Računovodstveni informacijski sustavi - RIS

Kontrola RIS-a

Prof.dr.sc. Dražena Gašpar

09.12.2015.

ZAŠTO kontrola

Glavni razlozi:

- *Osigurati razumnu vjerojatnost da će se postići ciljevi svakog poslovnog procesa*
- *Ublažiti rizik da će poduzeće biti izloženo nekom obliku štete, opasnosti ili gubitka*
- *Osigurati razumnu sigurnost da će se određene zakonske obveze ispuniti*

2

Prijetnje RIS-u

- ✓*Prirodne katastrofe*
- ✓ *Teroristički napadi*
- ✓ *Političke katastrofe*
- ✓ *Hardverske i komunikacijske greške*
- ✓ *Softverske greške*
- ✓ *Nehotično ponašanje koje dovodi do grešaka*
- ✓ *Namjerno izazivanje grešaka (računalni kriminal)*

3

Prijetnje RIS-u

- ✓*Prirodne katastrofe (uragani – Katrina New Orleans)*
- ✓ *Teroristički napadi (World Trade Center New York)*
- ✓ *Političke katastrofe (rat u BiH)*
- ✓ *Hardverske i komunikacijske greške*
- ✓ *Softverske greške (procjena gubitaka u USA preko 60 milijardi USD godišnje)*
- ✓ *Nehotično ponašanje koje dovodi do grešaka (pogreške pri unosu podataka,nepoštivanje procedura rada, nedovoljno obučeno osoblje) 65% sigurnosnih problema su ljudske greške*
- ✓ *Namjerno izazivanje grešaka (računalni kriminal) - nedozvoljen pristup podacima, lažiranje financijskih izvješća …)*

4

Istraživanje prijevara

1998. na 5000 USA kompanija i organizacija

1. *> 62% je imalo posla s nekim tipom prijevare*
    1. *21% je imalo gubitke > 1 mil. USD*
    2. *34% je imalo gubitke od 100.000 do 999.000 USD*
    3. *17% je imalo gubitke od 25.000 do 99.999 USD*
2. *5 najčešćih vrsta prijevare:*
    1. *Prijevara putem čekova*
    2. *lažne fakture i "fantomski" dobavljači*
    3. *prijevara putem kreditnih kartica*
    4. *zlouporaba računa za troškove*
    5. *krađa na popisu*

… godišnji gubici u USA preko 660 milijardi USD

5

Istraživanje prijevara

1987 – 1997 na 200 slučajeva lažnih financijskih izvješća

Kompanije su uglavnom bile male (ispod 100 mil. USD vrijednosti) i nisu bile na popisu Njujorške ili Američke burze

1. *Neke od kompanija su bile na granici gubitka*
2. *Generalni menadžeri su bili uključeni u 72% slučajeva, a izvršni u 43%*
3. *Tipične tehnike su se svodile na prikaz većih prihoda ranijim uknjiženjem ili fiktivno, uvećanjem vrijednosti imovine ili prikazom fiktivne imovine*
4. *Posljedice:*
    1. *Bankrot*
    2. *Značajne promjene u vlasničkoj strukturi*
    3. *Skidanje s burzovnih listi*
    4. *Financijske kazne*

6

Primjeri prijevara - USA

Lažiranje financijskih izvješća:

- *Enron (bankrot 2001, vrijedan 62 milijarde USD)*
- *WorldCom (bankrot 2002, vrijedan preko 100 milijardi USD)*
- *Tyco*
- *Adelphia*
- *HealthSouth*
- *Xerox …*

7

Zašto ???

- *Snažan pritisak da se ispune ili nadmaše očekivanja vezano za zaradu*
- *Pokriće za preoptimistične planove zarade*
- *Isplata menadžmenta u dionicama*
- *Menadžerska plaća usko vezana za rast dionica ili zarade*
- *Prijetnja poslovnog promašaja*
- *Nepovoljni ekonomski uvjeti (inflacija, recesija)*
- *Jaka tržišna konkurencija i pad dobiti*
- *Značajni problemi s likvidnošću*
- *Velika kreditna ovisnost ….*

8

Interna kontrola – propusti ???

- *Nema kontinuiranog nadzora interne kontrole*
- *Menadžment nije uključen u sustav kontrole*
- *Menadžment ne poštuje pravila kontrole*
- *Nepažljivost menadžmenta, ne poklanjanje pažnje detaljima*
- *Dominantni stil menadžmenta*
- *Neefikasan nadzor Upravnog vijeća*
- *Nema dobro uvježbanog osoblja za kontrolu*
- *Rijetka revizija od strane neovisne treće strane*
- *Nedovoljno odvajanje dužnosti*
- *Pretjerano povjerenje u ključne osobe*
- *Nejasne linije ovlasti*
- *Nedostatak odgovarajućih procedura autorizacije*
- *Neodgovarajuća dokumentacija*
- *Ne postoji fizički ili logički sustav zaštite*
- *Kompleksne transakcije*
- *Prekomplicirana organizacijska struktura…*

9

Računalne prijevare i zlouporabe

* *Računalo se rabi kao alat za prijevaru*

- *Računalo ili informacija pohranjena u njemu je meta kriminalne aktivnosti*

FBI procjene: otkrije se 1%
Ostale procjene: 5-20%

Preko 80% se ne prijavljuje

10

Tehnike zlouporabe računala

- Data diddling – promjena podataka prije unosa u sustav, tijekom obrade ili na izlazu
- Neovlašteno kopiranje organizacijskih podataka
- Softversko piratstvo
- Spaming – slanje neželjenih poruka s ciljem prodaje proizvoda ili usluge
- Izazivanje pada sustava – zatrpavanjem mnoštvom e-mailova
- Hakiranje – neovlaštenai pristup ili uporaba računalnog sustava
- Hijacking – preuzimanje kontrole nad nečijim računalom bez znanja korisnika s ciljem izvršavanja štetnih radnji (slanje spamova, virusa i sl.)
- Krađa identiteta – ilegalno prikupljanje i uporaba osobnih podataka
- Virusi

