SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

Radionica o proceni rizika

1. Međunarodni standardi u oblasti interne revizije (eng.*IIA* standardi)
2. Praktične smernice bazirane na IIA
3. PEM-PAL-ov model Priručnika
4. Primer

OECD

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

2010 Planiranje

Izvršni rukovodilac organa revizije mora uspostaviti planove zasnovane na proceni rizika kako bi utvrdio prioritetne aktivnosti interne revizije usklađene sa ciljevima organizacije.

Interpretacija:

Izvršni rukovodilac organa revizije je odgovoran za uspostavljanje plana zasnovanog na proceni rizika. Izvršni rukovodilac organa revizije uzima u obzir upravljanje rizicima jedne organizacije, uključujući korišćenje nivoa apetita rizika postavljenih od strane menadžmenta za različite aktivnost ili delove organizacije. Ukoliko okvir ne postoji, izvršni rukovodilac ograna revizije koristi svoju sopstvenu procenu rizika nakon konsultacija sa višim rukovodiocima i odborom.

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

Praktične smernice 2010-1: Povezivanje revizorskog plana sa rizikom i njegova izloženost uticajima

1. Razvijanje ili ažuriranje revizorskog univezuma: liste svih mogućih revizija koje mogu biti izvršene. Izvršni rukovodilac organa revizije može dobiti polazne informacije u vezi revizorskog univerzuma od strane višeg rukovodstva i odbora.

2. Revizorski univerzum može uključivati komponente iz strategijskog plana organizacije. On će uzimati u obzir i reflektovati sveukupne poslovne ciljeve. Revizorski univerzum će uobičajeno biti pod uticajem rezultata procesa upravljanja rizicima.

3. Izvršni rukovodilac organa revizije priprema revizorske planove interne revizorske aktivnosti zasnovane na revizorskom univerzumu, polaznim podacima dobijenim od strane višeg rukovodstva i odbora, i na osnovu procene rizika i izloženosti koji utiču na organizaciju.

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

Praktične smernice 2010-1: Povezivanje revizorskog plana sa rizikom i njegova izloženost uticajima

4. Preporučljivo je izvršiti procenu revizorskog univerzuma barem na godišnjoj osnovi kako bi se odrazile poslednje aktuelne strategije i pravci rada organizacije. U nekim okolnostima, revizorski planovi mogu trebati biti češće ažurirani (na primer, na kvartalnom nivou) kako bi se odrazile izmene u poslovanju organizacije, njenim operativnim aktivnostima, programima, sistemima i kontrolama.

5. Postoji veliki broj modela rizika. Većina modela rizika koristi faktore rizika, kao što su uticaj, verovatnoća, materijalnost, likvidnost sredstava, stručnost rukovodstvenog kadra, kvalitet i poštovanje internih kontrola, stepen promene ili stabilnost, vremenski okviri i rezultati poslednjeg revizorskog angažmana, složenost i odnosi zaposlenih lica sa upravljačkim strukturama.

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

Praktične smernice 2010-2: Upotreba procesa upravljanja rizicima u planiranju interne revizije

1. Upravljanje rizicima je krucijalni deo osiguravanja razumnog upravljanja koji se tiče svih oblika aktivnosti neke organizacije. Upravljački kadar tipično koristi okvir upravljanja rizicima kako bi vršio procenu i dokumentovao rezultate procene.

2. Implementacija kontrola je jedan uobičajeni metod koji rukovodstveni kadar koristi kako bi upravljao rizicima u okviru svojih apetita rizika. Interni revizori vrše reviziju ključnih kontrola i daju osiguravanja rukovodstvenom kadru u vezi značajnih rizika.

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

Praktične smernice 2010-2: Upotreba procesa upravljanja rizicima u planiranju interne revizije

3. Dva fundamentalna koncepta rizika su inherentan rizik i rezidualni rizik.

4. Ključne kontrole mogu biti definisane kao kontrole ili kao grupe kontrola koje pomažu da se na drugi način neprihvatljivi rizici umanje do određenog prihvatljivog nivoa:

   - značajno umanjenje od inherentnog prema rezidualnom riziku

   - kontole koje služe radi umanjenja velikog broja rizika.

