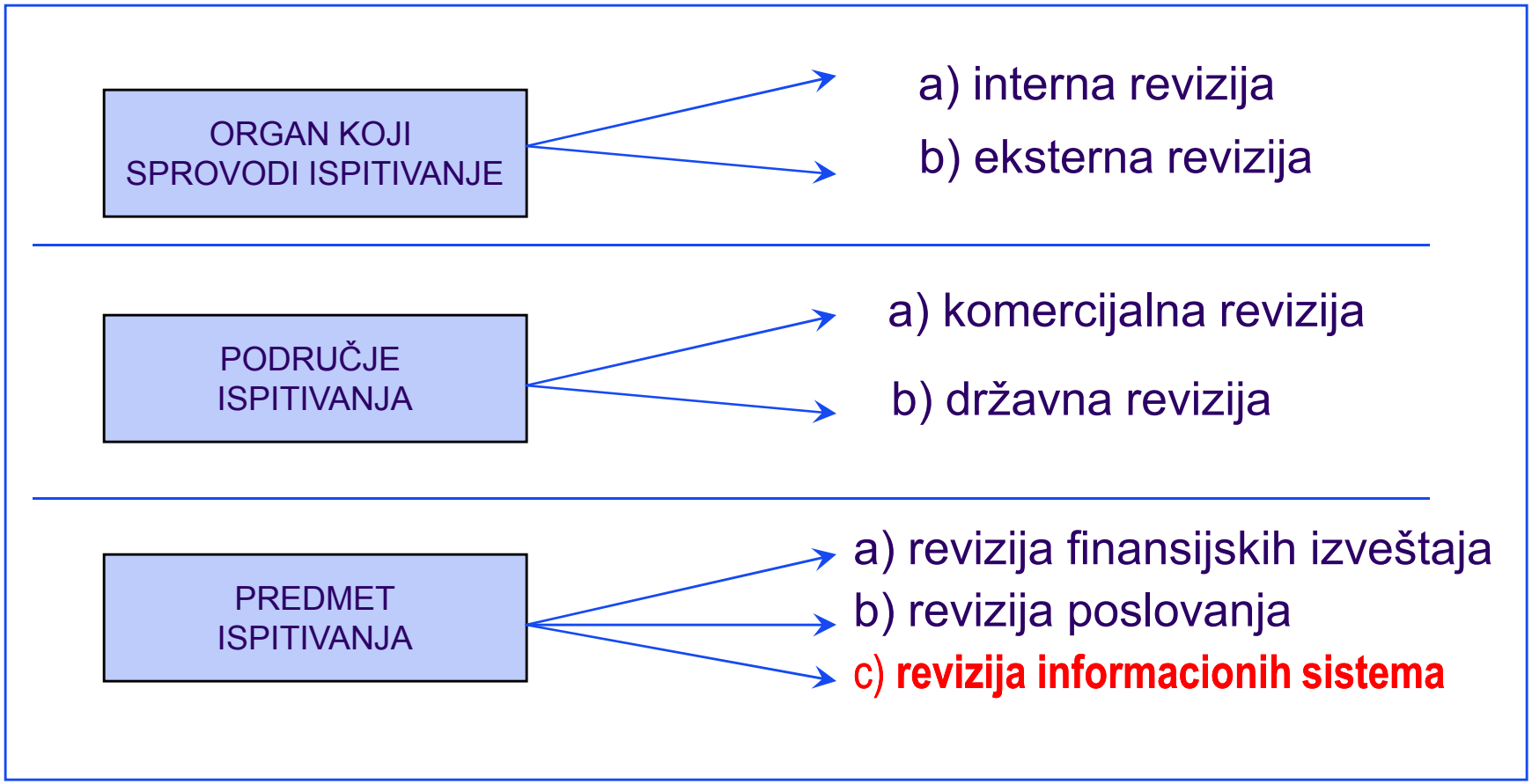
Ekonomski fakultet Beograd

REVIZIJA INFORMACIONIH SISTEMA

ISACA®
Serving IT Governance Professionals

VRSTE REVIZIJE



REVIZIJA INFORMACIONIH SISTEMA

- Revizori svoj rad, analize i ispitivanja uobičajno baziraju na računovodstvenim i finansijskim pravilima izveštavanja.
- S obzirom da preduzeća sve više primenjuju sofisticirane tehnologije upravljanja informacijama, dobijanje kvalitetnih informacija zavisi od pouzdanosti i ispravnosti hardvera, softvera, računarske mreže, sigurnosti i zaštite podataka.