11

Tehnike zlouporabe računala

- *Decimalno zaokruživanje*
- *SALAMA – "zaostale instrukcije" koje "sklanjaju" manje količine novca (povećanje potrošnje za djelić postotka)*
- *STRAŽNJA VRATA (engl.* back door*) – zaobilaženje kontrole – zaostali kod od testiranja*
- *LOGIČKA BOMBA – program miruje dok ga ne pokrenu neke posebne okolnosti*
- *TROJANSKI KONJ (npr. I LOVE YOU virus – krađa password-a preko udaljene kontrole)*
- *CRV je za razliku od virusa samostalan program i replicira se automatski*
- *Društveni inženjering – navođenje djelatnika da daju informacije neophodne za ulazak u sustav*
- *Interet dezinformacje – širenje lažnih informacija o pojedincima ili tvrtkama …*

12

Definicije interne kontrole

Interna kontrola je proces, koji provodi menadžment i ostali uposleni, osmišljen s ciljem da se omogući razumna sigurnost vezano za postizanje zadaća u slijedećim kategorijama:

- *efikasnosti i efektivnosti operacija*
- *vjerodostojnosti financijskih izvješća*
- *usklađenosti s zakonskom regulativom.*

13

Ciljevi interne kontrole

- *Zaštita imovine*
- *Provjera točnosti i vjerodostojnosti knjigovodstvenih podataka*
- *Promoviranje operativne efikasnosti*
- *Osiguranje privrženosti definiranoj menadžerskoj politici*

14

Ciljevi kontrole – operativni procesi

Osigurati EFEKTIVNOST operacija postizanjem definiranih ciljeva vezano za ciljeve operativnih procesa	*EFEKTIVNOST: mjera uspjeha u postizanju jednog ili više ciljeva.* *Ciljevi operativnih procesa: kriteriji koji se rabe za provjeru efektivnosti operativnih procesa.*
Osigurati EFIKASNU uporabu resursa	*EFIKASNOST: mjera produktivnosti resursa angažiranih za postizanje skupa ciljeva.*
Osigurati sigurnost resursa (specificirati primjenjive operativne procese i resurse informacijskih procesa)	*Sigurnost resursa: zaštita resursa organizacije od gubitka, uništenja, odavanja, kopiranja prodaje ili druge zlouporabe.*

Ciljevi kontrole – informacijski procesi

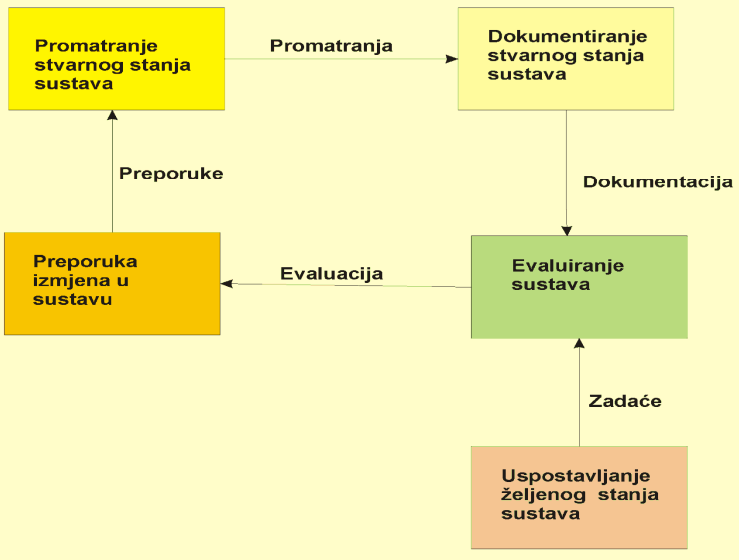
Osigurati vjerodostojnost ulaznih podataka (input validity)	*Kontrolni cilj koji podrazumijeva da su ulazni podaci na odgovarajući način provjereni i potvrđeni i da predstavljaju stvarne ekonomske događaje i objekte.*
Osigurati potpunost ulaznih podataka (input completeness)	*Kontrolni cilj koji podrazumijeva da su svi značajni događaji i objekti uneseni u sustav.*
Osigurati točnost ulaznih podataka (input accuracy)	*Kontrolni cilj koji podrazumijeva da su svi događaji korektno interpretirani i uneseni u sustav.*
Osigurati potpunost ažuriranja podataka	*Kontrolni cilj koji podrazumijeva da su svi u računalo uneseni događaji uneseni i u tzv. matične podatke.*
Osigurati točnost ažuriranja	*Kontrolni cilj koji podrazumijeva da su svi podaci uneseni u računalo korektni s obzirom na matične podatke.*

Značajke interne kontrole

- *Sredstvo za ostvarenje krajnjeg cilja*
- *To je sustav sam za sebe:*
  - *jasno definirani ciljevi*
  - *međusobno povezani dijelovi*
  - *proces*
- *Uspostavljanje kontrole je odgovornost menadžmenta*
- *Ovisna o ljudima*
- *Ne nudi apsolutnu sigurnost ostvarenja ciljeva organizacije već razumnu sigurnost*
- *Nije besplatna*

17

Opći model kontrole



18

Definicija interne kontrole

Interna kontrola je proces koji provodi uprava, menadžment i ostali zaposlenici, dizajnirana u svrhu omogućavanja razumne sigurnosti u postizanju ciljeva u sljedećim kategorijama:

– Efektivnosti i efikasnosti operacija
– Vjerodostojnosti financijskih izvješća
– Usklađenost s zakonskom regulativom

19

Komponente interne kontrole

- *Kontrolno okruženje*
- *Utvrđivanje rizika*
- *Kontrolne aktivnosti*
- *Informacije i komunikacija*
- *Nadzor*

20

Kontrolno okruženje

Uspostavlja, daje ukupan "ton" shvaćanju kontrole u organizaciji, utječući na svijest o značaju kontrole kod svih djelatnika organizacije, osiguravajući osnovnu disciplinu i strukturu.

