INFORMATION
MANAGEMENT
&TECHNOLOGY

Rizici i kontrole informativne tehnologije u oblasti finansijskih sistema

Radionica ZP Trezora PEM-PAL-a 2011

Kristin Lado Tufan

THE WORLD BANK GROUP

Uvod

- Službenik zadužen za IT rizike i usaglašenost u Informacionom menadžemntu i tehnologijama (IMT) Svetske banke; CISA, CRISC Sertifikati
- Upravljao poslovima interne kontrole Banke koje se odnose na Finansijsko izveštavanje (ICFR) IT opštih kontrola, od 2007. godine do danas
- U vremenskom periodu od 2000 – 2005. godine, savetovao Development Gateway stipendiste u Mongoliji, Sri Lanki i Istočnim Karibima (sa Rumunijom) u vezi sa web-zasnovanim poslovnim planovima i njihovom primenom, kao oblika podrške ministarstvima i donatorima
- Svetska banka se dobrovoljno usklađuje sa ICFR (slično sa US Sarbanes-Oxley), kao oblikom dobre prakse
- Primenjene aplikacije Banke uključuju SAP, PeopleSoft, i veliki broj trezorskih aplikacija
- Usaglašenost sa ICFR nije samo jednokratni događaj, već je to način vršenja poslovnih oparacija

Dnevni red

- Ukupno okruženje interne kontrole koje pruža razumno uveravanje, a koje se odnosi na sveobuhvatnost, tačnost i integritet Vašeg FMIS-a radi finansijskog izveštavanja
- Okviri koji pomažu u implementaciji procesa i kontrola
- Specifične operativne i kontrole infromativne bezbednosti za svaki sloj Vašeg FMIS-a
- Primer Svetske banke Sigurnog Web Portala

- “Poverenje nije kontrola”
- “Uradite ono šta dokumentujete, i dokumentujte ono šta uradite”

Kontekst Banke…

- **SAP**: Globalni ERP sa 24.000 korisnika; više od 12 velikih aplikacija, uključujući standardne module kao što su AP/AR i unutar-kuće razvijene aplikacije za distribuciju zajmova i putovanja; približno 8,6 miliona transakcija mesečno
- **PeopleSoft**: Globalni ERP sa približno 18.500 dinamičnih uloga/korisnika i 1.033 statičkih uloga; ukupno 3.756 dodeljenih transakcija; Podržava sektore ljudskih resursa, obračuna zarada, penzione procese
- Banka poseduje unutar-kuće razvijen **siguran website (Client Connection)** koji nudi vladinim zvaničnicima i agencijama koje primenjuju projekte da postignu brži pristup informacijama o svojim portfolijima i o radu Banke koji se odnosi na analitičku procenu zemlje
- Banka takođe ima veliki broj **trezorskih aplikacija** kao oblika podrške trezorskih operacija
- **Remote Access**: Banka ima nekoliko opcija za Remote Access, od kojih su svi omogućeni preko dvofaktorske autentifikacije
- Trenutno, ukupno **148 ključnih kontrola** su testirane svake godine preko svih finansijskih sistema u okviru potrebe Interne kontrole preko finansijskog izveštavanja (ICFR)

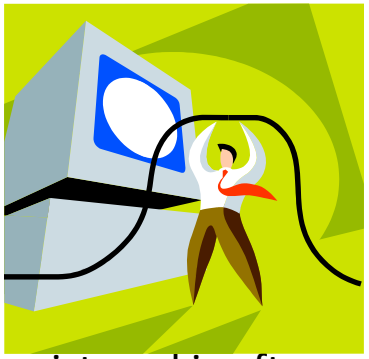
Neki rizici informativne tehnologije koji se odnose na finansijske sisteme

- **Neovlašćeni pristup:** Korisnički/Programerski pristup nije bio odobren za određeni nivo pristupa ili aktivnosti; Primer: Osiguravanje privilegovanog pristupa je odgovarajuće ograničen.
- **Prekomeran pristup:** Korisnički/Programerski nivo pristupa prevazilazi njihov opis posla, i sa njim u vezi odgovornosti; Primer: Osiguravanje uspostavljanja Principa najmanje privilegije – ljudi imaju samo onoliko pristupa potrebnim informacijama i transakcijama koliko je potrebno da bi izvršavali svoj posao i sa njim u vezi obimom odgovornosti
- **Neovlašćene izmene:** Programska izmena nije odobrena pre nego što se krenulo u produkciju; Primer:
- **Prevara** je jedan potencijalan rezultat ovih rizika ukoliko su aktivnosti namerne
- **Manjak kontrole** vezan za nabavku i primenu novih aplikacija i održavanja postojećih aplikacija
- **Manjak kontrole** vezan za nabavku, instalaciju, konfiguraciju, integraciju i održavanje IT infrastrukture.

