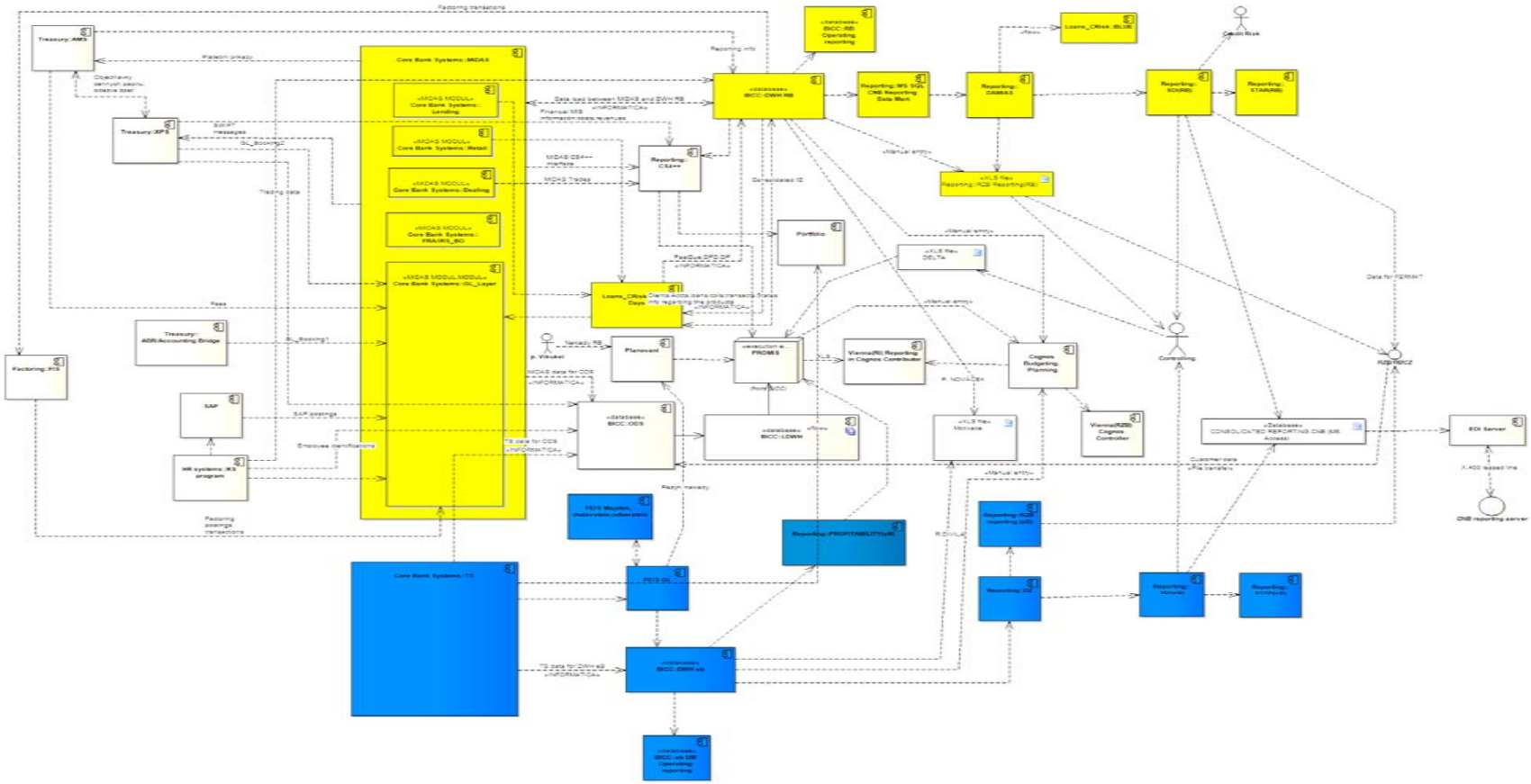
IT Arhitektura – Globalno

Belma Ohranović
IT Auditor

System Landscape

- **Landscape view**



Šta možemo revidirati?

Pitanja?

Šta možemo provjeriti za system landscape?

