



HRVATSKA NARODNA BANKA

Odluka o primjerenom upravljanju informacijskim sustavom

Damir Blažeković, CISA

voditelj Odjela za izravni nadzor informacijskih sustava banaka

Zagreb, 28. svibnja 2008.

SADRŽAJ

- Rezultati analize upitnika o informacijskom sustavu
- Koncept *Odluke o primjernom upravljanju informacijskim sustavom*
- Obveze banaka u razdoblju od 2008. – 2010.
- Otvorena pitanja

REZULTATI ANALIZE UPITNIKA

-uvod-

- ❑ u ožujku 2007. godine upućen je, svim bankama čija je pojedinačna aktiva u odnosu na ukupnu aktivu bankarskog sustava manja od 1%, upitnik o informacijskom sustavu
- ❑ 23 banke i 5 stambenih štedionica
- ❑ 317 pitanja iz 8 područja
- ❑ obrađeno je ukupno 8876 odgovora
- ❑ za svako pitanje - jedan od odgovora (Da ili Ne)
 - iznimka - pitanja gdje se tražila brojčana vrijednost
- ❑ odgovori na pitanja popraćeni su očitovanjima predsjednika Uprava banka o objektivnosti i istinitosti odgovora

REZULTATI ANALIZE UPITNIKA

-obuhvat analize/metodologija-

- ❑ analizirana područja informacijskog sustava:
 - UIS - UPRAVLJANJE INFORMACIJSKIM SUSTAVOM
 - URIS - UPRAVLJANJE RIZIKOM INFORMACIJSKOG SUSTAVA
 - UVR - UNUTARNJA I VANJSKA REVIZIJA
 - SIS - SIGURNOST INFORMACIJSKOG SUSTAVA
 - OIS - ODRŽAVANJE INFORMACIJSKOG SUSTAVA
 - RIE - RAZVOJ INFORMACIJSKOG SUSTAVA I EKSTERNALIZACIJA
 - UKP - UPRAVLJANJE KONTINUITETOM POSLOVANJA
 - EB - ELEKTRONIČKO BANKARSTVO

- ❑ odgovori određuju stanje pojedinih elemenata informacijskog sustava na način kakvim ga vide banke

- ❑ bodovana su pitanja čiji su odgovori "Da" ili "Ne", a za očekivati je da neposredno utječu na razinu rizika

- ❑ najvažnija pitanja nose 5 bodova, a najmanje važna 1 bod

REZULTATI ANALIZE UPITNIKA

(iz ožujka 2007.)

- **najrizičnija područja:**
 - upravljanje rizikom informacijskog sustava
 - unutarnja i vanjska revizija
 - upravljanje kontinuitetom poslovanja
 - sigurnost informacijskog sustava

Koncept *Odluke*

- I Opće odredbe
- II Značenje pojmova
- III Okvir za upravljanje informacijskim sustavom
- IV Upravljanje rizikom informacijskog sustava
- V Unutarnja revizija
- VI Sigurnost informacijskog sustava
- VII Održavanje informacijskog sustava
- VIII Upravljanje kontinuitetom poslovanja
- IX Razvoj informacijskog sustava i eksternalizacija
- X Elektroničko bankarstvo
- XI Prijelazne i završne odredbe

Značenje pojmova

- bolje razumijevanje sadržaja *Odluke*
- smanjuje se mogućnost nerazumijevanja ili pogrešnog shvaćanja odredaba *Odluke*:
 - resursi informacijskog sustava (da li uključuju i informacije?)
 - korisnici informacijskog sustava (da li uključuju i korisnike elektroničkog bankarstva koji nisu djelatnici banke?)
- većina pojmova povezanih s informacijskom tehnologijom potječe iz engleskog jezika
- potrebno definiranje pojmova za koje ne postoji opće prihvaćeni naziv na hrvatskom jeziku (*log, outsourcing, Recovery time objective, Recovery point objective, utility, driver, log*)
- pojmovi u *Odluci* su definicije za potrebe primjene *Odluke*
- u *Odluci* je objašnjeno ukupno **39** pojmova koji se koriste u člancima *Odluke*

Organizacijske i kadrovske promjene

□ **Voditelj organizacijske jedinice informacijske tehnologije**

- treba imati jasno definirane ovlasti, odgovornosti i djelokrug rada
- treba biti zadužen za upravljanje i koordinaciju rada organizacijske jedinice informacijske tehnologije te funkcionalnost i djelotvornost informacijskog sustava u cjelini

□ **Odbor za upravljanje informacijskim sustavom (2008.)**

- čija je uloga praćenje i nadziranje informacijskog sustava i njegovih aktivnosti te koordinacija inicijativa vezanih uz informacijski sustav, a koje se tiču usklađenosti s poslovnim ciljevima i poslovnom strategijom
- poveznica poslovnih korisnika i osoba koje razvijaju i održavaju informacijski sustav te se brinu o sigurnosti informacijskog sustava.