Okruženje interne kontrole

- **Kontrole na nivou entiteta**
  - Istonirano na vrhu i kultura organizacije
  - Menadžment osigurava da su uspostavljenje mere politika i procedura, kao i da su svi zaposleni svesni istih, kao i da se istih i pridržavaju
- **Kontrole aplikacija**
  - Razvijanje i održavanje aplikacija
  - Pristup programima i podacima/informacijama

  Bezbednosne kontrole (primenjuju se na sve nivoe)
- **Opšte kontrole informativne tehnologije**
  - Menadžement infrastrukturnih promena: Baza podataka, sistemski softver, mreža
  - Operacije informativnih sistema: Procesuiranje grupnih (batch) poslova, backup i povraćaj informacija



Ljudi, proces, tehnologija

Korisni okviri kao osnova za okruženje interne kontrole

- **COSO/COSO ERM** (Komitet sponzorskih organizacijaTreadway komisije): Integrisani okvir internih kontrola, fokusiran na Kontrolu okruženja, Procenu rizika, Kontrolne aktivnosti, Informacije & komunikaciju, i na Monitoring
- **COBIT** (ISACA): Kontrolni ciljevi informativne tehnologije koji se fokusiraju na četiri ključne domenske oblasti: Plan i oraganizaciju, Nabavku i implementaciju, Isporuku i podršku, i Monitoring i evaluaciju
- **ITIL** (Infrastrukturna biblioteka informativne tehnologije) Okvir za IT Servisno menadžerske prakse, kao što su Menadžment promena, Menadžemnt incidenata, Menadžemnt problema, Menadžemnt konfiguracija, Menadžment servisnih nivoa
- **CMMi** (Softverski inženjerski institut): Capability Maturity Model integracija za životni ciklus razvoja softvera
- **ISO20000**: Okvir i sertifikacija za IT Servisni menadžment
- **ISO27001**: Okvir i sertifikacija za informacionu bezbednost
- **RiskIT** (ISACA): Poslovni rizik u vezi sa IT , fokusiran na Evaluaciju rizika, Upravljanje rizikom, i Monirotingom/izveštavanjem o riziku

Razvoj i održavanje aplikacija

- **Ključni rizici:** Neovlašćen pristup/izmene, Prekomenran pristup, Prevara; Neefikasne kontrole u procesu
- Proces **dokumentacije** i identifikacija ključnih kontrola; podrška uz alatku radnih tokova
- **Segregacija dužnosti** (za poslove i IT)
  - Separacija između okruženja razvoja i proizvodnje;, na primer, Programeri ne bi trebali imati ažuriran pristup proizvodnom okruženju
  - Sve izmene u proizvodnoj aplikaciji trebaju biti dokumentovane i odobrene; osoba koja inicira promenu treba biti različita od osobe koja odobrava istu promenu, kao i različita od osobe koja uvodi tu istu promenu u proizvodnju
- **Pristup**
  - Korisnički pristup: Zasnovano na ulogama i odgovornostima određenim datim poslom
  - Privilegovani pristup: Jasna autorizacija, snažna autentifikacija;
  - Pravilo najmanje privilegije – pristup koji je potreban kako bi neko odradio svoj posao

Infrastrukturni menadžment promena

- **Ključni rizici**: Neovlašćen pristup/izmene, Prekomeran pristup, Prevara
- Mere politike **dokumentacije** menadžemnta promena, procesa i kontrola; podrška uz alatku radnih tokova
- Korišćenje rizično-baziranog pristupa promenama: Hitnost za velike promene; varirajući nivoi dokumentacije i odobrenja koji su zahtevani
- **Segregacija dužnosti**: osoba koja inicira promenu treba biti različita od osobe koja odobrava istu promenu, kao i različita od osobe koja uvodi tu istu promenu u proizvodnju
- Osiguravanje da su uloge i odgovornosti jasne, a koje se odnose na to ko može inicirati promenu, testirati promenu, odobriti je, i uvesti u proizvodnju
- Osiguravanje da su svi dokazi o promenama dokumentovani, da su one odobrene, i čuvane radi kasnijeg lakog korišćenja

Informacione sigurnosne kontrole: Pristup

- **Autentifikacija i autorizacija**: Kako se postiže pristup, i ko ga odobrava – novi korisnik i transfer
- **Privilegovani pristup:** Sistemski administratori
  - Osiguravaju da su ukinuta prava pristupa za zaposlene na vreme primenjena
  - Individualni napurot servisnih pristupa – mogućnost praćenja
- **Sigurnost i integritet podataka** – Osiguravanje transfera podataka; enkriptovanje podataka pri prenosu (Secure Socket Layer/SSL i Secured Hypertext Transmission Protocol/HTTPS)



- **Mrežni i Web aplikacioni Firewalls**: Review Logs, ograničeni pristup
- **Lozinke za sve vrste korisnika**: Složene, traže izmenu, zaključavanje računa
- **Fizička bezbednost** u Vašem Centru podataka – ko ima pristup čemu; da li je pristup periodično ponovo odobravan i razmatran?

