

**DOBRE PRAKSE ZA UPRAVLJANJE OPERATIVNIM
RIZIKOM I NADZOR NAD NJIM, 02/2003**
Baselski odbor za nadzor banaka

**SMJERNICE ZA UPRAVLJANJE
INFORMACIJSKIM SUSTAVOM U CILJU SMANJENJA
OPERATIVNOG RIZIKA, 03/2006**

HNB

**EN ISO 27001:2005
SUSTAV UPRAVLJANJA INFORMACIJSKOM
SIGURNOŠĆU, 2005**

Adria Kon
www.adriakon.hr

**DOBRE PRAKSE ZA UPRAVLJANJE OPERATIVNIM RIZIKOM I NADZOR
NAD NJIM, 02/2003, Baselski odbor za nadzor banaka**

Operativni rizik:

Rizik od gubitaka koji nastaje zbog neprimjerenih ili
neuspješnih unutarnjih procesa, ljudi ili sustava ili zbog
vanjskih događaja

Osim kreditnog, kamatnog i tržišnog rizika:

- veća uporaba visoko automatizirane tehnologije *
- rast elektroničkog poslovanja *
- stjecanja, spajanja, razdvajanja i konsolidacije –
utjecaj na integrirane sustave *
- unutarnje kontrole i sigurnosni sustavi visokog
stupnja, zbog velikih razmjera *
- tehnike rizika generiraju nove rizike – pravne
- eksterinizacija i kliring – smanjuju ali stvaraju nove
rizike

**DOBRE PRAKSE ZA UPRAVLJANJE OPERATIVNIM RIZIKOM I NADZOR
NAD NJIM, 02/2003, Baselski odbor za nadzor banaka**

Pristup operativnom riziku:

- Veličina i razna tehničke opremljenosti
- Priroda i složenost njenih aktivnosti

Razlozi operativnog rizika s velikim gubicima:

- unutarnja prijevara: pogrešno izvješćivanje, krađa i trgovanja *
- vanjska prijevara: pljačka, krivotvorenje, neovlaštena uporaba racuna *
- zapošljavanje i zaštita na radnom mjestu: potraživanja radnika, kršenje zakona diskriminacija i opće odgovornosti
- klijenti, proizvodi i poslovne prakse: neprimjerene aktivnosti trgovanja, zlouporaba informacija, pranje novca *
- oštećenje materijalne imovine: terorizam, vandalizam, potresi, požari i poplave

**DOBRE PRAKSE ZA UPRAVLJANJE OPERATIVNIM RIZIKOM I NADZOR
NAD NJIM, 02/2003, Baselski odbor za nadzor banaka**

Operativni rizik:

- uz Kreditni, Kamatni, Likvidnosni rizik
- Ne preuzima se izravno, u zamjenu za očekivanu dobit
- Prisutan i može izazvati gubitke

Načela razvijanja primjerne okoline za upravljanje rizikom:

1. Odbor Direktora treba usvojiti i periodično preispitivati upravljanje operativnim rizikom

Definirati načela za utvrđivanje, procjenjivanje, nadziranje i kontrolu-smanjivanje rizika. Or,Me

**DOBRE PRAKSE ZA UPRAVLJANJE OPERATIVNIM RIZIKOM I NADZOR NAD NJIM,
02/2003, Baselski odbor za nadzor banaka**

Načela razvijanja primjerne okoline za upravljanje rizikom:

2. Odbor Direktora osigurava unutarnju raviziju od neovisnog i sposobnog osoblja, koje ne upravlja operativnim rizikom Or,Ob
3. Viša uprava provodi a djelatnici su upoznati na svojim razinama. Razvijanje politike, procesi i postupci vezano uz upravljanje rizikom za značajne proizvode, procese i sustave banke. Or, Ob, Te
4. Utvrditi i procijeniti operativni rizik za proizvode, aktivnosti, procese i sustave, posebno prije uvođenja novih. Or, Me, Te
5. Redovno nadziranje profila rizika i izloženosti gubicima. Potrebno stalno izvješćivanje više uprave i odbora direktora. Or
6. Politike, procesi i postupci za kontroliranje-smanjivanje rizika, periodičko preispitivanje tih strategija i prilagodba svom profilu Me
7. Izraditi planove za nepredviđene okolnosti i planove za očuvanje kontinuiteta poslovanja Or,Ob,Me,Te