Faktori unutar kontrolnog okruženja:

- *Integritet, etičke vrijednosti i kompetentnost djelatnika u organizaciji*
- *Filozofija menadžmenta i stil rada*
- *Način na koji menadžment dodjeljuje autoritet i odgovornosti, kao i kako organizira i unapređuje razvoj svojih zaposlenika*
- *Pozornost i smjernice koje daje uprava organizacije.*

21

Kontrolno okruženje i etika

- *Etičko ponašanje i čestitost menadžmenta je rezultat korporacijske kulture".*
- *Zvanična (formalna) politika organizacije specificira ono što menadžment želi da se dogodi, dok korporacijska kultura određuje što se stvarno događa i koja pravila se poštuju, zaobilaze ili ignoriraju.*

22

Utvrđivanje rizika

Podrazumijeva da se svaka organizacija pri ostvarivanju svojih ciljeva suočava s rizikom, i to i internim i eksternim.

Rizici koji mogu ugroziti ostvarivanje ciljeva organizacije trebaju biti identificirani, analizirani i potrebno je imati spremne planove za djelovanje u slučaju pojave rizika.

23

Kontrolne aktivnosti

Politike i procedure koje pomažu pri osiguravanju da se provode smjernice i direktive menadžmenta.

Bitno je osmisliti i uspostaviti specifične kontrolne procedure kako bi se osiguralo poduzimanje neophodnih aktivnosti vezano za pojedine vrste rizika ostvarenja ciljeva organizacije.

24

Kontrolne aktivnosti

Tri su osnovne vrste kontrolnih procedura:

- *Preventivne kontrole*
- *Kontrole detekcije (otkrivanja)*
- *Korektivne kontrole*

25

Kontrolne aktivnosti

Preventivne kontrole – kontrole osmišljene i implementirane kako bi se spriječili potencijali problemi tijekom odvijanja određene aktivnosti.

Na primjer:

Pravilo koje kaže da knjigovođa odgovoran za bilježenje gotovinskih uplata, ne može imati izravan pristup gotovini.

26

Kontrolne aktivnosti

Kontrole detekcije (otkrivanja) – *daju menadžerima povratnu informaciju o tome da li se na operativnoj razini postupalo prema uputama menadžmenta ili nije.*

Na primjer:

Izvješće o odnosu između stvarnih i planiranih (standardnih) troškova proizvodnje.

27

Kontrolne aktivnosti

Korektivne kontrole – *osmišljene da "liječe" (rješavaju) probleme otkrivene pomoću kontrola detekcije.*

Primjer:

Vezano za prethodne povećane troškove proizvodnje – dodatna obuka djelatnika.

28

Informacije i komunikacija

Pojam informacije

odnosi se osiguravanje potrebnih informacija npr. računovodstveni sustav podrazumijeva metode za bilježenje, obradu, zbrajanje i izvješćivanje o transakcijama organizacije, kao i održavanje odgovornosti za imovinu, obveze i ravnotežu

29

Informacije i komunikacija

Pojam komunikacija

odnosi se na osiguranje razumijevanja i odgovornosti kod svih zaposlenika organizacije, vezano za to kako svačija pojedina aktivnost utječe na kvalitetu računovodstvenih podataka i izvješća.

30

Nadzor

Proces koji procjenjuje kvalitetu izvršavanja interne kontrole tijekom vremena.

Procjenjuju se dizajn i operativne kontrole na vremenskoj bazi i iniciraju korektivne akcije ukoliko je to potrebno.

31

Današnje organizacije su zaokupljene:

- Menadžmentom rizika
- Upravljanjem
- Kontrolom
- Sigurnošću

32

Definicija menadžmenta rizika

- Menadžment rizika je znanstveni pristup postupanju s čistim rizikom tako da se anticipiraju mogući gubitci i dizajniraju i implementiraju procedure koje minimiziraju pojavu ili financijski značaj gubitka. [Vaughan and Vaughan: *Fundamentals of Risk and Insurance*]
- Značenje: Rizik kao neizvjesnot koja se odnosi na pojavu gubitka.

33

Jednadžba rizika

Rizik = Ranjivost x Prijetnja x Značaj
*Vjerojatnost

- Ranjivost = *Greška ili slabost* u dizajnu, implementaciji ili radu sustava.
- Prijetnja = *Neprijatelj* koji je motiviran iskoristiti ranjivost sustava i sposoban je to uraditi
- Značaj = *vjerojatnost* da će ranjivost biti iskorištena ili da prijetnja može postati *štetna*.
- *Vjerojatnost = *vjerojatnost* je već faktorizirana u okviru *značaja*.

34

Tipovi rizika

- Strateški – *Ciljevi organizacije*
- Operativni – *Procesi koji postižu ciljeve*
- Financijski – *Čuvanje imovine*
- Zakonski – *Zakoni i regulativa*
- Reputacijski – *Javna slika (imidž)*

35

Odgovori na rizik

Jačina

Visok	Prebaciti	Izbjeći
Nizak	Prihvatiti	Prihvatiti/ Prebaciti
	Nizak	*Visok*

Učestalost

36

ERM okviri

- COSO ERM – *Integrirani okvir*
- Australija/Novi Zeland Standard – Menadžment rizika (*Risk Management)*
- ISO Risk Management - *Draft Standard*
- Standard menadžmenta rizika - Federation of European Risk Management Associations (FERMA)

37

COSO

COSO -
Commitee of Sponsoring Organizations

Grupa iz privatnog sektora (Američka asocijacija računovođa – AICPA, Institut internih revizora, Institut menadžerskih računovođa i institut za financijske izvršitelje)

1992. Interna kontrola – Integrirani Okvir koji definira internu kontrolu i daje smjernice za evaluaciju i unapređenje sustava interne kontrole

2001. Proširenje Integriranog okvira – ERM (Enterprise Risk Management – hrv. Upravljanje rizikom poduzeća) Integrirani okvir

38

Upravljanje rizikom poduzeća (ERM)

- Precizan pristup procjeni i prepoznavanju rizika iz svih izvora koji prijete postizanju organizacijskih strateških ciljeva. ERM identificira one rizike koji predstavljaju odgovarajuće mogućnosti za iskorištavanje kompetitivnih prednosti. [Tillinghast-Towers Perrin consultancy group]
- Sve što utječe na sposobnost organizacije da ostvari svoje ciljeve. [*Developing A Strategy to Manage Enterprisewide Risk in Higher Education*, NACUBO]

39

COSO ERM definicija

"... proces, izazvan od strane uprave, menadžmenta i ostalih zaposlenika, primijenjen u postavkama strategije i širom poduzeća, dizajniran da identificira potencijalne događaje koji mogu utjecati na organizaciju, i upravlja rizicima u okviru definirane sklonosti riziku, te omogući razumnu vjerojatnost u odnosu na postizanje ciljeva organizacije."