Operacije informacionih sistema / Planiranje za nepredviđene okolnosti

- **Ključni rizici**: Pad sistema, gubitak podataka; neefikasne kontrole u procesima
- **(Minimalni nivo)** procesa backup-a i povraćaja **dokumenata**
  - Nedostaci monitoringa i preuzimanje akcija
  - Izvršavanje periodičnih testova povraćaja kako bi se osigurala dostupnost podataka sa trake/diska
  - Sigurno, na drugom mestu, skladištenje
- Razvijanje mera politike koje se odnose na IT povraćaj podataka nakon incidenta; testiranje IT plana za nepredviđene okolnosti
- Dokumentovanje procesa koji se odnose na Batch poslove
  - Ko ima pristup *run*-u?
  - Poznavati opseg, uticaj i frekvenciju poslova
  - Preuzeti aktivnosti vezane za neuspešne poslove

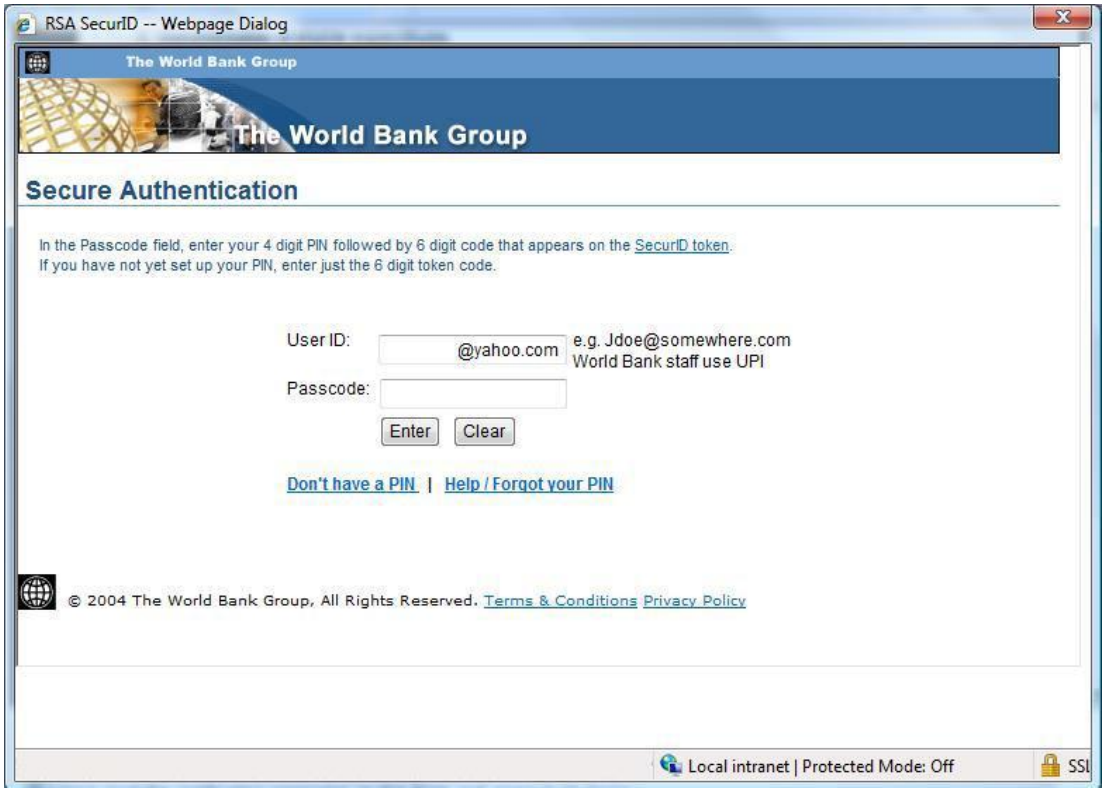
Primer Svetske banke: Client Connection

- Client Connection je osiguran web-based portal koji omogućava Davaocima/Primaocima, kao i Donatorima, pristup informacijama koje se odnose na zajmove, kredite, grantove i trust fondove
- Straight Through Processing (STP) je novija faza projekta eDisbursement – klijenti Banke mogu da podnesu online zahtev za isplatu sredstva, kao i da podnesu elektronski potpis na isti
- Autorizovani potpisnici i korisnici moraju biti odobreni, kao i što moraju biti unapred registrovani
- Odvojeni profili, kao što je Form Creator i Form Signatory, moraju biti uspostavljeni
- Različiti profili imaju različite nivoe pristupa, ili različite vrste transakcija koje oni mogu izvršavati
- Pristup je zagarantovan sa važećim korisničkim imenom i lozinkom, koja uključuje pin i dinamični token