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

Praktične smernice 2010-2: Upotreba procesa upravljanja rizicima u planiranju interne revizije

5. Planiranje interne revizije mora da iskoristi proces upravljanja operativnim rizicima, u okolnostima gde je isti razvijen.

6. Specijalizovana ekspertiza može biti potrebna.

7. Interni revizori vrše procenu procesa upravljanja operativnim rizicima i utvrđuju koji delovi mogu biti korišćeni radi razvijanja plana aktivnosti interne revizije.

8. Pored toga, interni revizor vrši koordinaciju zajedno sa drugim zaduženim za pružanjem osiguranja, i uzima u obzir planirano oslanjanje na njihov rad.

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

Praktične smernice 2010-2: Upotreba procesa upravljanja rizicima u planiranju interne revizije

9. Povelja interne revizije uobičajeno zahteva da se aktivnosti interne revizije fokusiraju na oblasti visokog rizika, uključujući i inherentne i rezidualne rizike. Aktivnosti interne revizije trebaju da identifikuju oblasti najviših inherentih rizika, najviših rezidualnih rizika i ključnih kontrolnih sistema na koje se jedna organizacija najviše oslanja. Ukoliko aktivnost interne revizije identifikuje oblasti koje se smatraju neprihvatljivim sa rezidualnim rizicima, upravljački kadar mora o tome biti obavešten kako bi se rizik mogao otkloniti.

.

9. Interni revizori takođe pokušavaju da identifikuju nepotrebne, prekomerne, preobimne ili složene kontrole koje na neefikasan način umanjuju rizik. U ovim slučajevima, trošak kontrole može biti veći od koristi koja se može dobiti, i stoga postoji mogućnost za postizanje efikasnije dobiti pri dizajniranju kontrola.

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

Praktične smernice 2010-2: Upotreba procesa upravljanja rizicima u planiranju interne revizije

11. Kako bi se osiguralo da su relevantni rizici identifikovani, pristup ka identifikaciji rizika je sistematizovan i jasno dokumentovan.

12. Mnoge organizacije su razvile registre rizika koje dokumentuju rizike.

13. Neke organizacije mogu identifikovati nekoliko visokih (ili viših) inherentnih rizičnih oblasti. Iako takvi rizici mogu osiguravati adekvatnu pažnju usmerenih aktivnosti internih revizora, nije uvek moguće vršiti njihovu reviziju.

14. Kod odabira poslovnih jedinica ili sektorskih jedinica sa nižim nivoom rizika, revizija se mora periodično uključivati u plan aktivnosti internih revizora, kako bi im osigurala pokrivenost i potvrdila da se njihovi rizici nisu promenili.

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

Praktične smernice 2010-2: Upotreba procesa upravljanja rizicima u planiranju interne revizije

15. Plan aktivnosti interne revizije se uobičajeno fokusira na:
    - Neprihvatljive aktuelne rizike gde je neophodno angažovanje rukovodstvenog kadra. Ovo bi bile oblasti sa minimalnih ključnim kontrolama ili olakšavajućim faktorima koje više rukovodstvo želi da budu neodložno revidirane.
    - Kontrolne sisteme na koje se organizacije najviše oslanjaju.
    - Oblasti gde postoji velika razlika između inherentnih rizika i rezidualnih rizika.
    - Oblasti gde su inherentni rizici vrlo visoki.

16. Kada se planiraju pojedinačne interne revzije, interni revizor identifikuje i procenjuje rizike relevantne oblasti u kojoj se vrši revizija.

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

2010 Planiranje

2010.A1 Plan aktivnosti interne revizije i pratećih aktivnosti mora biti baziran na dokumentovanoj proceni rizika, i mora se sprovoditi barem jednom godišnje. Početne informacije dobijene od strane višeg rukovodstva i odbora moraju biti uzete u obzir tokom vršenja procesa.