**DOBRE PRAKSE ZA UPRAVLJANJE OPERATIVNIM RIZIKOM I NADZOR NAD NJIM,
02/2003, Baselski odbor za nadzor banaka**

Načela razvijanja primjerne okoline za upravljanje rizikom:

8. Bankovni supervizori zahtijevati sustav upravljanja rizikom
9. Supervizori trebaju vrednovati politike, postupke i prakse banke vezano uz operativne rizike. Moraju postojati mehanizmi o obavješćavanju. Or
10. Objavljivati dovoljno informacija sudionicima na tržištu za procjenu pristupa upravljanja operativnim rizikom. Or

Or – organizacija
Ob – obrazovanje
Me – metodologije
Te - tehnologije

**DOBRE PRAKSE ZA UPRAVLJANJE OPERATIVNIM RIZIKOM I NADZOR NAD NJIM,
02/2003, Baselski odbor za nadzor banaka**

Načelo 6.:

...

- 38. ... zaštitu procesne tehnologije i informacijske tehnologije, ... povećana automatizacija može učestale gubitke malih vrijednosti pretvoriti u rijetke gubitke velikih vrijednosti. ...**

Načelo 7.

Banke trebaju imati planove za nepredviđene okolnosti i planove za očuvanje kontinuiteta poslovanja kako bi osigurale svoju sposobnost trajnog poslovanja i ograničile gubitke u slučaju ozbiljnog poremećaja u poslovanju:

- 42. ... uzeti u obzir različite vrste mogućih scenarija prema kojima banka može biti osjetljiva, ovisno o veličini i složenosti poslovanja banke.**

**DOBRE PRAKSE ZA UPRAVLJANJE OPERATIVNIM RIZIKOM I NADZOR NAD NJIM,
02/2003, Baselski odbor za nadzor banaka**

Načelo 7.

- 43. ... utvrditi ključne poslovne procese, uključujući one kod kojih postoji ovisnost o vanjskim izvršiteljima ili ostalim trećim stranama. ... utvrditi alternativne mehanizme za ponovnu uspostavu pružanja usluga u slučaju prekida rada. ... sposobnosti obnavljanja elektroničke ili materijalne evidencije koja je prijeko potrebna za ponovnu uspostavu poslovanja. ...**
- 44. ... periodično preispitivati svoje planove za oporavak od katastrofe i očuvanja kontinuiteta poslovanja ... periodično testirati ...**

RIZICI

Klasifikacija imovine:

- **Informacijska imovina**
- **Papirnati dokumenti**
- **Software**
- **Fizička imovina**
- **Ljudi**
- **Usluge**
- **Nematerijalna imovina**
- **Novac**

RIZICI

Prihvaćanje rizika	Risk Acceptance
Analiza rizika	Risk Analysis
Proračun rizika	Risk Evaluation
Procjena rizika	Risk Assessment
Upravljanje rizikom	Risk Management
Postupanje rizikom	Risk Treatment

RIZICI

Analiza rizika

Risk Analysis

- modeliranje poslovnih procesa
- klasificiranje i procjena imovine
- procjena prijetnji (threats) i ranjivosti (vulnerabilities)
- procjena rezultirajućeg rizika
- sustavna uporaba informacija kako bi se identificirali izvori i procijenio rizik

Upravljanje rizikom

Risk Management

- preporuke za protumjere
- identifikacija postojećih protumjera
- selekcija i implementacija protumjera
- scenarij "what if"

RIZICI

Metode:

Kvantitativna analiza:

uzima u obzir vjerojatnost i nastalu štetu

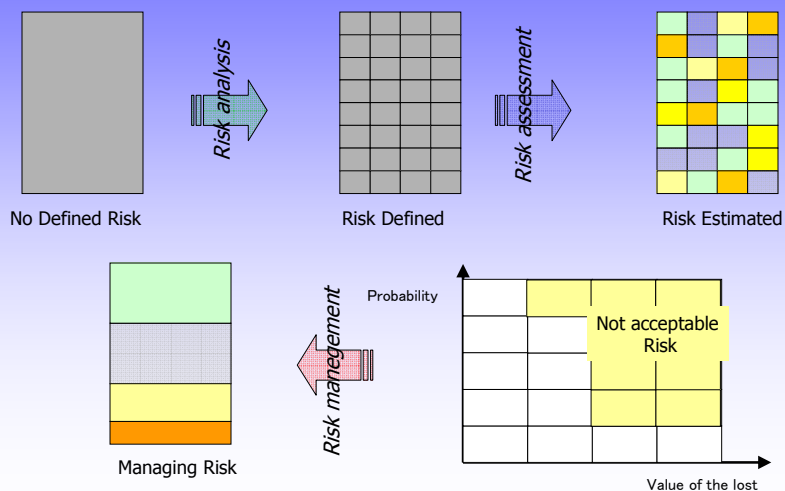
Polu-kvantitativna:

uzima u obzir prijetnje, ranjivost i utjecaj

Kvalitativna:

uzima u obzir sve vrste prijetnji, vjerojatnost i posljedice

Risk Assessment & Management



SMJERNICE ZA UPRAVLJANJE INFORMACIJSKIM SUSTAVOM U CILJU SMANJENJA OPERATIVNOG RIZIKA, 03/2006, HNB

Upravljanje informacijskim sustavom

Upravljanje rizikom informacijskog sustava

Unutarnja revizija

*

Sigurnost informacijskog sustava

Održavanje informacijskog sustava

Planiranje kontinuiteta poslovanja

Razvoj sustava i eksternalizacija

E-bankarstvo

(Načela upravljanja rizikom u elektroničkom bankarstvu, 07/2003)

ANEKS A - ISO 27001

SIGURNOSNA POLITIKA POLITIKA SIGURNOSTI INFORMACIJA DOKUMENT O POLITICI SIGURNOSTI INFORMACIJA PREGLED I PROCJENA	KONTROLA PRISTUPA ZAHTJEVI POSLOVANJA ZA KONTROLU PRISTUPA UPRAVLJANJE PRISTUPOM KORISNIKA ODGOVORNOSTI KORISNIKA KONTROLA PRISTUPA MREŽI KONTROLA PRISTUPA OPERATIVNOM SUSTAVU KONTROLA PRISTUPA APLIKACIJI NADZOR NAD PRISTUPANJEM I KORIŠTENJEM SUSTAVA MOBILNO RAČUNARSTVO I RAD NA DALJINU
SIGURNOST U ORGANIZACIJI INFRASTRUKTURA INFORMACIJSKE SIGURNOSTI SIGURNOST PRISTUPA TREĆE STRANE VANJSKI IZVORI	RAZVOJ I ODRŽAVANJE SUSTAVA SIGURNOSNI ZAHTJEVI SUSTAVA SIGURNOST U SUSTAVIMA APLIKACIJA KRIPTOGRAFSKE KONTROLE SIGURNOSTI SISTEMSKIH DATOTEKA SIGURNOST U POSTUPCIMA ZA RAZVOJ I PODRŠKU
KLASIFIKACIJA I KONTROLA DOBARA ODGOVORNOST ZA DOBRA KLASIFIKACIJA INFORMACIJA	UPRAVLJANJEM STALNOŠĆ U POSLOVANJA ASPEKTI UPRAVLJANJA STALNOŠĆ U POSLOVANJA
SIGURNOST OSOBLJA SIGURNOST U ODREĐIVANJU POSLOVA I RESURSA OBUKA KORISNIKA REAKCIJE NA SIGURNOSNE INCIDENTE I NEDOSTATKE	SUKLADNOST SUKLADNOST ZA ZAKONSKIM ZAHTJEVIMA PREGLED SIGURNOSNE POLITIKE I TEHNIČKE SUKLADNOSTI MIŠLJENA O SISTEMSKOM AUDITU
FIZIČKA SIGURNOST I SIGURNOST OKOLIŠA PODRUČJA SIGURNOSTI SIGURNOST OPREME OPĆE KONTROLE	
UPRAVLJANJE KOMUNIKACIJAMA I RADOM OPERATIVNI POSTUPCI I ODGOVORNOSTI SUSTAV ZA PLANIRANJE I PRIHVATANJE ZAŠTITA OD ZLONAMJERNOG SOFTWARE-a ODRŽAVANJE UPRAVLJANJE MREŽOM RUKOVANJE MEDIJIMA I SIGURNOST RAZMJENA INFORMACIJA I SOFTWARE-a	

ISO 13335 "Guidelines for the Management of Information Security"
ISO 13569 "Banking and Related Financial Services – Information Security Guidelines"
ISO 15408 "Evaluation Criteria for IT Security (Common Criteria)"

USA NIST's 800 Series
USA GAO's Federal Information Systems Controls Audit Manual (FISCAM)
German BSI "IT Baseline Protection Manual"

ISF's Standard of Good Practice
SEI's OCTAVE
SEI's SW-CMM
ISACA's COBIT
FFIEC IT Examination Handbooks
ISSA's GAISP
 ...

