

● Interna revizija informacijskog sustava osiguravajućeg društva

Arlena Štulić, Služba interne revizije

Sadržaj

1. Uvod
2. Interna revizija
3. Informacijski sustav
4. Potreba za revizijom informacijskog sustava
5. Revizija informacijskog sustava
 - a) Revizijski standardi informacijskog sustava
 - b) Faze revizije informacijskog sustava
6. Kontrole revizije informacijskog sustava
7. Koristi revizije informacijskog sustava

1. Uvod

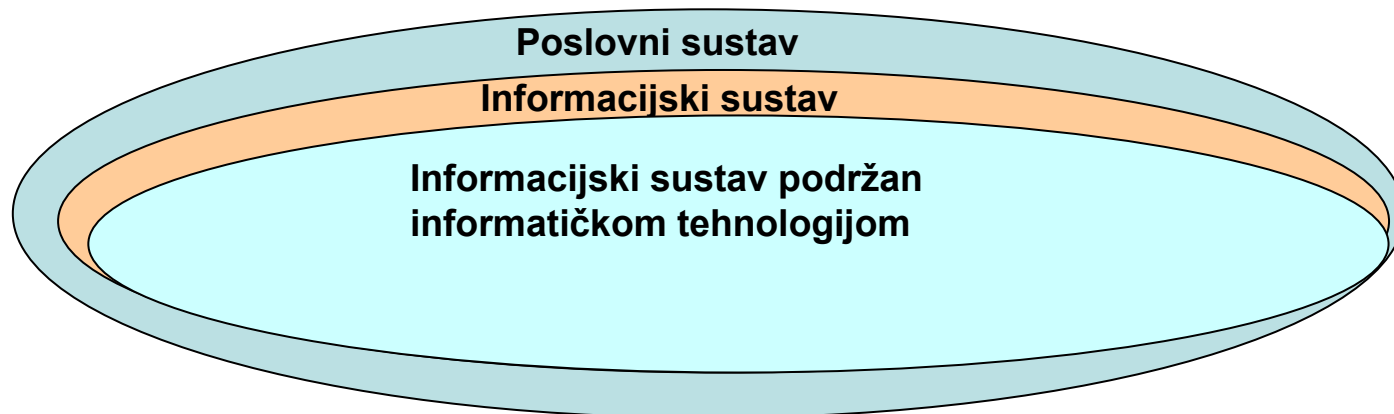
- Imidž – slika sigurnosti i stabilnosti
- “Veliko” i “SIGURNO”
- Ulaganje u informatičku tehnologiju > povećanje efikasnosti poslovnog sustava
- Upotreba tehnologije stvara rizik
- Nemogućnost zakona u praćenju ritma razvoja tehnologije

2. Interna revizija

- Procjena sukladnosti ciljeva informacijskog sustava sa:
 - Zakonima,
 - Strategijom,
 - Standardima,
 - Najboljim praksama
- Ocjena uputa, procedura, mjera i praksi
- Očuvanje dostupnosti, cjelovitosti i povjerljivosti informacija
- Neovisna ocjena funkcionalnosti informacijskog sustava
- Ukazivanje na rizike i moguće štete
- Mjerenje i izvještavanje o ispunjenju ciljeva

3. Informacijski sustav

- “Organizacijski uređen i svrhovit skup aktivnosti, postupaka, metoda i tehnologije za prikupljanje, obradu, čuvanje i distribuciju poslovnih informacija”.
- 90% informacijskog sustava podržano informatičkom tehnologijom
- Informacijski sustav je jak koliko je jaka njegova najslabija karika



4. Potreba za revizijom informacijskog sustava (1)

- Povećanje količine poslovnih informacija
- Složena obrada podataka
- Kontrola toka poslovnih informacija
- Upravljanje poslovnim informacijama uz pomoć informacijskog sustava
- Klasifikacija poslovnih informacija
- Kontrola pristupa poslovnim informacijama