2010.A2 Izvršni rukovodilac organa revizije mora identifikovati i uzeti u obzir očekivanja višeg rukovodstva, odbora i ostalih zainteresovanih strana pri pravljenju mišljenja o internoj reviziji, kao i kod ostalih oblika zaključaka.

2010.C1 Izvršni rukovodilac organa revizije treba uzeti u obzir prihvatanje predloženih konsultantskih angažovanja zasnovanih na potencijalu angažovanja radi unapređenja upravljanjem rizika, dodavanju na vrednosti, i unapređenju operativnosti organizacije. Prihvaćeni angažmani moraju biti uključeni u plan.

Predložene izmene Standarda 2010

Izvršni rukovodilac organa revizije mora uspostaviti **jedan određen** ***plan zasnovan na riziku (rizicima) kako bi utvrdio prioritete aktivnosti rada interne revizije, a koji trebaju biti usklađeni sa ciljevima organizacije.***

Interpretacija:

Izvršni rukovodilac organa revizije je odgovoran za razvijanje plana zasnovanog na rizicima. Izvršni rukovodilac organa revizije uzima u obzir okvir upravljanja rizicima jedne organizacije, uključujući nivoe prema apetitima rizika koje uspostavlja rukovodstvo prema različitim aktivnostima ili delovima organizacije. Ukoliko okvir ne postoji, izvršni rukovodilac organa revizije koristi svoje rasuđivanje u vezi rizika, ~~a nakon konsultacija sa višim rukovodstvom i odborom~~ uzimajući u obzir polazne podatke dobijene od strane višeg rukovodstva i odbora. Izvršni rukovodilac organa revizije mora izvršiti reviziju i prilagođavanje plana, a prema potrebi, kako bi odgovorio na izmene u poslovanju organizacije, prema rizicima, operacijama, programima, sistemima i kontrolama.

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

PEM-PAL-ov Priručnik o revizorskom univerzumu

- Celokupnost procesa, funkcija i lokacija podložnim revidiranju
- Horizontalni ili vertikalni pristup
- Ključni procesi
- Oblasti kritičke kontrole
- Upravljive komponente
- Dinamični univerzum

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

PEM-PAL-ov Priručnik o metodologiji procene rizika

- Definicija kategorija rizika: definiše koji rizici će biti obrađeni.
- Definicija kriterijuma rizika radi određenja njihovog uticaja i kontrole (ranjivost?).
- Definicija konteksta ocenjivanja rizika: u kojim situacijama će rizik biti ocenjen kao rizik visokog, srednjeg ili niskog nivoa? (srednje vrednosti!).

Metodologija i pristup procene rizika

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

Okvir rizika

Okvir rizika se koristi radi mapiranja identifikovanih ključnih rizika prema glavnim kategorijama rizika, a kako bi se osiguralo da su sve kategorije rizika pokrivene.