REVIZIJA INFORMACIONIH SISTEMA

- Informacije i informacioni sistemi mogu biti sredstvo manipulacije i prikrivanja istinitosti za onoga ko kontroliše, posredno ili neposredno, organizaciju i procese upravljanja informacionim sistemom preduzeća.
- Zbog toga su potrebni nove metode i načini dolaženja do pouzdanih informacija o poslovanju kako bi se prezentovao fer i istinit izveštaj i oformilo mišljenje kao osnovni proizvod revizorskog rada.

Šta je revizija informacionih sistema?

- Proces prikupljanja i nezavisne, stručne procene dokaza kojim se proverava efikasnost delovanja i konačno procenjuje kvalitet informacionog sistema preduzeća.
- Radi se o skupu složenih menadžerskih, revizorskih i tehnoloških aktivnosti kojima se pregledaju (proveravaju) učinci, ali i rizici upotrebe informacionih sistema i konačno ocenjuje njihov uticaj na poslovanje.

Kvalitet informacionog sistema

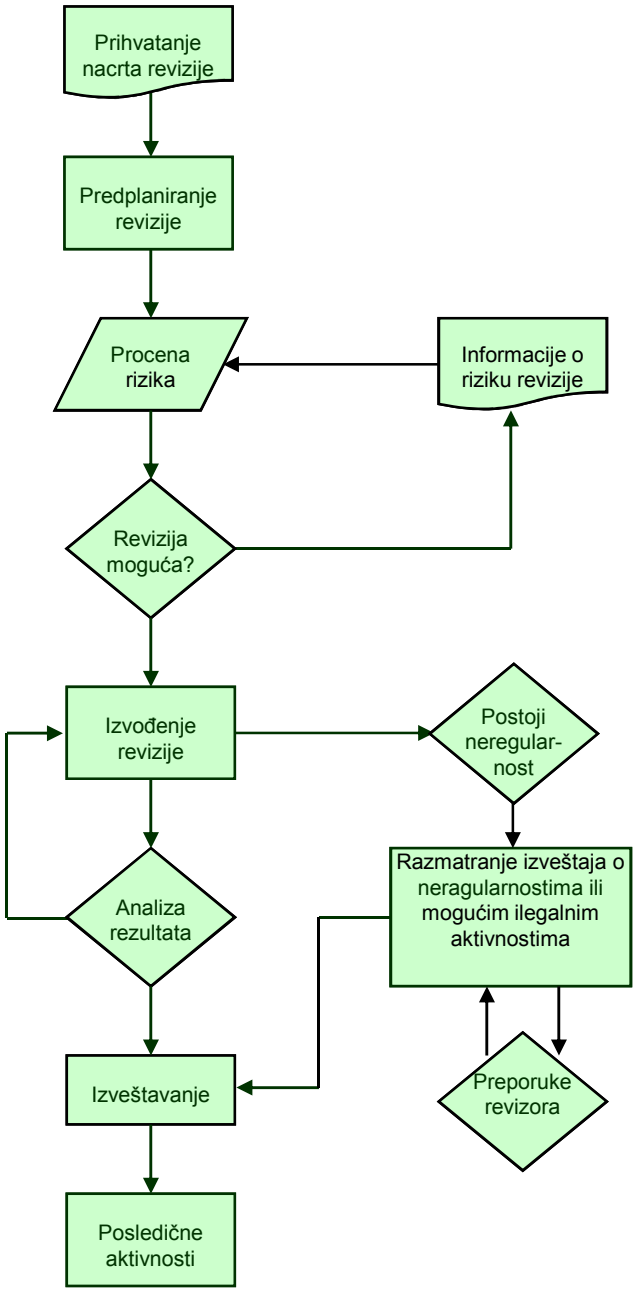
- Interni kvalitet informacionog sistema osigurava se internom kontrolom sistema, a stepen tog kvaliteta utvrđuje se njegovom **internom revizijom**.
- Da bi se ispravno ocenio stvarni i objektivni kvalitet informacionog sistema, treba ga podvrći i **eksternoj reviziji**, čiji će se nalazi smatrati valjanima za izvođenje konačne ocene kvaliteta posmatranog informacionog sistema.