4. Potreba za revizijom informacijskog sustava (2)

- Smanjenje izloženosti rizicima:
 - Neisplativih ulaganja u IT (40% direktora financija zadovoljni rezultatima ulaganja u IT – časopis CFO 2005., 42% društava imalo negativne financijske pokazatelje unatoč ulaganjima u IT – Strassmann, “Information Payoff”)
 - Neuspješne provedbe IT projekata (samo 30% IT projekata se smatra uspješnima, 20% IT troškova je nepotrebno – Gartner 2002.)
 - Operativnih performansi informatizacije (fokus na određena područja IS-a, dok se druga zapostavljaju – DeLeone, McLean – “Information systems success: the quest for the dependent variable”)
 - Prekid odvijanja poslovnih procesa (93% društava bez BCP nakon proživljene katastrofe se ugase nakon 5 godina – Disaster Recovery Institute 2005.)
 - Napada na imovinu IS-a

5. Revizija informacijskog sustava

- Revizija cjelokupne tehnologije informacijskog sustava
- Vrste revizije informacijskog sustava
 - Samostalna revizija IS-a
 - Revizija dijela IS-a u sklopu integralne revizije
- Skupine kontrola IS-a:
 - kontrole okruženja,
 - fizičke sigurnosne kontrole,
 - logičke sigurnosne kontrole,
 - kontrole operacijskog sustava

5. a) Revizijski standardi informacijskog sustava

- ISO-9786 – Informacijska tehnologija – Security techniques
- ISO-17799 – Principi upravljanja informacijskom sigurnošću
- ISO-27001 – Sustav upravljanja informacijskom sigurnošću
- ISO-20000 – Upravljanje uslugama
- ITIL – Information Technology Infrastructure Library
- FIPS – Državni standard za obradu informacija (USA)
- COBIT – Skup najboljih praksi pri upravljanju i revidiranju informacijskih sustava

5. b) Faze revizije informacijskog sustava

1. Planiranje
 - a) Definiranje ciljeva revizije informacijskog sustava
 - b) Prikupljanje općih informacija o sustavu
 - c) Raspodjela radnih zadataka unutar revizijskog tima
 - d) Identifikacija mogućih revizijskih rizika
 - e) Identifikacija izvora potrebnih dokaza
2. Testiranje internih kontrola
 - a) Provjera pisanih procedura
 - b) Provjera ovlaštenja korisnika
 - c) Provjera ovlaštenja zaposlenika informatičko-administrativnog osoblja
 - d) Provjera pristupa aplikacijama i podacima
 - e) Provjera aplikativnih kontrola
3. Testiranje transakcija
 - a) Provjera ispravnosti izvršavanja transakcija
 - b) Provjera djelotvornosti i učinkovitosti transakcija

5. c) Faze revizije informacijskog sustava

4. Testiranje sukladnosti
 - a) Provjera sukladnosti kontrola s relevantnom eksternom legislativom
 - b) Provjera jednakosti podataka između različitih organizacijskih jedinica
5. Testiranje ukupnih rezultata
6. Identificiranje naknadno utvrđenih rizika obavljenom revizijom
7. Objedinjavanje rezultata revizije
8. Izrada revizijskog izvještaja, te pružanje smjernica za poboljšanjem
9. Praćenje implementacije danih smjernica

6. Kontrole revizije informacijskog sustava

- Aktivnosti vezane za ispitivanje sustava potrebno pažljivo planirati kako ne bi utjecale na izvođenje poslovnih procesa
- Smjernice za implementaciju:
 - Potrebno odobrenje uvjeta od odgovornog menadžmenta
 - Doseg ispitivanja provjeren i kontroliran
 - Provjere nad podacima uz isključivo pravo čitanja podataka
 - Sve procedure, uvjeti i obveze uredno dokumentirani
 - Revizor neovisan od ispitivanih aktivnosti

7. Koristi revizije informacijskog sustava

- Postizanje sukladnosti ciljeva informacijskog sustava sa strategijom tvrtke
 - Postizanje sukladnosti sa relevantnom eksternom legislativom
 - Utvrđivanje stupnja rizika
 - Utvrđivanje efikasnosti i efektivnosti kontrola
 - Mogućnost sustavnog pristupa u zaštiti društva od opasnosti i mogućih troškova računalne zlouporabe
 - Utvrđivanje opravdanosti povrata iz ulaganja u rješenja i tehnologije za informacijsku sigurnost
 - Upravljanje i kontrola troškova informacijskog sustava
 - Neovisna ocjena zrelosti informacijskog sustava
 - Implementacija najboljih praksi u upravljanju rizicima
-
- Preporuke za unapređenjem
 - Osiguranje implementacije preporuka kroz sustavno praćenje