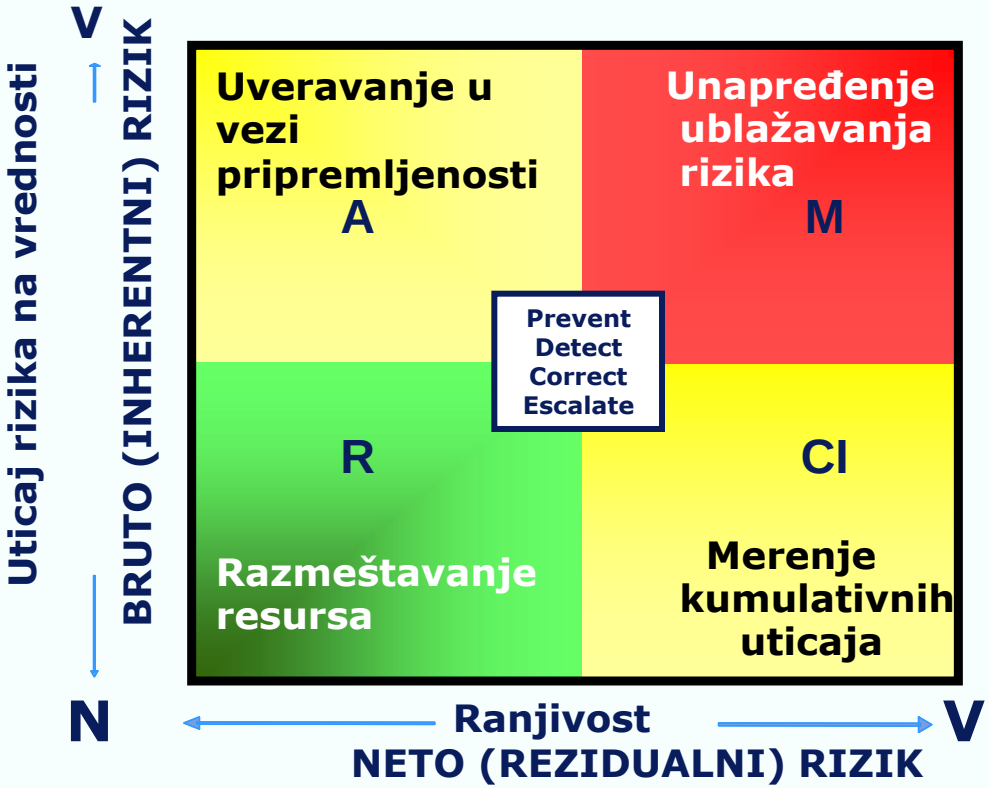
Prioritizacija rizika – Kriterijum uticaja (primeri)

UTICAJ	FINANSIJSKI	REPUTACIONI	PRAVNI / REGULATORNI	ZADOVOLJSTVO KORISNIKA	KAPACITET
Visok	Rizici koji mogu stvoriti gubitke > približno 3% operativnih prihoda.	Nacionalna i međunarodna pokrivenost u javnim medijima.	Značajne aktivnosti (npr. kazne, penali) koje su nametnute od strane Evropske komisije, lokalnih organa vlasti itd.	Značajan uticaj na postizanje ciljeva korisničkog (internog ili eksternog) zadovoljstva / metrika	Značajan uticaj na kapacitete organizacije prema promenama (procesima, organizacionim sistemima, proizvodima, itd.)
Srednji	Rizici koji mogu stvoriti gubitke između 0,5% i 3% operativnih prihoda.	Eskalacija aktivizma u okviru zajednice ili grupe korisnika, reginalna pokrivenost u javnim medijima.	Bilo koji oblik vladinog nadzora i/ili nadzora regulatornih vlasti, i/ili aktivnost korisnika usluga.	Umeren uticaj na postizanje ciljeva korisničkog (internog ili eksternog) zadovoljstva / metrika	Umeren uticaj na kapacitete organizacije prema promenama (procesima, organizacionim sistemima, proizvodima, itd.)
Nizak	Rizici koji mogu stvoriti gubitke < približno 0,5% operativnih prihoda.	Lokalna pokrivenost u javnim medijima.	Bilo koji oblik nadzora korisnika usluga.	Vrlo nizak uticaj na postizanje ciljeva korisničkog (internog ili eksternog) zadovoljstva /metrika	Vrlo nizak uticaj na kapacitete organizacije prema promenama (procesima, organizacionim sistemima, proizvodima, itd.)

Prioritizacija rizika – Kriterijumi izloženosti / ranjivosti (primeri)

RANJIVOST	PRETHODNO ISKUSTVO U VEZI RIZIKA	SVEPRISUTNOST	SPOSOBNOST (LJUDI)	SPOSOBNOST (PROCESI)	SPOSOBNOST (SISTEMI)
Visok	Iskustvo prethodno visokog nepovoljnog rizika.	Rizik ima uticaj na veliki broj transakcija i/ili procesa.	Ograničeni broj ključnog osoblja ili osoblje sa ograničenim sposobnostima za upravljanje rizicima.	Ne postoje procesne kontrole ili one ne funkcionišu onako kako su osmišljene.	Ne postoje sistemske kontrole, ili one ne funkcionišu na način kako su osmišljene.
Srednji	Iskustvo prethodno umerenog nepovoljnog rizika.	Rizik ima uticaj na umerenibroj transakcija i/ili procesa.	Ograničeni broj ključnog osoblja ili osoblje sa umereno ograničenim sposobnostima za upravljanje rizicima.	Procesne kontrole efikasno funkcionišu onako kako su osmišljene, ali njihov dizajn može biti unapređen.	Sistemske kontrole efikasno funkcionišu onako kako su osmišljene, ali njihov dizajn može biti unapređen.
Nizak	Iskustvo prethodno niskog nepovoljnog rizika.	Rizik ima uticaj na manji broj transakcija i/ili procesa.	Najveći broj osoblja ima visoku stručnost za upravljanje rizicima.	Procesne kontrole su osmišljene, implementirane i efikasno funkcionišu.	Sistemske kontrole su osmišljene, implementirane i efikasno funkcionišu.

