utvrditi prioritete delovanja sve sa ciljem dostizanja žilavosti organizacije u segmenitima kao što su bezbednost, infrastruktura i IT.

Jedan od ključnih benefita cloud computing tehnologije, koji se često previdi je kako cloud computing može da obezbedi kontinuitet poslovanja i brz oporavak od katastrofe. U današnjoj ekonomiji, kompanije svih veličina moraju da pronađu način da isporuče usluge, da obezbede kvalitet i pouzdanost, kontinuirano svojim kupcima i klijentima. Cloud computing predstavlja pristupačno rešenje za kontinuitet usluge i oporavak od katastrofe, posebno za male i srednje kompanije što se tiče troškova, za razliku od velikih organizacija čije rešenje zahteva znatno veći budžet.

Tradicionalne metode kontinuiteta poslovanja mogu biti ekstremno skupe. Obično zahtevaju kupovinu i održavanje infrastrukture u vidu hardvera, platformi, softvera koja će podržati kritične operacije, a to se svodi na replikaciju data centra koji uključuje dovoljno prostora za poslovne podatke, dobre komunikacije, kritične aplikacije i mere zaštite koje je potrebno implementirati na kritičnoj infrastrukturi, kako bi se održao kontinuitet bezbednosti informacija i u vanrednim situacijama. Dodatno ovaj data centar bi morao da bude na udaljenoj lokaciji u odnosu na primarnu.

Kapitalni troškovi za dodatni hardver, instalacija i podešavanje aplikacija, sinhronizacija podataka na obe lokacije, redovna testiranja funkcionalnosti, tekuće održavanje sekundarne infrastrukture (update

softvera, upgrade svaki put kada se desi na produkciji, itd.) predstavljaju preventivne aktivnosti koje je neophodno da budu pripremljene i uvežbane za slučaj vanredne situacije.

Većina kompanija su male i srednje i one nisu u mogućnosti da imaju investiciju ove vrste, već žive sa rizikom da nestanu ili pretrpe ozbiljne poslovne gubitke za slučaj katastrofe. Pre svega za ove kompanije je namenjeno cloud computing rešenje gde one za mala sredstva u vidi operativnih mesečnih troškova mogu da priušte sebi i svojim klijentima kontinuitet isporuke usluge i brz oporavak od katastrofe.

Velike kompanije često razvijaju privatna cloud computing rešenja ili hibridna cloud rešenja u partnerskom odnosu sa provajderom cloud usluge. I za njih je ovo jeftinije i racionalnije rešenje nego kopija postojećeg data centra.

Da bi kompanija znala kako da prepozna pouzdanog cloud provajdera u smislu kvaliteta usluge, bezbednosti podataka, ispunjavanja zakonskih normi i ispunjavanja dogovorenih parametara isporuke servisa EuroCloud Europe organizacija, podržana od EC je razvila sertifikacionu šemu Star Audit certification kojom se uređuje tržište cloud service provajdera. Svi cloud servisi koji su sertifikovani prema ovoj šemi sertifikacije pružaju svojim korisnicima garanciju koja se odnosi na kontinuitet servisa, bezbednost poslovnih podataka i zaštitu privatnih podataka na nivou kvaliteta koji zahteva sertifikat Star Audit kriterijum.

ZAKLJUČAK

Liderstvo kao sposobnost da se motivišu ljudi ka zajedničkom cilju je važna veština u današnjem poslovnom svetu. Bez snažnog liderstva mnogi poslovi ne bi bili uspešni. Neke od najprepoznatljivijih osobina lidera su da motivišu na promenu i inspirišu zajedničku viziju, kao i da znaju kako da pridobiju ljude i usmere njihov rad na postizanje ciljeva, dobri lideri moraju biti samouvereni ljudi koji omogućavaju drugima da uspeju.

Menadžment se uglavnom tiče procesa, dok se liderstvo tiče ponašanja i atmosfere u organizaciji. Menadžment se oslanja na merljive veličine, kao što su efikasno planiranje ili upotreba organizacionih resursa. Umesto toga, liderstvo se oslanja na poverenje, inspiraciju, stav, sposobnost odlučivanja. Sve ovo je neophodno da bi se postigli ciljevi sistema menadžmenta, koji su u skladu sa strategijom organizacije i kontekstom u kojem organizacija posluje. Lideri uspostavljaju svrhu i strategiju organizacije. Oni kreiraju i održavaju interno okruženje gde su ljudi potpuno posvećeni postizanju organizacionih ciljeva. Ka ostvarivanju ciljeva put nije pravolinijski i bez prepreka. Ove prepreke mogu biti predvidive ili potpuno iznenađujuće. Efekat nesigurnosti koje ovi neplanirani događaji mogu imati na ostvarivanje ciljeva zove se rizik u poslovanju.

Kombinacija verovatnoće da se događaj desi i njegove posledice je rizik. Proces procene rizika određuje verovatnoću i uticaj različitih pretnji koje mogu da uzrokuju prekid poslovanja ili imaju značajne posledice na ekonomske performanse. Utvrđivanjem prioriteta, moguće je primeniti mere za smanjenje verovatnoće ili smanjenje uticaja pretnji.

ISO 31000 uspostavlja određen broj principa i preporučuje da organizacije razviju, implementiraju i stalno unapređuju proces upravljanja rizicima čiji je cilj da bude integrisan u sve procese organizacije i da se rizicima upravlja na sistemski način, primenom jedinstvene metodologije za procenu rizika, jedinstvene strategije za tretman rizika i jasnom podelom odgovornosti i ovašćenja u sistemu upravljanja rizicima.