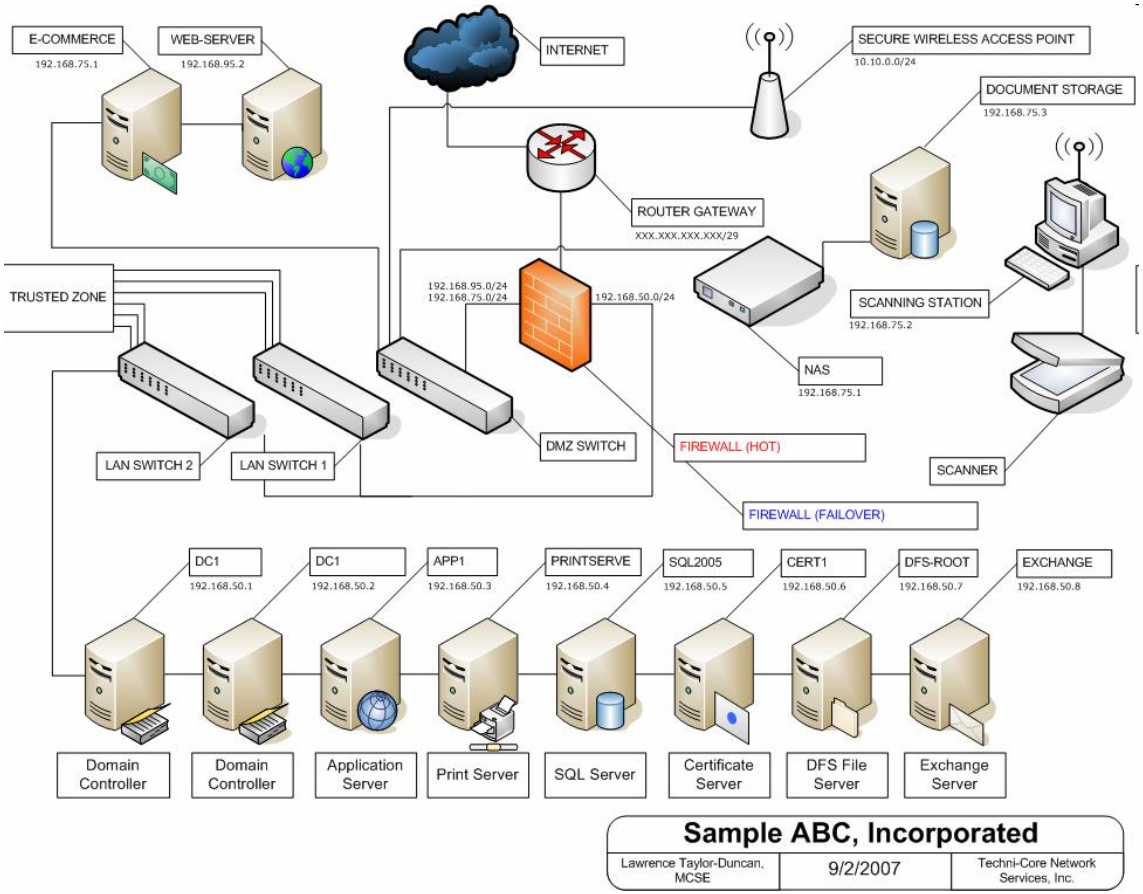
Koje zahtjeve možemo pokriti?

Šta možemo revidirati?

- Strategiju i planiranje
- Usaglašenost sa standardima
- Konzistentnost standarda(systems / technologies / interfaces)
- Dokumentaciju za system landscape
- Kompleksnost system landscape
- Funkcionalne redundancije
- Redundancije storeage-a podataka
- Komunikaciju između komponenti
- Troškovnu opravdanost (Održavanje sistema)

Infrastruktura

- Infrastructure view



Šta možemo revidirati?

Pitanja?

Šta možemo provjeriti za infrastrukturu sistema?