Prioritizacija rizika – Mapa rizika



- **Ublažavanje** – Upravljačka strategija radi umanjenja ili minimizacije uticaja na raznjivost prema rizicima.
- **Osiguravanje** – Povećavanje nivoa poverenja koji postoji u odnosu na eksponiranost prema rizicima u okviru apetita rizika neke organizacije.
- **Razmeštanje resursa** – Određivanje da li su sredstva upravljanja rizicima bolja ukoliko su razmeštena negde drugde.
- **Kumulativni uticaj** – Dalje ispitivanje radi određivanja agregatnog uticaja određenog broja manjih uticajnih rizika

	B
1	**Segmenti podležni revidiranju**
2	**Informacija/konsolidacija informacionih sistema**
3	**Kontinuitet poslovnih procesa/plan oporavka od katastrofa**
4	**Procesuiranje zahteva**
5	**Regulatorna istraživanja**
6	**HIPAA**
7	**Razvoj novih sistema**
8	**Kontrola i sigurnost informativnih sistema**
9	
10	**Procesuitanje zahteva za farmaceuticima**
11	**Trezor**
12	**Rezervacije**
13	**Opšte kompjuterske kontrole**
14	**Litigacije**
15	**Odnos rizika – konfliktne usklađenosti**
16	**Naplate i plaćanja**
17	**Kontrole aplikacionih nivoa**
18	**Komisije brokera**
19	**Opšte računovodstvo**
20	**Obaveze prema dobavljačima (trgovina)**
21	**Kontrole finansijskog računovodstva**
22	
23	**Regulatorna usklađenost ljudskih resursa**
24	**Budžetiranje**
25	**Kompenzacije i benefiti**
26	**Javna nabavka**
27	**Administrativne usluge**
28	**Korporativna komunikacija**
29	
30	**Specijalni projekti**
	Administracija (Revizorska komisija / sastanci)
	Revizorski univerzum i procena rizika
	Menadžemtn i supervizija

Kategorija rizika	Ocenjivanje rizika	Budžetski sati	Preporučeno za svrstavanje u interni revizorski plan
	Score	hours	Internal Audit Plan
Visok	520	300	✓
Visok	520	300	
Visok	500	300	✓
Visok	500	200	
Visok	480	150	✓
Visok	480	200	✓
Visok	460	250	
Srednji	440	300	✓
Srednji	440	250	✓
Srednji	400	150	
Srednji	400	100	✓
Srednji	380	150	
Srednji	380	200	
Srednji	380	250	
Srednji	380	100	✓
Srednji	360	200	✓
Srednji	360	150	
Srednji	360	250	
Nizak	360	200	
Nizak	340	200	
Nizak	340	150	
Nizak	320	200	
Nizak	320	250	
Nizak	300	150	
Nije ocenjen	300	150	
Nije ocenjen	0	150	✓
Nije ocenjen	0	100	✓
Nije ocenjen	0	150	✓
	0	100	✓

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

Zaključak

- Potrebo je da prvo razvojemo adekvatni revizorski univerzum.
- Na drugom mestu, adekvatni kriterijumi rizika trebaju biti korišćeni. Nikakvi složeni matematički modeli nisu potrebni.
- Naposletku, rezultati naše procene rizika će imati smisla i revizorima i rukovodećem kadru.