Zadatak revizije IS-a

Osnovni zadatak revizije IS-a:

- Proceniti njegovo trenutno stanje (zrelost, nivo uspešnosti).
- Otkriti rizična područja i nivo rizika.
- Dati preporuke menadžmentu za poboljšanje prakse upravljanja informacionim sistemom

Proces revizije informacionih sistema



Proces revizije informacionih sistema banke

- Prihvatanje nacrta revizije
- Predplaniranje revizije
- Procena rizika
- Određivanje granica revizije
- Izvođenje revizije
- Prikupljanje dokaza
- Izvođenje revizorskih testova
- Analiza rezultata
- Izveštavanje o rezultatima
- Povezivanje sa narednim aktivnostima

Predplaniranje revizije IS-a

- Pregled – ‘snimak stanja’ informacionog sistema ili odabranog područja provere (revizije)
- Određivanje prioriteta rada (određivanje **predmeta (objekta)** revizije IS-a i **ciljeva kontrole**)

Pregled – ‘snimak stanja’ informacionog sistema

(Information request letter)

1. Osnovne informacije o informacionom sistemu: (koje su aplikacije prisutne, koje se održavaju od strane preduzeća, a koji se održavaju od strane dobavljača, ako postoji opis celokupnog IT sistema dostaviti ovaj dokument, na kojoj bazi podataka rade aplikacije i na kom operativnom sistemu, da li je u toku godine bilo krupnijih izmena na sistemu i na šta se odnose?)
2. Mrežni dijagram
3. Organizaciona šema IT odeljenja
4. Lista svih zaposlenih radnika u IT odeljenju sa opisom dužnosti
5. Pisana procedura koja opisuje Change Management proces - proces vršenja programskih izmena (ako postoji)
6. Lista (evidencija) svih programskih izmena tokom godine, odnosno zahteva za programske izmene sa datumom zahteva i statusom zahteva
7. Iz liste naknadno treba izabrati uzorak za testiranje (autorizacija, testiranje, odobravanje puštanja u produkciju)
8. Spisak korisnika (user-a) koji imaju pristup produkcionom okruženju
9. Pisana procedura koja opisuje User Administration proces (proces otvaranja korisničkih naloga, izmena i brisanje) ako postoji

Pregled – ‘snimak stanja’ informacionog sistema

(Information request letter)

10. Lista svih novih radnika i radnika koji su napustili preduzeće tokom godine sa tačnim datumom zasnivanja i raskidanja radnog odnosa
11. Iz liste naknadno treba izabrati uzorak za testiranje (prikupljanje zahteva za otvaranje novih korisnika, korisnika koji menjaju prava i onih koji se ukidaju)
12. Spisak svih user-a na sistemu (aplikacijama) zajedno sa dodeljenim pravima (profilima)
13. Lista svih aktivnih i neaktivnih korisnika na nivou domena
14. Lista svih korisnika sa dodeljenim pravima na nivou baze podataka
15. Izveštaj o pregledu korisničkih prava ako se radi i ako ga je bilo u toku godine
16. Da li neko vrši periodični pregled aktivnosti korisnika - monitoring korisničkog pristupa
17. Password politika na domenu i aplikacijama

    - kompleksnost password-a
    - minimalna dužina
    - vreme na koje se menja password

    ...

Analiza rizika

Sa stanovišta revizije informacionih sistema posmatraju se tri komponente rizika:

- **Inherentni rizici** – rizici koji su vezani za informacione resurse ili resurse koji se koriste u kontroli informacionih sistema kao što su krađa opreme, destrukcija, otkrivanje informacija, neautorizovana modifikacija ili drugi način ugrožavanja sistema.
- **Kontrolni rizici** – rizici od materijalnih grešaka u podacima koji neće biti pravovremeno detektovani i korigovani sprovođenjem interne kontrole.
- **Rizici detekcije** – rizici koje neće uočiti revizori tokom pregleda finansijskih izvještaja.