Source: COSO Enterprise Risk Management – Integrated Framework. 2004. COSO.

40

ERM — Integrirani okvir

COSO ERM okvir definira osnovne elemente, predlaže zajednički jezik i osigurava jasan smjer i upute za upravljanje rizikom poduzeća.

41

COSO – ERM

Osnovni principi ERM-a:

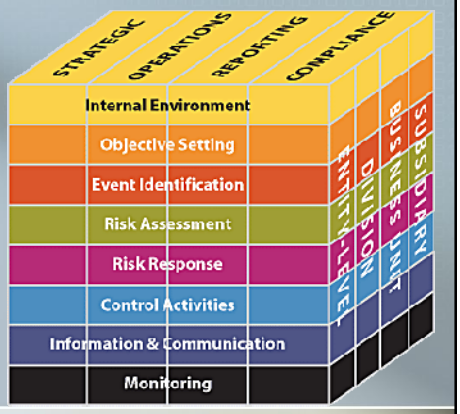
- Kompanije postoje da bi kreirale vrijednost za svoje vlasnike
- Menadžment kompanije mora odlučiti koliku neizvjesnost može podnijeti pri kreiranju vrijednosti
- Rezultat neizvjesnosti je rizik tj. mogućnost da se dogodi nešto što će utjecati na sposobnost kompanije da kreira vrijednost ili će umanjiti postojeću
- Rezultat neizvjesnosti može biti i prilika – mogućnost da će se dogoditi nešto što će pozitivno utjecati na sposobnost kompanije da kreira ili sačuva vrijednost
- ERM okvir pomaže menadžmentu u upravljanju neizvjesnošću, i povezuje rizike i prilike, kako bi se očuvala vrijednost.

42

ERM okvir

Ciljevi organizacije mogu se promatrati u kontekstu 4 kategorije :

- Strategija
- Operativa
- Izvešćivanje
- Zakonitost

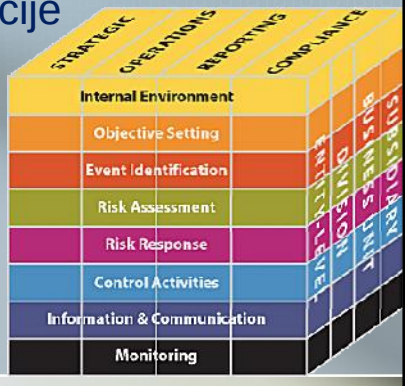


43

ERM okvir

ERM promatra aktivnosti na svim razinama organizacije:

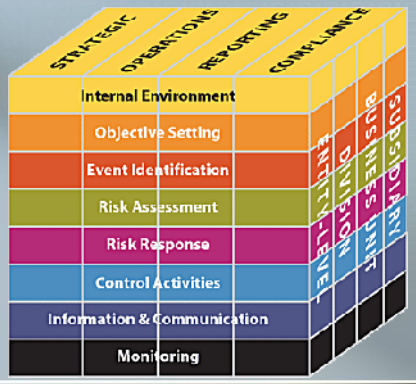
- Razina organizacije
- Odjel ili podružnica
- Procesi na razni poslovne jedinice



44

ERM okvir

Osam komponenti okvira su međusobno povezane …



45

COSO – ERM

Osam (8) komponenti rizika i kontrole ERM-a:

1. Interno okruženje – korporacijska kultura (“ton”) – temelj za sve ostale komponente
2. Postavljanje ciljeva – strateških, operativnih, izvještajnih, usklađenih sa zakonom
3. Identificiranje događaja – menadžment treba prepoznati događaje koji mogu utjecati na sposobnost organizacije da implementira ciljeve
4. Određivanje rizika – prepoznavanje rizika i određivanje kako upravljati rizicima

47

COSO – ERM

5. Odgovor na rizik – povezivanje rizika s kompanijinom tolerancijom na rizik. Odgovor može biti: izbjeći, smanjiti, podijeliti ili prihvatiti rizik
6. Kontrolne aktivnosti – da bi se implementirao odgovor na rizik moraju se uspostaviti kontrolne politike i procedure na svim razinama
7. Informacije i komunikacije – Informacije so ERM komponentama moraju biti prikupljene i svi djelatnici upoznati sa svojom odgovornošću
8. Nadzor – kako bi sustav bio efikasan treba osigurati stalni nadzor i evaluaciju.

48

Interno okruženje

- Uspostavlja filozofiju koja se odnosi na upravljanje rizikom. Prepoznaje da se mogu dogoditi i očekivani i neočekivani događaji.
- Uspostavlja kulturu rizika.
- Razmatra sve druge aspekte o tome kako organizacijske aktivnosti mogu utjecati na kulturu rizika.

49

Postavljanje ciljeva

- Primjenjuje se kada menadžment razmatra strategiju rizika pri postavljanju ciljeva.
- Oblikuje sklonost organizacije riziku – globalni pristup tome koju razinu rizika su menadžment i uprava voljni prihvatiti.
- Tolerancija rizika, prihvatljiva razina odstupanja od ciljeva, povezano sa sklonošću riziku.

50

Postavljanje ciljeva

Sklonost riziku:

Koristiti kvantitativne ili kvalitativne izraze (npr. Rizik zarade naspram rizika reputacije) i razmotriti toleranciju na rizik (raspon prihvatljivih varijacija).

Ključna pitanja:

- Koje rizike organizacija ne može prihvatiti? *(npr. Zaštita okoliša ili kompromis u kvaliteti)*
- *Koje rizike će organizacija preuzeti sa novim incijativama*? *(npr. Nova proizvodna linija)*
- *Koje rizike će organizacija prihvatiti zbog konkurentnosti*? *(npr. Profitna stopa naspram tržišnog udjela?)*

51

Identificiranje događaja

- Razlikuje rizike i prilike.
- Događaji koji mogu imati negativan utjecaj predstavljaju rizike.
- Događaji koji mogu imati pozitivan utjecaj predstavljaju prilike koje menadžment treba uključiti u strategiju.