RIZICI – APEKTI - PROCJENA

	Važnost (1-10):		
	Back-up	Antivirus	Tajnost
1. Proizvodno poduzeće	5	3	8
2. Novinska kuća	8	8	8
3. Trgovačko poduzeće	5	3-8	5
4. Financijska ustanova	5	3	9
5. Turistička ustanova	3	7	9

...,zatvoreni sustavi, real-time sustavi,...

RIZICI HW

Utjecaj:

ograničen na radno mjesto
unutar organizacije
šire
zaštita u okviru tekućih troškova
treba dodatna sredstva

Vlastita ocjena:

važan
nepoznato
samostalni nadzor moguć
potrebna vanjska usluga

Važnost:

za tim za sigurnost
za korisnika
za korisnikov odjel
za ustanovu

Zainteresirane strane:

pritužba (korisnika, ...)
medijska ili pravna reakcija moguća
Nepoznato

Zakonski zahtjev:

jasan
naslućuje
nepoznat
nema

RIZICI SOFTWARE

- ...
 - Uredski programi
 - E-mail programi
 - Internet
 - Aplikacije
 - Sistemska SW
 - ...
- ...
 - virusi
 - spyware
 - greške u korištenju
 - pogrešan unos
 - neovlaštene instalacije
 - privatna upotreba
 - poslovna tajna
 - lozinke
 - E-mail
 - internet
 - ...

RIZICI DOBAVLJAČI

- Podaci/aktivnost/oprema
- Dobavljač
- Trajanje ugovora
- Ugovoren odziv
- Procjena rizika
- Zastoj kod kvara izražen u vremenu
- Zastoj kod kvara izražen u vrijednosti
- Protokoli kod prekida suradnje
- Postupci kod incidenta
- Lista odobrenog osoblja
- Ograničenje pristupa

RIZICI OSOBLJE

Broj sa she me	HW rizik A	SW rizik B	Tajn ost poda taka C	Uključ eno u back up	Potrebn o obrazov anje opće	Potreb no obrazo vanje sigurn ost	Priman je statisti ka- sigurn osti	Lokacije važnost		
								za tim	za ustanov u	za javnos t
10	2,3		1,2,3	odjelni			NE	3	3	5
11	2,3	1,2,3,4	1,2,3	osobni			DA	3	1	1
12	2,3	1,2,3,4	1,2,3	osobni	off, autocad		NE	5	1	1
13	2,3	1,2,3,4	1,2	osobni	off, autocad		NE	5	1	1
...										

RIZICI OSTALO

- ...
- požar
 - poplava
 - krađa
 - energetika i instalacije
 - el. ometanja
 - neovlašteni pristupi
 - greške trećih strana (dobavljači,...)
- ...

PRAVNI ASPEKTI:

Interni:

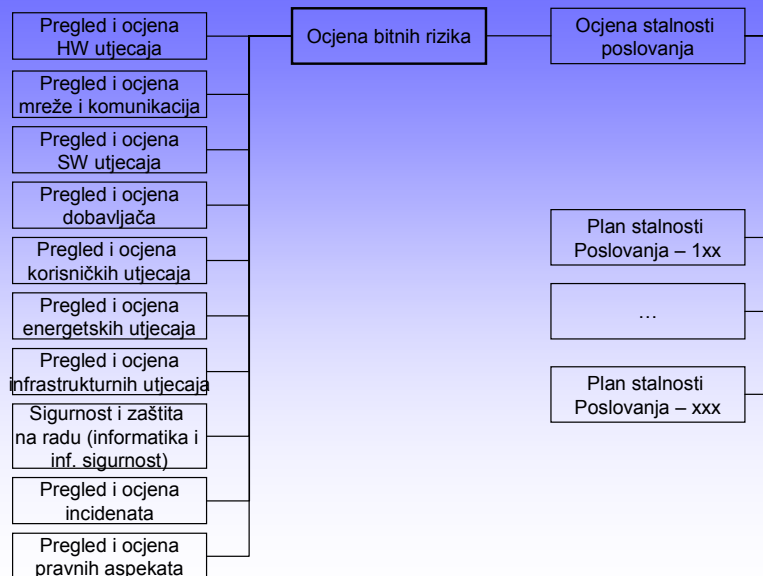
- tajnost podatka – pravila ponašanja (osoblje)
- strukture podataka (službeno, interno, javno)
- kvalifikacija – procjena osoblja