Izvođenje revizije IS-a

- Analiza dokumentacije
  - Upravljačka dokumentacija
  - Radni dokumenti
  - Pomoćni dokumenti

- Prikupljanje revizorskih dokaza
  - Intervjui, ankete i neformalni razgovori
  - Tehničko ispitivanje i testiranje sistema (vreme odziva, vreme reakcije, propusna moć, kapacitet sistema, pouzdanost, raspoloživost, …)
- Analiza i vrednovanje revizorskih dokaza
  - Ocena zaštite imovine sistema
  - Ocena delotvornosti sistema (kvalitet IS-a, kvalitet informacija, korisnost sistema, jednostavnost sistema, funkcionalnost sistema)
- Preporuke i izveštaj revizora IS-a
- Predstavljanje revizijskog izveštaja

Trajanje faza revizije IS-a

Faza revizije informacionog sistema banke	% od ukupnog vremena trajanja revizije
Priprema i planiranje	10
Analiza dokumentacije	10
Prikupljanje revizorskih dokaza: – Intervjui, ankete i neformalni razgovori – Tehničko ispitivanje i testiranje sistema	 10 15
Analiza i vrednovanje revizorskih dokaza	20
Priprema revizorskih izveštaja	20
Predstavljanje revizorskog izveštaja	5
Postrevizorske aktivnosti	10

Izveštaj revizora IS-a – nalazi, objašnjenje rizika, mišljenje, preporuke

Primer (Izveštaj revizora – X banka)

k4509024 www.fotosearch.com

- **Područje revizije:** Pristup programima i aplikacijama
- **Nivo rizika:** Srednji
- **Nalazi:**

  Slabosti u procesu otvaranja korisničkih naloga. Pronađeni su korisnički nalozi koji su otvoreni a da procedura nije u potpunosti poštovana.
- **Ocena rizika:**

  Neautorizovani pristup ključnim finansijskim aplikacijama i deljenje korisničkih naloga i lozinki može ugroziti integritet, validnost, tačnost i kompletnost finansijskih i drugih podataka koji su kritični za poslovanje.
- **Preporuke menadžmentu:**

  Pravilno pridržavanje već postojeće zvanične procedure za otvaranje korisničkih naloga (sa zahtevom za otvaranje naloga potpisanim od strane nadležnog rukovodioca odeljenja) i definisanje procedure za kontrolu čitavog procesa.