http://clientconnection.worldbank.org

Korišćenje dvofaktorske autentifikacije…

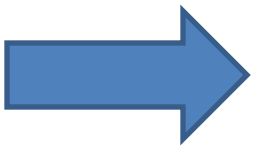
- Korisničko ime
- Osmocifreni PIN
- Dinamična šestocifrena token šifra



eForm Primer

STP je pružen, Potpis se čeka…

Potpisivanje formulara...



B. Payment instructions

6a. Application currency	6b. Application amount	6c. Equivalent payment currency (if different from application currency)
United States Dollars	5,750,125.79	

6d. Application amount (in words)
United States Dollars FIVE MILLION SEVEN HUNDRED FIFTY THOUSAND ONE HUNDRED TWENTY-FIVE And 79

7. If the application covers more than one loan (as specified in item 2 above), please provide amounts allocated to each financier.

Loan/Financing/Grant No.(s)	Amount	Loan/Financing/Grant No.(s)	Amount
Loan/Financing/Grant No.(s)	Amount	Loan/Financing/Grant No.(s)	Amount

8. Name and address of beneficiary	9. Amount to be paid in installments?	
NATL HIVAIDS CONTROL PROJ III 1234 ANYWHERE IN NEW DELHI	No (if yes, complete "Requested Schedule for Advance Payments" Form 2381)	
10a. Name and address of the beneficiary's bank	10b. Account number (or IBAN for euro payments) of the beneficiary at the beneficiary's bank	10c. SWIFT code of the beneficiary's bank
BANK OF BARODA MADHUBAN: NEW DELHI	CHARITO ACC 123	BARBINBBNND
11a. Name and address of the intermediary bank	11b. Account number (or IBAN for euro payments) of the beneficiary's bank at the intermediary bank	11c. SWIFT code of the intermediary bank
FEDERAL RESERVE BANK OF NEW YORK FLOOR 7: NEW YORK		FRNYUS33XXX
12. Special payment instructions(if any)		

The supporting documentation contains 1 electronic document(s).

1 more signature(s) still needed(to access the eSignatories tab, click here)

☑ I have read the certification appearing on this form and agree to its terms.

Sign **Reject** **Cancel**

Supporting Documents

Documentation Type/Name	Size	Attached By
Statement of Expenditure STP Statement of Expenditures.xls	16KB	STP Create User3 26-OCT-2010 06:02 PM EST

Metode za preventivne i detektivne kontrole

- Segregacija dužnosti: Operativni i privilegovani pristup
- Dvofaktorska i Višefaktorska autentifikacija
- Periodični pregled uloga i prisupa na svim nivoima, od pristupa mreži do pristupa aplikaciji
  - Izvršavati najmanje jednom u šest meseci; dokumnetovati pregled i preuzete aktivnosti
- Monitoring kontinuiranih kontrola – automatizovan i manuelni
  - Praćenje pristupa sistemima - Ponavljani neuspešni zahtevi za logovanjem i za neovlašćenim pristupom
  - Praćenje promena iz izvora (aplikacija/baza podataka/operativni sistem), i poređenje sa promenama koje su zabeležene u ticketing sistemima
  - Praćenje firewall aktivnosti
- Enkriptovani podaci u tranzitu
- Uzeti u razmatranje firewall aplikacije

Benefiti revizije

- Revizije mogu dati osnovano uveravanje da je pripremanje finansijskih izveštaja podržano adekvatnim i održivim praćenjem principa interne kontrole
- Revizori mogu otkriti nedostatke u procesiranju informacionih sistema koji kada se ponovo obrade, mogu ojačati kontrolno okruženje i integritet sistema
- Gledajte na reviziju kao na mogućnost za poboljšanje procesa i kontrola, racionalizaciju kontrola, i kao na osiguranje da će se operacije vršiti bez ometanja na jedan efektivan i efikasan način
- Gledajte na revizore

kao na strateške partnere!

Pitanja i komentari ?