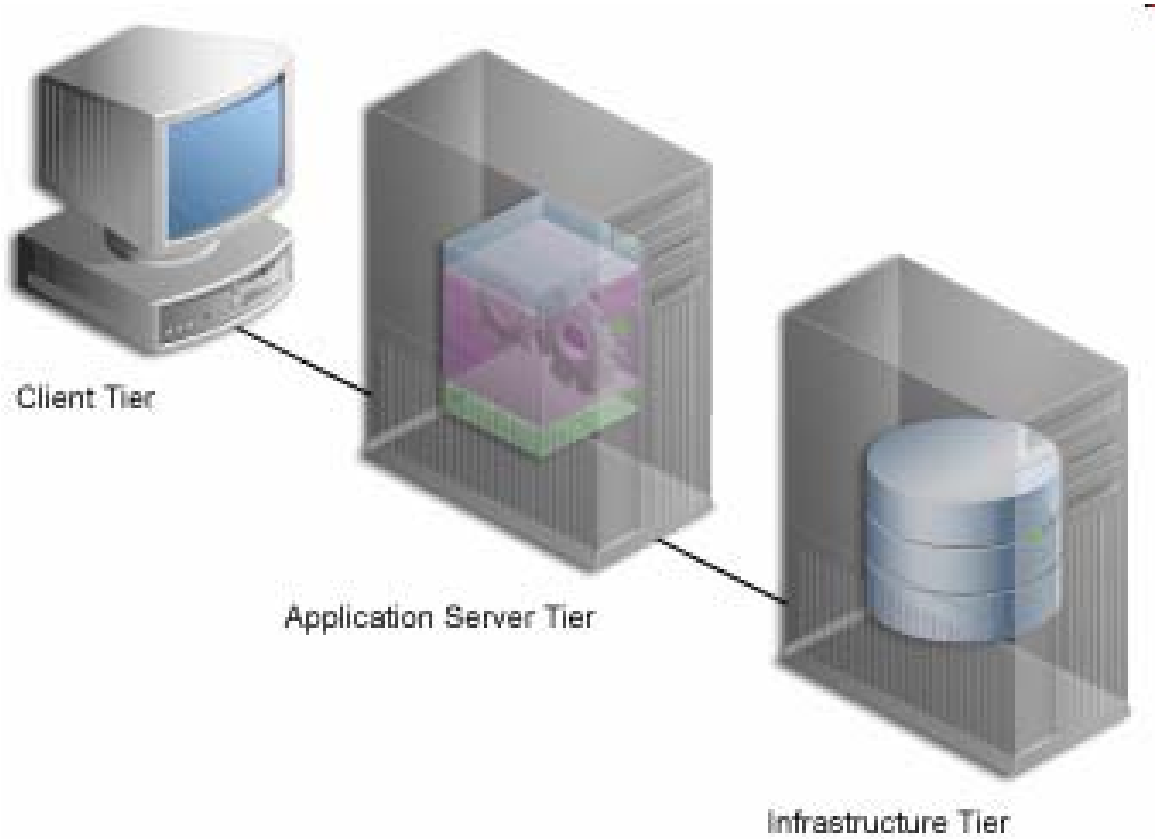
Koje zahtjeve možemo pokriti?

Šta možemo revidirati?

- Hardware / veličinu mreže
  - Kapacitet (peak times, load balancing)
- Redundancije HW, network
- Efikasnost HW
  - Troškovi HW
  - Homogene sisteme?
- Sigurnost mreže
  - VLANs, DMZ
- Data storage / Mirroring

