Periodična procena rizika vršena od strane interne revizije

I Uvod

Obrazac priručnika dobre prakse interne revizije, razvijen od strane Zajednice prakse (ZP) interne revizije PEMPAL, definiše važnost i uticaj koji efektivna strategija interne revizije i revizorski plan mogu imati na ispunjavanje sveukupnih ciljeva, zadataka i misije jedinice interne revizije. Planiranje obezbeđuje sistematski pristup u radu interne revizije i zahteva znanje i stručnost u velikom broju oblasti kao što je procena rizika i interna kontrola.

Ovaj Obrazac metodologije procene rizika detaljnije elaborira proces procene rizika kao što je opisano u odeljku 3.1.2 Obrasca priručnika dobre prakse interne revizije:

- Identifikaciju i definiciju odgovarajućih kategorija rizika;
- Identifikaciju i definiciju kriterijuma rizika radi uticaja i verovatnoće;
- Definiciju sadržaja bodovanja rizika i obrazloženje razloga za dodelu visoke, srednje ili niske ocene određenom riziku.

Ovaj obrazac je zasnovan na Standardu iz 2010. godine Instituta internih revizora (IIR) u kojem se nadovi da:

“Glavni izvršni revizor mora da utvrdi planove zasnovane na rizicima, kako bi utvrdio prioritete aktivnosti interne revizije usaglašene sa ciljevima organizacije”, a 2010.A1 zahteva da -
“Plan radnih angažovanja aktivnosti interne revizije mora biti zasnovan na dokumentovanoj proceni rizika, sprovedenoj najmanje jednom godišnje. U ovom procesu moraju biti uzeti u razmatranje davani polazni podaci višeg rukovodstva i upravnog organa”.

U procesu pravljenja nacrta obrasca se takođe koriste savetodavne beleške i smernice IIR, kao i opšte prihvaćeni primeri dobre prakse usvojeni za potrebe vršenja takvih vežbi.

Obrazac prati proces za vršenje procene rizika korak-po-korak i za svaki korak daje po praktični primer. U prilozima se može naći više primera korišćene terminologije.

II Zašto je procena rizika važan deo interne revizije?

Rukovodilac jedinice interne revizije je odgovorno lice za razvijanje strateškog i godišnjeg plana interne revizije. Ovi planovi su razvijeni preko procesa koji identifikuje i vrši prioritizaciju potencijalnih tema interne revizije. Sveukupni zbir potencijalnih tema (koje mogu postati operativne za procese ili jedinice) se naziva **revizorski univerzum**[i1]. Za svaku od tih relevantnih tema u okviru revizorskog univerzuma se moraju obraditi rizici ili mogućnosti.

Šta su rizici?

Rizik je mogućnost da će se određeni događaj desiti i da će negativno uticati na postizanje određenog cilja.

Ključni rizici su oni rizici koji, ukoliko se njima pravilno rukovodi, čine organizaciju uspešnom po pitanju postizanju njenih ciljeva, ili oni koji, ukoliko njima nije pravilno rukovođeno, čine organizaciju neuspešnom.

Ko je odgovoran za rizike?

Više rukovodstvo određene organizacije je odgovorno za ublažavanje rizika na jedan troškovno-efikasan način. Kao **„vlasnici rizika“** oni moraju da uspostave sistem za upravljanje rizicima.

Upravljanje rizicima se odnosi na sprečavanje od dešavanja loših stvari (ublažavanje rizika), ili na aktivnosti kod neuspevanja osiguravanja od dešavanja dobrih stvari (iskorišćavanje prilika). Iako mnogi rizici predstavljaju opasnost za određenu organizaciju, neuspevanje postizanja pozitivnih rezultata takođe može stvoriti prepreku u postizanju određenog cilja, a kao takvo, isto se mora smatrati rizikom.

Rizici, kao i način na koji se njima rukovodi od strane organizacije, trebaju biti nezavisno procenjeni od strane interne revizije. Rezultati ovakve procene će pružiti odgovarajuću periodičnu revizorsku pokrivenost određenog rizika rangiranog prema revizorskom univerzumu.

Pored toga, interna revizija će uzeti u obzir polazne podatke koji su dati od strane višeg rukovodstva kako bi osigurala da su prioritizovani rizici usklađeni sa stavovima i očekivanjima rukovodioca.