52

Identificiranje događaja

- Uključuje identificiranje onih situacija koje se javljaju interno ili eksterno, a mogu utjecati na strategiju i postizanje ciljeva.
- Pokazuje kako se interni i eksterni faktori kombiniraju i međusobno djeluju na način da utječu na profil rizika.

53

Određivanje rizika

- Omogućava organizaciji da razumije u kojoj mjeri potencijalni događaji mogu utjecati na ciljeve.
- Razmatra rizik iz dvije perspektive:
  - Vjerojatnost
  - Utjecaj
- Koristi se za određivanje rizika i obično se koristi za mjerenje odgovarajućih ciljeva.

54

Određivanje rizika

- Koristi kombinaciju i kvalitaitvnih i kvanititativnih metodologija određivanja rizika.
- Povezuje vremensku perspektivu s perspektivom ciljeva.
- Određuje rizike na prirođenoj i drugoj osnovi.

55

Odgovor na rizik

- Identificira i evaluira moguće odgovore na rizik.
- Procjenjuje mogućnosti u odnosu na sklonost organizacije riziku,troškove naspram koristi od potencijalnih odgovora na rizike i stupanj do kojega će odgovor smanjiti utjecaj i/ili vjerojatnost rizika.
- Odabire i provodi odgovore bazirane na procjeni portfolija rizika i odgovora.

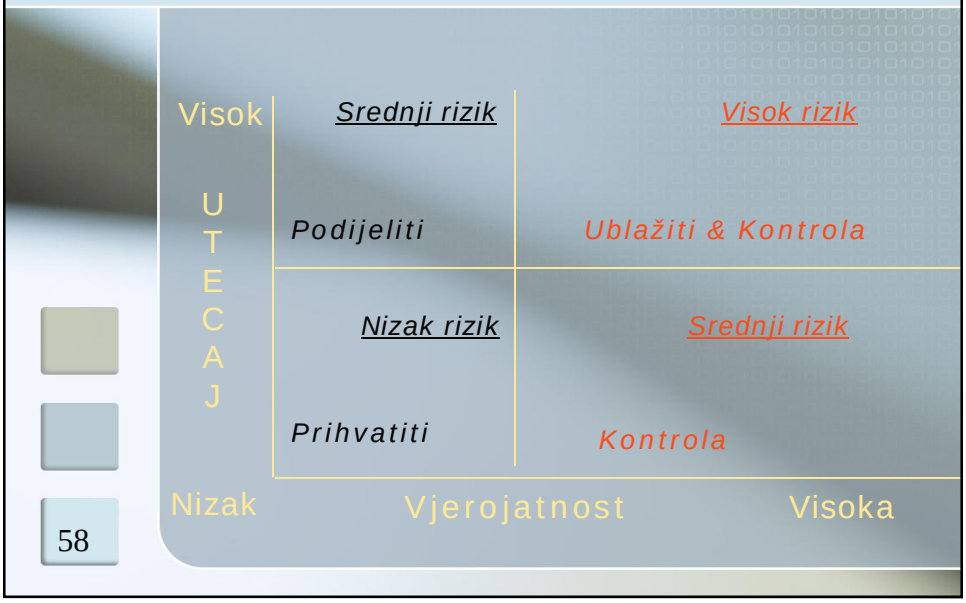
56

Odgovor na rizik

- Kvantifikacija izloženosti riziku
- Raspoložive opcije:
  - Prihvatiti = nadzirati
  - Izbjeći = eliminirati *(izići iz te situacije)*
  - Smanjiti = uspostaviti kontrole
  - Podijeliti = partnerstvo s nekim *(npr. osiguranje)*

57

Utjecaj vs. vjerojatnost



58

Kontrolne aktivnosti

- Politike i procedure koje pomažu osigurati odgovore na rizik, kao i ostale naredbe.
- Događaju se širom organizacije, na svim razinama organizacije i funkcijama.
- Uključuje aplikacijsku i opću IT kontrolu.

59

Informacije i komunikacije

- Menadžment identificira, prikuplja i priopćava primjerene informacije u obliku i vremenskom okviru koji omogućava ljudima da izvršavaju ono što je njihova odgovornost.
- Informiranje se pojavljujue u svim segmentima organizacije i širi se u svim smjerovima (prema gore, dolje, ...).

60

Informacije i komunikacije

Mogućnosti:

- Kontrolne ploče (Dashboard) rizika i odgovarajućih odgovora (vizualni satus odnosa ključnih rizika u odnosu na toleranciju prema riziku)
- Dijagrami procesa s uključenim ključnim kontrolama
- Opisi poslovnih ciljeva povezani s operativnim rizicima i odgovorima na iste
- Lista ključnih rizika koje treba nadzirati
- Menadžment treba razumjeti ključne rizike i odgovornost koju ima.

61

Nadzor

Efektivnost drugih ERM komponenti se nadzire kroz:

- Stalne aktivnosti nadzora.
- Posebne procjene.
- Kombinacijom oba pristupa.

62

Interna kontrola i COSO ERM

- Proširuje i detaljno razrađuje elemente interne kontrole kao što je postavljeno u COSO kontrolnom okviru.
- Uključuje postavljanje ciljeva kao posebnu komponentu. Ciljevi su “preduvjet” za internu kontrolu.
- Proširuje kontrolne okvire financijskog izvješćivanja i određivanja rizika.