Izveštaj revizora IS-a - nalazi, objašnjenje rizika, mišljenje, preporuke

R. br	Područje	Observacija	Rizik	Zapis o diskusijama	Preporuke
1	**Izmene u aplika-cijama**	**<u>Procedura za izmene u aplikacijama ne poštuje se u potpunosti</u>** Za vreme našeg testiranja koje se odnosi na izmene u aplikacijama pronašli smo da se procedura koja je ustanovljena ne poštuje. Na 9 izmena (zahteva) u aplikacijama se pokazalo da procedura nije ispoštovana u potpunosti. U većini slučajeva (7) nije bilo moguće videti ko je isporučio i ko je implementirao izmenu. Takođe 5 izmena (zahteva) nije imalo formalno popunjenu sekciju prihvatanja od strane krajnjeg korisnika.	Procedura koja je trenutno važeća se mora poštovati dok se ne promeni. Testirali smo neke od izveštaja koji su propisani kao zakonska obaveza. Ako ne postoji formalno testiranje izmena od strane korisnika, kako Banka može biti sigurna da su izmene urađene korektno. Takođe, mora postojati odgovornost provajdera za svaku izmenu. Ovako Banka ne zna ko je i kada isporučio novu funkcionalnost i ko je implementirao. **Rizik: Srednji**	Ova primedba je razmotrena sa direktorom IT-a. Rukovodstvo se složilo sa iznetim argumentima i shvatilo je posledice ovog problema.	Zaposleni koji su zatražili promenu moraju preuzeti odgovornost u testiranju, i kada potvrde da je test urađen moraju preuzeti odgovornost za tu izmenu. Takođe, vendori moraju popunjavati njihov deo CC baze, tako da Banka zna ko je odgovoran i ko je isporučio izmenu a pre svega ko je implementirao izmenu. Procedura se mora u potpunosti poštovati od strane zaposlenih u Banci.
2	**Kompju-terske ope-racije**	**<u>Plan oporavka u slučaju katastrofe (DRP)</u>** Banka nema razvijen i implementiran plan oporavka u slučaju katastrofe, ali je na nivou kompanije implementiran Plan za obezbeđenje kontinuiteta poslovanja i da se tim planom definišu pravca daljeg razvoja DRP-a. IT odeljenje je formiralo zvaničan zahtev sa neophodnim elementima.	DR kontrole su važne operativne kontrole koje osiguravaju da će organizacija moći da nastavi sa poslovanjem u slučaju katastrofe. Nedostatak DRP-a može dovesti do ozbiljnih poslovnih problema u slučaju katastrofe. **Rizik: Visok**	Ova primedba je razmotrena sa IT direktorom. Rukovodstvo se složilo sa iznetim argumentima i shvatilo je posledice ovog problema.	**Kontrola za smanjenje rizika:** Preporučujemo da Banka pripremi i usvoji DRP koji uključuje makar sledeće: • detaljne i prioritetne procedure za određene osobe koje bi obezbedile potpuni oporavak na novoj lokaciji, ako je neophodno, dok se prvobitna lokacija popravlja ili obnavlja, • listu ključnog osoblja i njihovih brojeva za kontakt, • kompletan inventar hardvera i softvera, • sliku konfiguracije sadašnjeg hardvera i telekomunikacija • definiciju vremena za koje se aplikacije moraju oporaviti i staviti ponovo u funkciju da bi se izbegli značajniji gubici • zvaničan sporazum sa dobavljačem hardvera o isporuci hardvera koji zadovoljava tehničke specifikacije, u dogovorenom vremenskom periodu i na dogovorenu lokaciju, • ovakvi sporazumi moraju važiti i za raspoloživost druge lokacije, tako da hardver tamo može biti postavljen za kratko vreme u slučaju katastrofe, • Detaljne procedure za test u pisanoj formi.
3	**Pristup programi ma i aplika-cijama**	**<u>Slaba procedura za otvaranje korisničkih naloga</u>** Slabosti u procesu otvaranja korisničkih naloga. Pronađeni su korisnički nalozi koji su otvoreni a da procedura nije u potpunosti poštovana.	Neautorizovani pristup ključnim finansijskim aplikacijama i deljenje korisničkih naloga i lozinki može ugroziti integritet, validnost, tačnost i kompletnost finansijskih i drugih podataka koji su kritični za poslovanje. **Rizik: Srednji**	Ova primedba je razmotrena sa IT direktorom. Rukovodstvo se složilo sa iznetim argumentima i shvatilo je posledice problema.	Ove slabosti u kontroli su po svojoj prirodi ozbiljne, te mogu ozbiljno ugroziti ukupnu kontrolu u IT okruženju. **Kontrola za smanjenje rizika:** Pravilno pridržavanje već postojeće zvanične procedure za otvaranje korisničkih naloga (sa zahtevom za otvaranje naloga potpisanim od strane nadležnog Rukovodioca odeljenja) i definisanje procedure za kontrolu čitavog procesa.

Kontrola revizije informacionih sistema

- **U početnoj fazi revizorskog procesa** potrebno je kontrolisati ciljeve revizije i potrebna sredstva.
- **Tokom revizije** se kontroliše napredak u procesu revizije. Određena odstupanja od planirane dinamike potrebno je razmotriti i preduzeti odgovarajuće mere. Pored dinamike tokom kontrole se vrši i provera kvaliteta obavljenih aktivnosti.
- **U posljednjoj fazi revizije** se kontroliše sam rad revizora. Cilj ove kontrole je da se utvrdi da je radna dokumentacija nastala u procesu revizije potpuna, te da je rad koji je obavljen bio dobro planiran i nadziran, kao i da su primenjene odgovarajuće revizorske procedure. Ova kontrola se sprovodi pre potpisa konačnog izveštaja od strane odgovorne osobe.
- Tokom kontrole revizije posebna pažnja se posvećuje izveštajima o rezultatu revizije. Revizorski izveštaji moraju biti jasno i argumentovano potkrepljeni činjenicama. Izveštaj treba da sadrži preporuke i smernice za dalji rad.
- **Nakon završetka revizije** potrebno je osigurati dobijanje povratnih informacija, kako bi se utvrdilo da je revizija ostvarila svoj cilj i zadovoljila naručioce projekta.