Kada procenjivati rizike?

Periodična procena rizika bi idealno trebala da se desi pred kraj godine, na primer tokom novembra ili decembra meseca. Međutim, svaki put kada se desi određeni značajni događaj, na primer revizija budžeta ili radikalno smanjenje troškova, izloženost riziku će se izmeniti, a određena nova (delimična) procena rizika treba biti

[1] Objašnjavanje procesa definisanja Revizorskog univerzuma nije pokriveno ovim obrascem, ali je to prvi korak u revizorskom procesu. U ovom obrascu isto je smatrano datim.

izvedena. Rezultati ove obnovljene procene rizika mogu voditi prema promenama u godišnjem planu interne revizije.

III Šta je proces procene rizika?

Svaka organizacija će se suočiti sa različitim vrstama rizika. Rizik predstavlja opseg mogućih rezultata, od najboljeg do najgoreg mogućeg scenarija. Proces procene rizika se sastoji iz **pet koraka**.

Korak 1. Postoji veliki broj rizika sa kojima se suočavaju organizacije tokom njihovog napora usmerenog ka izvršavanju svojih strategija i kod postizanja svojih ciljeva. Stoga je mudro započeti sa **kategorizovanjem rizika**.

Korak 2. Nakon toga, potrebno je da se za svaki rizik definiše (pod)-kategorija u okviru koje će rizici biti obrađeni. Ovaj deo procesa procene rizika se naziva **definisanje faktora rizika**.

Korak 3. Ne predstavlja svaki definisani rizik isti stepen pretnje za organizaciju. Zbog toga u Koraku 3, interna revizija procenjuje uticaj određenog rizika i verovatnoću dešavanja određenog rizika. Ovaj deo procesa procene rizika se naziva **definisanje kriterijuma rizika** u smislu kako će rizici biti procenjeni i mereni.

Korak 4. Kada se završi sa definisanjem relevantnih faktora rizika i kriterijuma rizika, potrebno je da se isti procene i boduju. Ovaj korak se naziva **bodovanje rizika**.

Korak 5. Rezultati procene različitih relevantnih rizika će biti konsolidovani u revizorskom univerzumu. Ovaj korak se naziva **definisanje revizorskog univerzuma prema rangiranim rizicima**, koji će predstavljati osnovu za razvijanje višegodišnjih i godišnjih planova interne revizije.

POLJE ZA VIZUELIZACIJU KORAKA

IV Koraci rizika – Procena u više detalja

1. Kako doći do kategorija rizika?

Kako bi se kategorizovali rizici, obavezno je pratiti metodologiju radi mapiranja i vršenja procene različitih rizika.

Dobar način za postizanje strukturisanog pristupa kod procene rizika je da se rizici dodele određenoj grupi kategorija rizika.

U javnom sektoru ima smisla za identifikovanjem sledećih širokih kategorija:

- *Upravljanje, strategija i planiranje.* Ovo je kategorija rizika koji se odnose na način na koji je sama organizacija organizovana, uključujući razvijanje njenih ciljeva, strategije i planiranja.
- *Poslovanja.* Ovo su rizici koji se odnose na ključna poslovanja određene organizacije. Kao primer, za Ministarstvo prosvete, ova kategorija će uključivati rizike povezane sa aktivnostima održavanja škola, zapošljavanja dobrih učitelja, izdavanja priznatih diploma, itd.
- *Infrastruktura*. Ovo su rizici koji se odnose na različite procese podrške u okviru određene organizacije. Primeri procesa podrške su ljudski resursi, informatička tehnologija, finansije, itd.
- *Usaglašenost*. Ovo su rizici koji se odnose na pravne i regulatorne zahteve. Primeri ovih rizika se odnose na neusaglašenost sa odredbama zakonima iz oblasti rada, fiskalnih zahteva, zdravstvenih i bezbednosnih propisa, itd.
- *Izveštavanje*. Ovo su rizici koji se odnose na finansijsko i poslovno, kao i obavezno ili zahtevano izveštavanje. Primeri su izjave rukovodilaca, finansijski izveštaji, saopštenja za štampu, itd.