63

Ključni implementacijski čimbenici

1. Organizacijsko ustrojstvo poslovanja
2. Uspostavljanje i organiziranje ERMa
3. Izvršavanje određivanja rizika
4. Utvrđivanje globalne sklonosti riziku
5. Identificiranje odgovora na rizik
6. Objavljivanje i analiza rezultata rizika
7. Nadzor
8. Nadzor i povremena analiza od strane menadžmenta

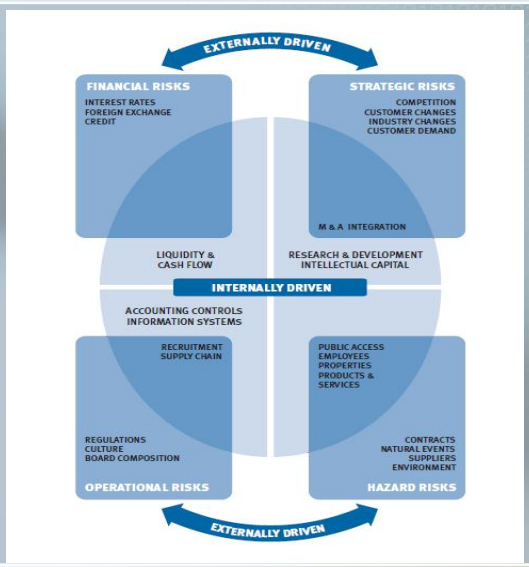
64

Efektivan ERM

- Menadžment ima “tok vjerodostojnih informacija” o svakoj komponenti kontrole za sve ciljeve, iz svih područja organizacije.
- COSO ne specificira tko bi trebao osigurati koju informaciju, samo da menadžment treba dobiti informaciju i djelovati na bazi iste.
- Mnogo različitih izvora ili tokova informacija postoji u organizaciji.
- “Soft” kontrole odnose se na ljude koji rade kako bi ispunili ciljeve organizacije; “hard” kontrole se odnose na procese i aktivnosti koje ljudi trebaju izvršiti.

65

Standardi upravljanja rizikom
Federation of European
Risk Management Associations (FERMA)



66

Standardi upravljanja rizikom
Federation of European
Risk Management Associations (FERMA)

67

Standardi upravljanja rizikom
Federation of European
Risk Management Associations (FERMA)

Upravljanje rizikom štiti i dodaje vrijednost organizaciji i zainteresiranim stranama (učesnicima) na način da podržava ciljeve organizacije:

- Osiguravanjem organizacijskog okvira koji omogućava izvršavanje budućih aktivnosti na konzistentan i kontroliran način
- Poboljšavanjem odlučivanja, planiranja i uspostavljanja prioriteta kroz sveobuhvatno i strukturirano razumijevanje poslovnih aktivnosti, projektnih mogućnosti i prijetnju
- Doprinosi efikasnijoj uporabi/alokaciji kapitala i resursa unutar organizacije
- Smanjuje promjenjivost u područjima poslovanja koja nisu ključna za organizaciju
- Štiti i uvećava imovinu i imidž organizacije
- Razvija i podržava ljude i organizacijsku bazu znanja
- Optimizira operativnu efikasnost

68

ISO 31000

- Objavljeno 2009. godine
- Cilj je osigurati potporu za novi, menadžmentu bliži način promišljanja o riziku i upravljanju rizikom
- Rizik se definira kao „djelovanje nesigurnosti na ciljeve“
- Rizik sam po sebi nije niti pozitivan niti negativan, ali njegove posljedice po organizaciju (djelovanje) mogu varirati od gubitka i štete do dobitka.

69

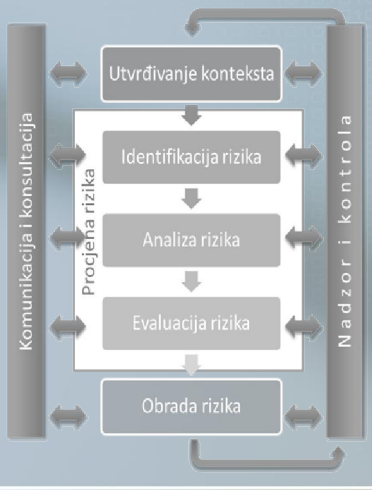
ISO 31000

- ISO 31000 sadrži:
  - vokabular,
  - skup kriterija performansi,
  - zajednički proces identificiranja, analiziranja, evaluiranja i obrade rizika,
  - smjernice kako bi taj proces trebalo integrirati u proces donošenja odluka bilo koje organizacije

70

ISO 31000

- Polazi od globalnog upravljanja rizikom



71

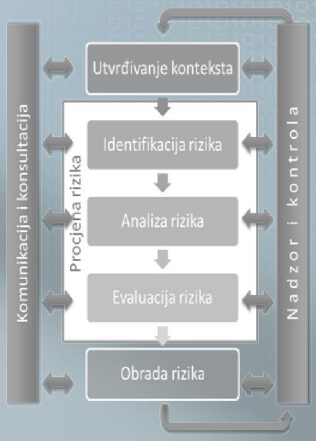
ISO 31000

- Utvrđivanja konteksta - prvi korak
- Obuhvaća
  - temeljne ciljeve organizacije,
  - okruženje u kojem organizacija djeluje i u kojem pokušava realizirati svoje ciljeve,
  - dionič̆are tj. osnovne učesnike,
  - posebne kriterije rizika
  - CILJ: olakšati kasnije ocjene značajki i složenosti rizika organizacije

72

ISO 31000

- Procjena obuhvaća tri osnovna koraka:
  - identifikaciju,
  - analizu i
  - evaluaciju rizika.



73

ISO 31000

- Identifikacija rizika
- Traži primjenu sustavnog pristupa kako bi se razumjelo što bi se moglo dogoditi, kako, kada i zašto.

74

ISO 31000

- Analiza rizika

  odnosi se na poboljšanje razumijevanja svakog rizika, njegovih posljedica i vjerojatnosti tih posljedica

75

ISO 31000

- Evaluacija rizika

  se odnosi na donošenje odluke o razini rizika i prioritetu za praćenje.