Organizacijske i kadrovske promjene

- ❑ **Voditelj sigurnosti informacijskog sustava (2009.)**
 - treba biti neovisan o funkciji voditelja organizacijske jedinice za informacijsku tehnologiju
 - treba biti usmjeren na pitanja sigurnosti informacijskog sustava u cjelini
 - na primjeren način nadzirati i koordinirati aktivnosti vezane uz sigurnost informacijskog sustava u skladu s ovlastima, odgovornostima i djelokrugom rada
 - inicirati primjenu dobrih praksi i prihvaćenih standarda vezanih uz sigurnost informacijskog sustava
 - imati savjetodavnu ulogu u svezi sa sigurnošću informacijskog sustava

- ❑ **Unutarnji revizor informacijskog sustava - IT revizor (2009.)**
 - unutarnja revizija dužna je obavljati reviziju informacijskog sustava banke

Uspostava različitih procesa

- ❑ proces izvješćivanja uprave i nadzornog odbora banke (2008.)
- ❑ proces upravljanja rizikom informacijskog sustava (2009.)
- ❑ proces upravljanja incidentima (2009.)
- ❑ proces razvoja informacijskog sustava (2009.)
- ❑ sustav upravljanja korisničkim pravima pristupa (2009.)
- ❑ proces upravljanja hardverskom imovinom informacijskog sustava tijekom njezina životnog ciklusa (2009.)
- ❑ postupci izrade, pohrane, održavanja i čuvanja dokumentacije koja se odnosi na informacijski sustav (2009.)
- ❑ proces planiranja kontinuiteta poslovanja (2010.)
- ❑ proces upravljanja pričuvnom pohranom (2010.)
- ❑ proces upravljanja promjenama softverskih komponenata informacijskog sustava (2010)

Usvajanje i primjena internih akata

- ❑ **strategija informacijskog sustava (2008)**
- ❑ **metodologije (2009.):**
 - **metodologija upravljanja projektima** kojom će se definirati kriteriji, načini i postupci upravljanja projektima vezanima uz informacijski sustav
 - **metodologija upravljanja rizikom informacijskog sustava** kojom će se definirati kriteriji, načini i postupci upravljanja rizikom informacijskog sustava
 - **metodologija za provođenje revizije informacijskog sustava** zasnovana na procjeni rizika, a kojom se definiraju kriteriji, načini i postupci revizije informacijskog sustava banke

Usvajanje i primjena internih akata

- **planovi:**
 - strateški i operativni planovi koji proizlaze iz strategije informacijskog sustava (2009.)
 - plan(ovi) kontinuiteta poslovanja (2010.)
 - plan(ovi) oporavka informacijskog sustava (2010.)
- **Politika sigurnosti informacijskog sustava (2009.)**
- **akti kojima se uređuje upravljanje informacijskim sustavom** (primjerice, različite vrste politika, procedura, uputa vezanih uz informacijski sustav) - 2009.

Izvješća

- ❑ pisano izvješće o provedenoj analizi utjecaja na poslovanje (BIA)
- ❑ pisana izvješća o rezultatima testiranja:
 - plan(ova) kontinuiteta poslovanja (BCP)
 - plan(ova) oporavka informacijskog sustava (DRP)
- ❑ rezultati procjene rizika informacijskog sustava
- ❑ pisana izvješća za upravu i nadzorni odbor banke o relevantnim činjenicama vezanima uz funkcionalnost i sigurnost informacijskog sustava
- ❑ pisana izvješća unutarnje revizije o provedenim revizijama (dijela) informacijskog sustava

Kontrola/nadzor provedbe *Odluke*

- ❑ revizijom informacijskih sustava od strane unutarnje revizije banke
- ❑ revizijom informacijskih sustava od strane vanjskog revizora
- ❑ izravnim nadzorima informacijskih sustava banaka od strane HNB-a
- ❑ dostavljanjem dokumentacije u HNB (Direkcija bonitetne analize)
- ❑ različitim istraživanjima (ankete, upitnici....)

Rokovi primjene *Odluke*

- ❑ *Odluka o primjernom upravljanju informacijskim sustavom* stupila je na snagu **1. siječnja 2008. godine**
- ❑ stupanje na snagu pojedinih članaka *Odluke* definirano je u poglavlju **XI-Prijelazne i završne odredbe**
- ❑ rokovi za primjenu pojedinih članaka *Odluke* definirani su u razdoblju od **siječnja 2008. do srpnja 2010. godine**
- ❑ uspostava svih navedenih procesa zahtijeva vrijeme i ljudske resurse
- ❑ uspostava nekih procesa odvijat će se paralelno i zahtijevat će angažman istih ljudskih resursa

Rokovi primjene *Odluke*

- primjerice, projekt uspostave procesa planiranja kontinuiteta poslovanja (BCP):
 - za takav projekt potreban je angažman većine organizacijskih jedinica u bankama
 - u pravilu takav projekt traje duže od godinu dana

- rokovi u Odluci su **krajnji rokovi**, što ne znači da ih banka ne može ranije ispuniti ili da HNB ne može sukladno procjeni stanja informacijskog sustava odrediti i kraći rok ukoliko je rizik koji proizlazi iz korištenja informacijske tehnologije odnosno informacijskog sustava velik

- zadovoljavanje forme nije ideja *Odluke* (banka treba dokazati da je nešto uistinu implementirala i testirala)

- u konačnici primjena *Odluke* trebala bi pomoći bankama u procesu planiranja i budžetiranja kako bi se IT rizici u što kraćem roku sveli na prihvatljivu razinu



HRVATSKA NARODNA BANKA

HVALA NA PAŽNJI

PITANJA?