Upravljanje kontinuitetom poslovanja je holistički proces upravljanja kojim se identifikuju potencijalni uticaji koji ugrožavaju organizaciju i kojim se obezbeđuje okvir za razvoj otpornosti i sposobnosti za efektivan odgovor koji štiti interese ključnih aktera, ugled i brend kao i aktivnosti koje prave novu vrednost.

Proces menadžmenta kontinuitetom poslovanja je vlasništvo menadžmenta i mora biti integrisan potpuno u organizaciju kao sastavni deo menadžment sistema. Ovaj proces ima za cilj da razvije i unapredi žilavost organizacije.

Adekvatan plan kontinuiteta poslovanja neće samo zadovoljiti specifične zahteve, već će dati odgovore na poslovne rizike i doprineti podizanju svesti o ukupnim rizicima koji prete poslovanju jedne organizacije.

Standard ISO 22301:2012 Sistemi menadžmenta kontinuitetom poslovanja – Zahtevi – definiše zahteve koje kada jedna organizacija ispuni, ona praktično dobija organizaciju u vanrednim, kriznim situacijama. Glavna svrha sistema kontinuiteta je da osigura organizaciji adekvatan odgovor na katastrofu koja ugrožava njen opstanak. Neke organizacije imaju čak zakonske obaveze koje se odnose na kontinuitet poslovanja ili upravljanje rizicima kao deo korporativnog upravljanja.

Jedan od benefita implementacije ISO standarda koji se odnose na sisteme menadžmenta je usaglašenost sa zakonskim zahtevima i ostalom regulativom, kako lokalno, u zemlji u kojoj se posluje, tako i šire, poštujući međunarodne direktive.

Standard ISO 31000 koji pruža okvir za dobru praksu upravljanja rizicima korišćen je prilikom pripreme Priručnika za upravljanje rizikom i procenu rizika u javnom sektoru od strane Ministarstva finansija i privrede. Ovaj Priručnik definiše koncept rizika i opisuje način na koji se rizik može identifikovati, proceniti i tretirati, pratiti i preispitivati. Postupanje u skladu sa Priručnikom ima za posledicu kreiranje registra rizika.

U februaru 2016. godine stupio je na snagu Zakon o informacionoj bezbednosti, kojim se uređuju kontrole za upravljanje informacionom bezbednošću, odgovornosti i ovlašćenja i nadležni organi za praćenje primene ovog Zakona. Ovim Zakonom je predviđeno osnivanje Nacionalnog centra za prevenciju bezbednosnih rizika u informaciono-komunikacionim sistemima (nacionalni CERT), za koji je nadležna Regulatorna agencija za elektronske komunikacije i poštanske usluge.

Sve aktivnosti koje uređuje NIS direktiva su podržane od Evropske agencije za mrežnu i informacionu bezbednost (ENISA), kao i evropskog CERT-a. Kako bi se pomoglo malim i srednjim kompanijama da se uhvate u koštac sa rizicima informacione bezbednosti definisane su smernice i online NIS platforma u vidu portala za razmenu znanja i dobre prakse. Nedavno je osnovan i Centar za evropski sajber kriminal koji je osnovao Europol i koji bi trebalo da deluje kao centralna tačka za borbu protiv sajber kriminala u EU.

Identifikujuću unapred potencijalne uticaje iznenadnih katastrofa na poslovanje, moguće je pripremiti odgovor i utvrditi prioritete delovanja sve sa ciljem dostizanja žilavosti organizacije u segmenitima kao što su bezbednost, infrastruktura i IT.

U današnjoj ekonomiji, kompanije svih veličina moraju da pronađu način da isporuče usluge, da obezbede kvalitet i pouzdanost, kontinuirano svojim kupcima i klijentima. Cloud computing predstavlja pristupačno rešenje za kontinuitet usluge i brz poravak od katastrofe. Da bi kompanija znala kako da prepozna pouzdanog cloud provajdera u smislu kvaliteta usluge, bezbednosti podataka, ispunjavanja zakonskih normi i ispunjavanja dogovorenih parametara isporuke servisa EuroCloud Europe organizacija, podržana od EC je razvila sertifikacionu šemu Star Audit certification kojom se uređuje tržište cloud servis provajdera.

REFERENCE

RATEL (2016) Usvojen zakon o informacionoj bezbednosti http://www.ratel.rs/informacije/novosti.234.html?article_id=1724 *(Pristupano 21.05.2016.)*

EC (2015) Cybersecurity https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-strategy-2nd-high-level-conference *(Pristupano 21.05.2016.)*

BSI (2015) The importance of leadership in the new ISO standards (www.bsigroup.com/en-IN)

SGS Training Course, *Business Continuity Management Systems Auditor/Lead Auditor,* SGS 2014

ISO 22301:2012, *Social security – Business continuity management systems – Requirements*

ISO 31000:2009, *Risk management - Principles and guidelines*

GPG 2008, *Business Continuity Management Good Practice Guidelines 2008,* British Continuity Institution (BCI) 2007

Sharp, J (2008) *The Route Map to Business Continuity Management* : British Standards Institution

BS 25999-1, *Business continuity management – Code of practice,* British Standards Institution (BSI)

BS 25999-2, *Business continuity management – Specification,* British Standards Institution (BSI)