76

ISO 31000

- Obrada rizika

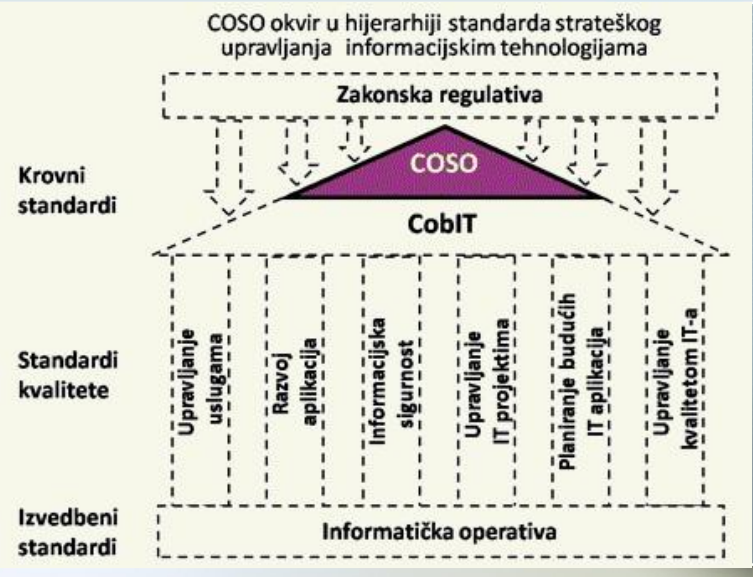
  je proces pomoću kojega se postojeće kontrole poboljšavaju ili se nove kontrole razvijaju i primjenjuju.

Obuhvaća:

- vrednovanje i odabir odgovarajućih opcija,
- analizu troškova i dobit,
- ocjenu novih rizika koje može generirati odabir konkretne opcije,
- uspostavljanje prioriteta
- primjenu odabrane obrade rizika u okviru dobro planiranog procesa.

77

Interna kontrola i IT



78

COBIT

- *CONTROL*
- *OBJECTIVES*
- *for INFORMATION*
- *and RELATED*
- *TECHNOLOGY*

79

Izazovi vezani za računalnu kontrolu

- *Efekti grešaka mogu biti značajno uvećani*
- *Smanjeni broj ručnih intervencija, može dovesti do neadekvatnog razdvajanja dužnosti*
- *Promjene na računovodstvenim podacima i programima mogu napraviti pojedinci*
- *Puno veći broj ljudi može pristupati kritičnim podacima*

80

COBIT

http://www.cis.hr/dokumenti/cobitframework-5.html

- svjetski prihvaćen standard
- propisuje područja i pojedinačne kontrole za korporativno upravljanje informacijama i pripadajućim informacijskim procesima.
- Autori COBITa su neprofitne organizacije ISACA (eng. Information System Audit and Control Association, ISACA) i ITGI (eng. Technology Governance Institute, ITGI).
- COBIT radni okvir spaja poslovne i informatičke ciljeve
- pruža mogućnost praćenja zrelosti informacijskog sustava
- COBIT pruža menadžmentu mogućnost optimizacije informacijskih resursa (programski paketi, informacije, infrastruktura i ljudi)

81

COBIT okvir 5.0

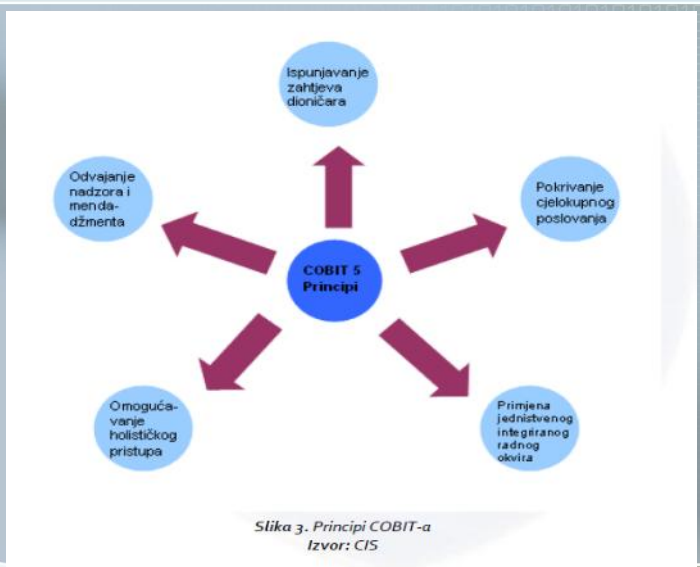
Sastoji se od:

- 37 ključna poslovna kontrolna procesa i za svaki proces opisuje model zrelosti.
- preko 300 detaljnih informacijskih kontrola.
- Primarni kontrolni ciljevi podijeljeni su u pet domena.

COBIT 5
AN ISACA® FRAMEWORK

82

COBIT 5 - Principi

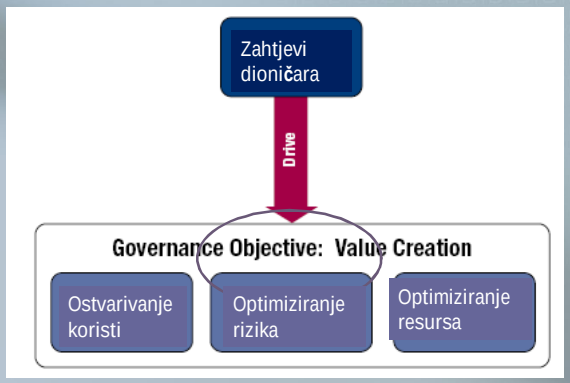


Slika 3. Principi COBIT-a
Izvor: CIS

83

Ispunjavanje zahtjeva dioničara (stakeholders)

Poduzeće postoji kako bi kreiralo vrijednost za svoje dioničare (stakeholders)



84

Ispunjavanje zahtjeva dioničara (stakeholders)

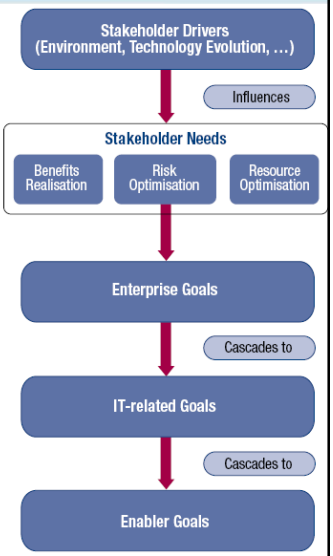
- Poduzeća imaju više dioničara (stakeholders), i 'kreiranje vrijednosti' znači različite i ponekad konfliktne stvari za svakoga od njih.
- Upravljanje (governance) se odnosi na pregovaranje i odabir i odlučivanje između različitih interesa dioničara.
- Sustav upravljanja bi trebao uzeti u razmatranje sve dioničare kada se odlučuje o koristima, resursima i određivanju rizika.
- Za svaku odluku, trebala bi se postaviti sljedeća pitanja:
  - Tko ima koristi od toga?
  - Tko snosi rizik?
  - Koji su resursi potrebni?