Zbog toga što određene kategorije mogu postati veoma velike, možemo ih podeliti na pod-kategorije. Na primer, možemo podeliti **kategoriju Infrastruktura** na sledeće pod-kategorije:

- *Ljudski resursi*. Ova pod-kategorija može uključivati zapošljavanje, platne spiskove, obuku, penzioni program, učinke i nadoknade, itd.
- *Informatička tehnologija.* Ova pod-kategorija može uključivati IT infrastrukturu, menadžment promena, poslovni kontinuitet, informatičku bezbednost, zaštitu podataka i privatnost, licenciranje softvera, itd.
- *Pravne usluge*. Ova pod-kategorija će uključivati pravna i regulatorna pitanja, uključujući upravljanje ugovorima.
- *Finansije*. Ova pod-kategorija će uključivati sva pitanja iz oblasti budžetiranja, računovodstva i finansija.

POLJE SA PRIMEROM SLUČAJA KATEGORIJA RIZIKA

2. Kako doći do faktora rizika?

Interna revizija će morati da razvije listu svih potencijalnih i relevantnih rizika zasnovanu na polaznim podacima datih od strane rukovodioca, informacijama koje su dostupne u okviru organizacije, informacijama dobijenim od strane drugih strana po pitanju garancija ili na informacijama dobijenim od strane kolega. U praksi, interni revizori će intervjuisati odgovorne rukovodioce različitih jedinica određene organizacije („vlasnike rizika“), dok će istovremeno gledati i u naučne publikacije i prema postojećim profesionalnim telima koja se bave upravljanjem rizikom i

revizijom, kao i prema analizama rizika napravljenim od strane rukovodioca rizicima, itd.

Primeri faktora rizika su:

- Kategorija „Upravljanje, strategija i planiranje“.
    - Pod-kategorija „Organizaciona struktura“.
        - Rizik 1: Nejasna razgraničenja ovlašćenja
        - Rizik 2: Složen organizacioni dizajn
        - Rizik 3: Prekomerno diviziono fokusiranje
        - Rizik 4: …
- Kategorija „Infrastruktura“.
    - Pod-kategorija „Informatička bezbednost“.
        - Rizik 1: Nedovoljno efikasne kontrole pristupa
        - Rizik 2: Ranjivost na maliciozne napade
        - Rizik 3: Nedostatak podele dužnosti
        - Rizik 4: …

POLJE SA PRIMEROM SLUČAJA FAKTORA RIZIKA

3. Šta su kriterijumi rizika u organizacijama javnog sektora?

Svaka organizacija treba da definiše kriterijume koji će biti korišćeni za evaluaciju značajnosti rizika. Kriterijum rizika treba da odražava vrednosti određene organizacije, njene ciljeve i resurse. Određeni kriterijumi mogu biti nametnuti od strane, ili proizići iz pravnih i regulatornih zahteva i ostalih zahteva na koje je organizacija obavezna. Kriterijum rizika treba biti konzistentan sa javnom politikom upravljanja rizicima određene organizacije, biti definisan na početku svakog procesa upravljanja rizicima, kao i biti kontinuirano analiziran.

Rizici se mere u smislu **uticaja i verovatnoće**. Uticaj definiše finansijske ili nefinansijske posledice za organizaciju u slučaju da se određeni rizik desi. Verovatnoća definiše izglede za dešavanjem određenog rizika. Što je organizacija ranjivija prema ublažavanju specifičnih rizika, veća je verovatnoća da se određeni rizik može desiti.

Sledeći **kriterijumi za uticaj** mogu biti uzeti u razmatranje:

- *Finansijski uticaj*. Monetarne posledice za organizaciju ukoliko bi se desio rizik.
- *Uticaj na reputaciju.* Posledice u vezi sa reputacijom organizacije, ministra ili čak na višem nivou - reputacija celokupne zemlje u očima agencija za procenu rizika (rejting agencija), međunarodnih donatora, itd.

- *Regulatorni uticaj*. Dešavanje rizika može rezultovati u zamrzavanju budžeta ili programa, ili čak u kaznama (na primer, EU fondova).
- *Uticaj na misiju*. Misija organizacije može biti pod uticajem dešavanja određenog rizika.