Dobavljači:

- tajnost podatka – pravila
- prava pristupa
- prijelazni period (otkaz)
- odgovornost za štetu

Treće strane:

- tajnost podataka – pravila ponašanja
- kvalifikacija - procjena osoblja



PLAN STALNOSTI POSLOVANJA (BUSINESS CONTINUITY PLAN) Datum revizije: _____
SERVERI I SERVERSKA PROSTORIJA (ako je pojedinačni server, naziv s servera)

A instalacija: 1 nova oprema 2 migracija 3 integracija 4 druga.....
 B intervencija: 5 testiranje 6 neispravnost 7 završena 8 druga.....
 C demonstracija D prezentacija E vježba F istraživanje G druga.....

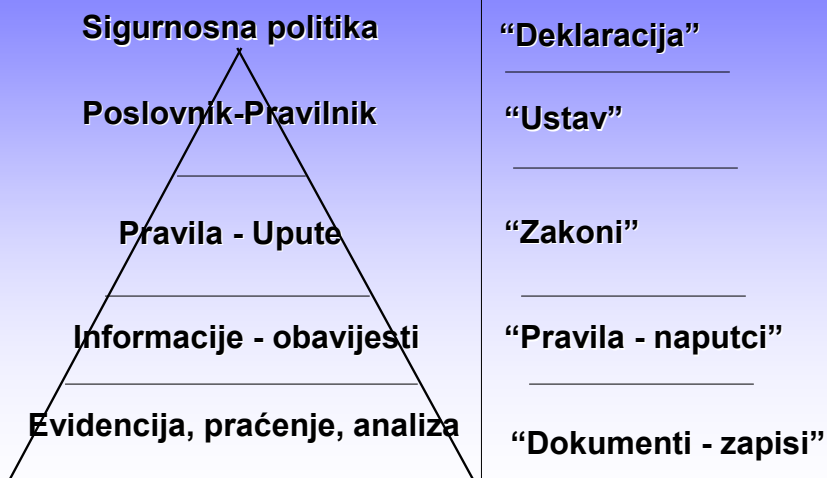
Datum aktivnosti: _____ Zahtjevatelj: _____ Koordinator: _____ Naslov: _____

1. Oprema i lokacija: _____
 2. Ciljano vrijeme oporavka: _____
 3. Obavješćavanje: _____
 4. Dokumentacija – upute: _____

Planirani resursi – oprema – osoblje – izvođači:	Dinamika:	Rizik:
.....
.....
.....

Rizici i utjecaji: _____

STRUKTURA DOKUMENTI ISO 27001:



Organizacijski preduvjeti:

- tajnost podatka – pravila ponašanja (osoblje)
- strukture podataka (službeno, interno, javno)
- odgovorne osobe
- pregled rizika – procesi (povezani sa informacijskim teh.)

Tehnički preduvjeti:

- pregled opreme: HW, SW, comm.
- pregled lokacija
- pregled rizika - resursi

Funkcionalne operativne upute:

- stalnost poslovanja
- zaštita podataka

Koraci (informacijska sigurnost):

- snimka stanja prema zahtjevima HNB +:
 - primjedbe revizije
 - primjedbe HNB
- organizacija i interna pravila
- snimka važnosti procesa
- snimke stanja strukture resursa
- minimalne operativne upute
- ocjena rizika
- ocjena primjenjivih zahtjeva HNB
- izrada organizacijske i tehničke dokumentacije
- definiranje tehničkog i internog nadzora
- periodička provjera sustava

DOSTUPNOST, POVJERLJIVOST, INTEGRITET:

Sigurnost nije stanje nego proces.

**Alat kojim,
koristeći razne metode i tehnološka rješenja,
rizik informacijske sigurnosti svodimo na minimum.**