85

 85

Ispunjavanje zahtjeva dioničara (stakeholders)

- Zahtjevi dioničara trebaju biti transformirani u izvršivu strategiju.
- COBIT 5 ciljevi kaskadno prevode zahtjeve dioničara u specifične, izvršive i prilagođene ciljeve u okviru poduzeća, IT ciljeve i ciljeve pokretača.



86

 86

Pokrivanje cjelokupnog poduzeća

- COBIT 5 pokriva sve funkcije i procese u poduzeću
- COBIT 5 se ne fokusira samo na 'IT funkciju', već tretira informacije i tehnologiju kao imovinu s kojom treba raspolagati na isti način kao i bilo kojom drugom imovinom.

87

 87

Primjena jedinstvenog integriranog okvira

- COBIT 5 je usklađen s najnovijim relevantnim drugim standardima i okvirima koje poduzeća koriste:
  - Poduzeće: COSO, COSO ERM, ISO 9000, ISO 31000
  - IT: ISO 38500, ITIL, ISO27000 series, TOGAF, PMBOK/PRINCE2, CMMI
  - Itd.
- Ovo omogućava poduzeću korištenje COBIT 5 kao uspješnog upravljačkog i menadžerskog integracijskog okvira.

88

 88

Odvajanje upravljanja (governance) od menadžmenta (management)

- COBIT 5 okvir pravi jasnu razliku između upravljanja i menadžmenta.
- Ove dvije discipline:
  - Obuhvaćaju različite tipove aktivnosti
  - Traže različitu organizacijsku strukturu
  - Imaju različitu svrhu
- Upravljanje — u većini poduzeća upravljanje je odgovornost upravnog odbora.
- Menadžment— u većini poduzeća, menadžment je odgovornost izvšnog menadžmenta.

89

 89

Odvajanje upravljanja (governance) od menadžmenta (management)

- Upravljanje osigurava da se ciljevi poduzeća ostvaruju putem vrednovanja zahtjeva dioničara, uvjeta i opcija, postavljanjem smjernica kroz prioritete i odlučivanje, kao i nadzor performansi, zakonitosti i napretka prema usvojenim smjernicama i ciljevima.
- Menadžment planira, definira, izvršava i nadzire aktivnosti sukladno postavljenim smjernicama od strane upravnog odbora za postizanje ciljeva poduzeća.

90

 90

Omogućavanje holističkog pristupa

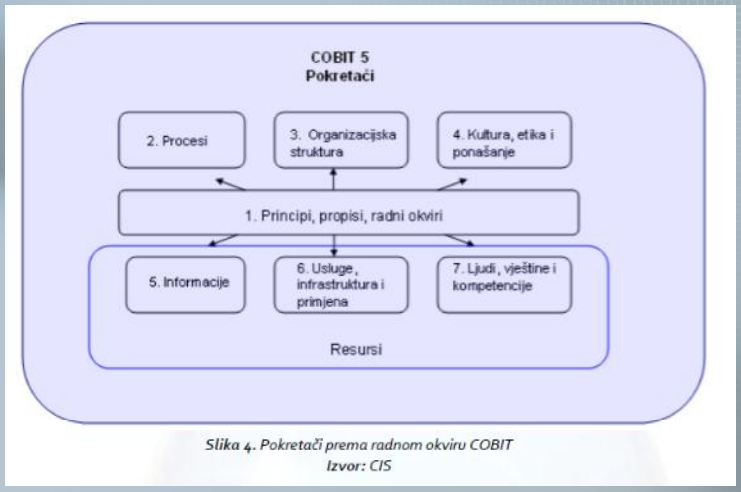
COBIT 5 pokretači (enablers) su:

- Faktori koji, pojedinačno ili skupno, utječu da li će nešto raditi – u slučaju COBITa, upravljanje (governance) i menadžment IT-ija u poduzeću.
- Pokretani kaskadom ciljeva, tj. viša razina IT ciljeva definira što različiti pokretači trebaju postići
- Opisani u COBIT 5 okviru sa sedam kategorija

91

 91

COBIT pokretači



Slika 4. Pokretači prema radnom okviru COBIT
Izvor: CIS

92

COBIT pokretači

- 1. principi i politike upravljanja u radnom okviru (eng. *principles, policies, frameworks),*
- 2. procesi (eng. *processes),*
- 3. organizacijska struktura (eng. *organizational structures),*
- 4. kultura, etička pripadnost i ponašanje(eng. *culture, ethics, behavior),*
- 5. informacije (eng. *information),*
- 6. usluge, infrastruktura i primjena (eng. *services, infrastructure, application) i*
- 7. ljudi, vještine, kompetencije (eng. *people, skills, competencies)*

93

COBIT

http://www.cis.hr/dokumenti/cobitframework-5.html

Radni okvir COBITa omogućuje integraciju poslova vezanih za nadzor poslovnih procesa, problematiku poslovnog rizika, oblikovanje komunikacijskih kanala te razinu nadzora prema potrebama vlasnika tvrtke. Moguć je razvoj dobrih politika i poslovnih praksi ispitivanja sustava ICT u organizacijama.

94

COBIT

http://www.cis.hr/dokumenti/cobitframework-5.html

COBIT upravama i vlasnicima tvrtki omogućuje:

- lakše razumijevanje koncepta upravljanja ICT sustavima,
- definiranje odgovornosti koje su potrebne za kvalitetnu integraciju ICT sustava,
- usklađivanje sustava s regulatornim obvezama
- organiziranje aktivnosti unutar ICT sustava na prihvatljiv način.

95

COBIT

http://www.cis.hr/dokumenti/cobitframework-5.html

COBIT Framework 5 omogućuje optimizaciju informacijskih resursa kao što su programski paketi, informacije, infrastruktura i ljudi. COBIT preporuča praksu koja je proizvod rada mnogih stručnjaka i proizvod je dobre prakse, primjenjive u bilo kojoj organizaciji.

96


Pitanja ????