Sledeći **kiterijumi za verovatnoću ili ranjivost** mogu biti uzeti u razmatranje:

- *Efektivnost sistema interne kontrole.* Ovo može biti procenjeno zasnovano na prethodnom iskustvu vršenja poslova interne revizije, ili na postojanju / odsustvu značajnijih neuspeha u nedavnoj prošlosti.
- *Brzina odgovora.* Ne mogu svi rizici imati neposredni uticaj na organizaciju. Brzina odgovora određuje vreme koje data organizacija ima za reagovanje na određeni rizik pri dešavanju istog. Što organizacija ima više vremena da ispravi stanje, manje je ranjivija.
- *Složenost poslovanja.* Složene poslovne operacije razume samo određeni mali broj ljudi u okviru organizacije. Što manji broj ljudi razume poslovanje veće su šanse da se može primetiti da nešto nije u redu.
- *Stopa vršenja izmena u okviru organizacije.* Stabilni sistemi i procesi čine organizaciju manje ranjivom.
- *Sposobnost ljudi i procesa.* Što su procesi više strukturisani i transparentni, to je organizacija manje ranjiva. Manje sposobni ljudi čine organizaciju ranjivijom.

Gore pomenuti kriterijumi su samo primeri. Adekvatni kriterijumi trebaju biti odabrani u zavisnosti od specifičnosti određene organizacije. Kao rezultat toga, mogu biti odabrani manji broj ili drugačiji kriterijumi.

Kod definisanja kriterijuma rizika, faktori koji trebaju biti uzeti u razmatranje trebaju da uključuju sledeće:

- prirodu i vrste uzroka i posledica koji se mogu desiti, kao i kako će oni biti mereni;
- kako će verovatnoća biti definisana;
- vremenski(e) okvir(e) verovatnoće i/ili posledicu(e);
- kako će nivo rizika biti utvrđen;
- stavove zainteresovanih strana;
- nivo na kojem rizik postaje prihvatljiv ili podnošljiv; kao i da li kombinacije višestrukih rizika trebaju biti uzeti u razmatranje i, ukoliko je to slučaj, kako i koje kombinacije trebaju biti razmotrene.

POLJE SA PRIMEROM SLUČAJA KRITERIJUMA RIZIKA

4. Kako bodovati rizike?

Jednom kada su relevantni rizici identifikovani, potrebno je da budu procenjeni i bodovani. Preporučuje se da se rizici ne boduju na čisto matematički način. Praktičnije je da se oni procene i boduju u skladu sa prethodno utvrđenom tabelom za procenu rizika. U postojećoj literaturi često nalazimo na tri nivoa bodovanja, ali ovo može navoditi na preterano bodovanje u srednjoj kategoriji. Tabela za procenu rizika bi u idealnom slučaju trebala da se sastoji od **četiri nivoa bodovanja**:

- Nizak rizik. Uticaj, kao i verovatnoća su procenjeni kao niski i nerelevantni.
- Srednje nizak. Uticaj, ili verovatnoća su procenjeni kao potencijalna, ali ne previše relevantna opasnost.
- Srednje visok. Uticaj, ili verovatnića su procenjeni kao potencijalna i relevantna opasnost.
- Visok. Uticaj, kao i verovatnoća su procenjeni kao visoki i relevantni.

Ljudi procenjuju rizike na različite načine. Određeni ljudi imaju averziju po pitanju rizika, dok su drugi spremni na preuzimanje rizika. Ukoliko jedna osoba proceni rizik kao visok, a druga kao nizak, rezultat nikad ne može biti srednja vrednost. Mora se doći do konsenzusa. Stoga se preporučuje da se unapred dogovori kako će rizici biti bodovani, koristeći se tabelom za procenu rizika.

POLJE SA TABELOM ZA PROCENU RIZIKA

Nekolliko primera:

- Može se smatrati da određeni rizik ima visok finansijski uticaj ukoliko pojavljivanje datog rizika može generisati gubitke koji su veći od 3% budžeta organizacije u pitanju.
- Reputacija neke organizacije može ozbiljno biti ugrožena ukoliko pojavljivanje određenog rizika može generisati nacionalnu i međunarodnu pokrivenost u štampi.
- Organizacija se može smatrati visoko ranjivom ukoliko pojavljivanje rizika utiče na veliki broj transakcija i/ili procesa.
- Organizacija može delovati manje ranjivom ukoliko su procesi kontrole dobro dizajnirani i implementirani, kao i ukoliko efikasno funkcionišu.

POLJE SA PRIMEROM SLUČAJA BODOVANJA RIZIKA