Ocena revizije informacionih sistema

Revizija informacionih sistema je uspešna ukoliko uspe da odgovori na ključna pitanja koja se odnose na kvalitet informacionog sistema koji je bio predmet revizije.

1. Na koji način informacije utiču na rizik poslovanja banke?
2. U kojoj meri informacioni sistem odgovara potrebama banke?
3. Način na koji informacioni sistem utiče na očuvanje imovine banke?
4. Način na koji informacioni sistem utiče na efikasnost zaposlenih?
5. Na koji način informacije utiču na konkurentsku sposobnost banke?
6. Na koji način informacije koje nastaju u informacionom sistemu utiču na ponašanje osoba koje donose odluke?

Standardi revizije informacionih sistema

Posebna priroda revizije informacionih sistema zahteva standarde koji se mogu primeniti na reviziju konkretnog informacionog sistema.

Za te potrebe oformljena je **ISACA** (*Information System Audit and Control Association*) organizacija koja okuplja stručnjake iz celog sveta koji se bave upravljanjem, kontrolom, revizijom i bezbednošću informacionih sistema i ima za cilj donošenje i unapređenje primenjivih standarda.

- **Standardi** – njima se definiše:
  - Minimalni nivo prihvatljivih perfomansi revizije informacionih sistema, profesinalnih odgovornosti i etičkih kodeksa za revizore informacionih sistema;
  - Upravljanje i način profesinalnog obavljanja predviđenih aktivnosti;
  - Zahteve za certifikovanje i dobijanje zvanja certifikovanog revizora informacionog sistema (*eng. Certified Information System Auditor* – CISA).
- **Uputstva** (*eng. guidelines*) – predstavljaju vodiče za primenu revizorskih standarda. Svrha uputstava je obezbeđenje da izvedeni zaključci budu u skladu sa revizorskim standardima.
- **Procedure** - obezbeđuju informacije kako da se standardi primene u reviziji informacionih sistema.

ISACA
Serving IT Governance Professionals

Kodeks profesionalne etike

ISACA (*The Information Systems Audit and Control Association)* je donela Kodeks profesionalne etike kojeg treba obavezno da se pridržavaju njeni članovi i certifikovani revizori informacionog sistema (CISA) u svom radu :

- Pridržavati se Standarda za reviziju informacionog sistema koje je donela ISACA;
- Služiti u interesu zaposlenih, akcionara, klijenata i javnosti na najbolji mogući način i ne učestvovati u nikakvim ilegalnim ili neprimerenim aktinostima;
- Čuvati sve poverljive informacije do kojih se dođe u radu. Tako dobijene informacije ne smeju biti korišćene u cilju lične koristi ili dati trećim licima;
- Izvršavati svoje dužnosti na nezavisan i objektivan način i izbegavati aktivnosti koje ugrožavaju, ili mogu ugroziti, nezavisnost u radu;
- Informisati relevantne strane o rezultatima svog revizorskog rada;
- ...

ISACA®
Serving IT Governance Professionals

Regulativa i kriterijumi provere (revizije) uspešnosti IS-a

- **Zakonska regulativa**
- **Standardi i svetski priznati okviri** (COBIT, ISO 27000, ITIL, SAS 70,...)

  - Basel II okvir - koji banka obvezno treba da koristiti u svrhu boljeg upravljanja operativnim rizicima
- **Politike i pravila preduzeća**

BANK FOR INTERNATIONAL SETTLEMENTS

ISO International Organization for Standardization

ZAKLJUČAK

- Revizija informacionog sistema spaja informacionu i ekonomsku komponentu poslovnog sistema.
- Rezultat revizije je davanje preporuka ili signala menadžmentu u pravcu poboljšanja poslovnih procesa i organizacije.