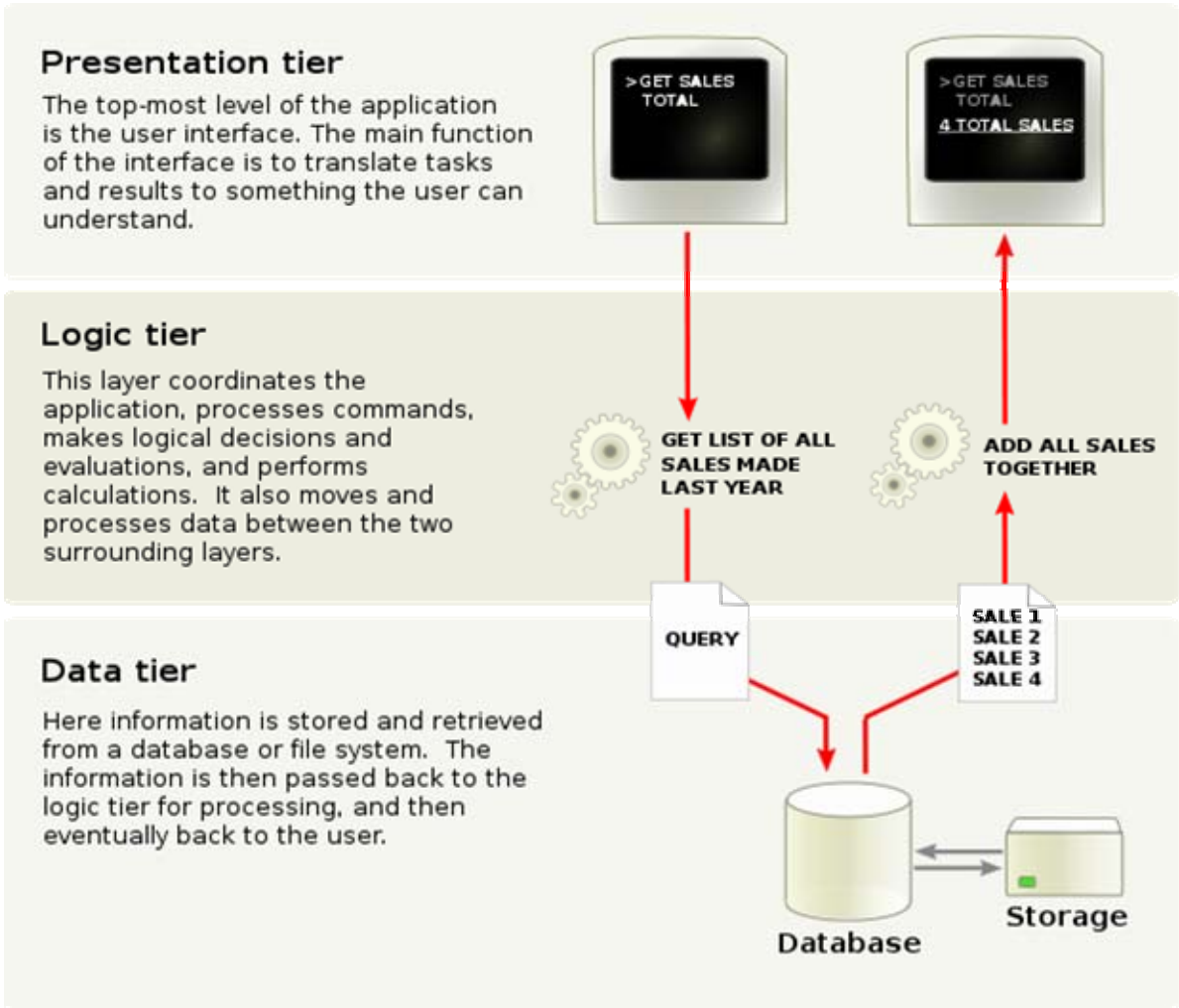
Aplikativna arhitektura

Application Level



System Architecture

3-tier Architecture



System Architecture

- Presentation Layer
  - Fat clients
  - Thin clients
  - Web frontend…
- Application Layer
  - Contains business logic
- Database Layer
- Integration Layer

System Architecture

Principi

- Business logic mora da bude unutar aplikacijskog nivoa
  - (ne u Frontend-u ni u Database layer-u)
- Logika kontrole pristupa bi trebala da bude u aplikativnom layer-uAccess control logic should be in application layer
  - (ne u Frontend-u ni u Database layer-u)
- Podaci bi trebali da budu u database layer-uData storage should be in database layer

System Architecture

Pitanja?

Da li su sistemi u Vašoj organizaciji postavljeni u skladu sa ovim principima?

System Architecture

Izuzeci:

- Uglavnom vezani za pitanja konekcije
- Privremeni storage podataka klijenata
  - npr. FX rates
- Biznis logika u front end-u (validacijske kontrole)

System Architecture

Problemi sa raznolikom arhitekturom

- Održavanje distribuirane biznis logike
  - Update svih klijenata
- Upgrad-i jedne komponente imaju uticaj na druge
  - npr. ukoliko je logika ugrađena u database
- Nekonzistentnost podataka
  - Provođenje provjera podataka koji nisu tekući

System Architecture

Implikacije revizije:

- Dodatne kontrole moraju biti postavljene
  - Provjera verzija za klijente
  - Provjera verzija za podatke (npr. FX rates, blacklists)
  - Sigurnosne implikacije (falsifikovanje vlastitih klijenata?)

Fokus revizije na sistemskim komponentama

Audit Focus

Šta provjeriti na Front End-u?

- Funkcionalnost (npr. ulazne kontrole)
- Sigurnost
  - Web sigurnost
  - Upotreba enkripcije (SSL, certificates)
  - Da li se java cashe briše nakon isteka sesije?
- Updates
- Upotreba sistema
  - Zadovoljstvo korisnika?

Audit Focus

Šta provjeriti na Application Layer?

- funkcionalnost (kontrole procesiranja)
- Sigurnost
  - Zaštita aplikativnih datoteka
- Usaglašenost sa standardima arhitekture
- Usaglašenost sa standardima razvoja
- Job scheduling (EDO)
- Dokumentacija
- Svi procesi koji podržavaju aplikacije

Audit Focus

Šta provjeriri za operativne sisteme?

- Sigurnost
  - Jačinu sistema
  - Mehnizmi autentifikacije
  - Prava pristupa (sistemskim datotekama, apliaktivnim datotekama, database datotekama)
  - Patch nivoi
  - Instalirani Software
  - Razvojni alati
  - Alati za direktni pristup database
- Usaglašenost sa standardima arhitekture

Audit Focus

Šta provjeriti za Database?

- Sigurnost
  - Prava pristupa (direktni pristup database)
  - Standardni korisnici (poznati passwordi)
  - Patch Nivoi
  - Backup
  - Enkripcija
- Usaglašenost sa standardima arhitekture

Audit Focus

Šta provjeriti za interfejse?

- Kako interfejsi funkcioniraju?
- Sigurnost
  - Prava pristupa (privremenim datotekama)
  - Enkripcija file-ova
  - Upotreba nesigurnih protokola (ftp)
- Frekvencija interface polling
- Kako se odigurava integritet
  - Checksums, data validation checks, Rollback
- Upotreba standardnih formata interfejsa
- Upravljanje greškama