Interne Kontrole
Belma Ohranović
IT Auditor

Interne Kontrole

Revizija bazirana na kontrolama vs. Neovisna revizija

- Revizija bazirana na kontrolama (također se naziva i revizija usaglašenosti)
- Koja je razlika?
  - Termin poznat više u finansijskoj revizije (kontrole vs. računi)
  - Termin također validan u IT reviziji
  - Neovisno testiranje je pouzdanije
  - Primjeri:
    - Code review
    - User access rights
    - Data Quality

Interne Kontrole

Kada koristiti neovisno testiranje

- Ukoliko su otkrivene kontrolne slabosti
- Ukoliko se kontrolne efikanosti ne mogu dokazati
- U slučaju visokog rizika: postojeće kontrole nisu dovoljne
- Za validaciju kontrola generalno
  - Slabosti neovisnog testiranja uvijek impliciraju kotnrolne slabosti

Interne Kontole

Šta je kontrola?

Kontrola se definira kao poštivanje specifičnog seta politika, procedura i aktivnosti kako bi se dostigli željeni **ciljevi.**

Kontrola može biti uspostavljena kao određena funkcija ili aktivnost u procesu.

Uticaj kontrole moze biti opsežan ili specifičan za stanje računa, klasu transakcije ili aplikaciju.

Kontrole imaju jedinstvena obilježja-npr. mogu biti: automatizovane ili manuelne; usaglašavanje; razdvajanje dužnosti; pregled ili odobravanje; zaštita informacija; spriječavanje i detekcija grešaka i zloupotrebe.

Kontrole unuttar procesa se mogu sastojati od kontrola finansijskog izvještavanja i operativnih kontrola (koje su dizajnirane da dostignu operativne ciljeve). controls (that is, those designed to achieve operational objectives).

Interne Kontrole

Opis kontrola

Control Description	**Proces**	Ime procesa
	Broj kontrole	Jedinstveni broj kontrole (proces.podproces.i tako redom)
	Kontrolni Cilj	Kratki opis kontrolnog cilja. Zašto se postavlja kontrola i koji se rizik smanjuje.
	Opis kontrole	Kratki i precizni opis kontrole koja se treba usmjeriti na relevantnu kontrolnu akciju.
	Odgovornost	Ko je odgovoran za uspostavljanje kontrole

Interne Kontrole

Kontrolni atributi

Kontrolni atributi	**Tip (P/D)**	**Tip kontrole može biti preventivni(P) i detektivni(D). Preventivne kontrole sprečavaju nastajanje grešaka dok se detektivne kontole koriste za pronalazak i ispravku grešaka koje su nastale.**
	Mehanizam (A/M/B)	**Da li se kontrola provodi:** • **manuelno (M),** • **automatski (A) ili** • **oboje (B).**
	Frekventnost	**Kako se često obavlja kontrola.frekventnost kontrole se koristi za definisanje veličine ispitivanje u fazi testiranja. Moguće vrijednosti za ove atribute su: Više puta dnevno (250+), Dnevno (250), Sermično (50) Mjesečno (12), Kvartalno (4), Godišnje (1), Po nalazu (N/A), Stalno (N/A).**

Interne Kontole

Upotreba okvira i standarda:

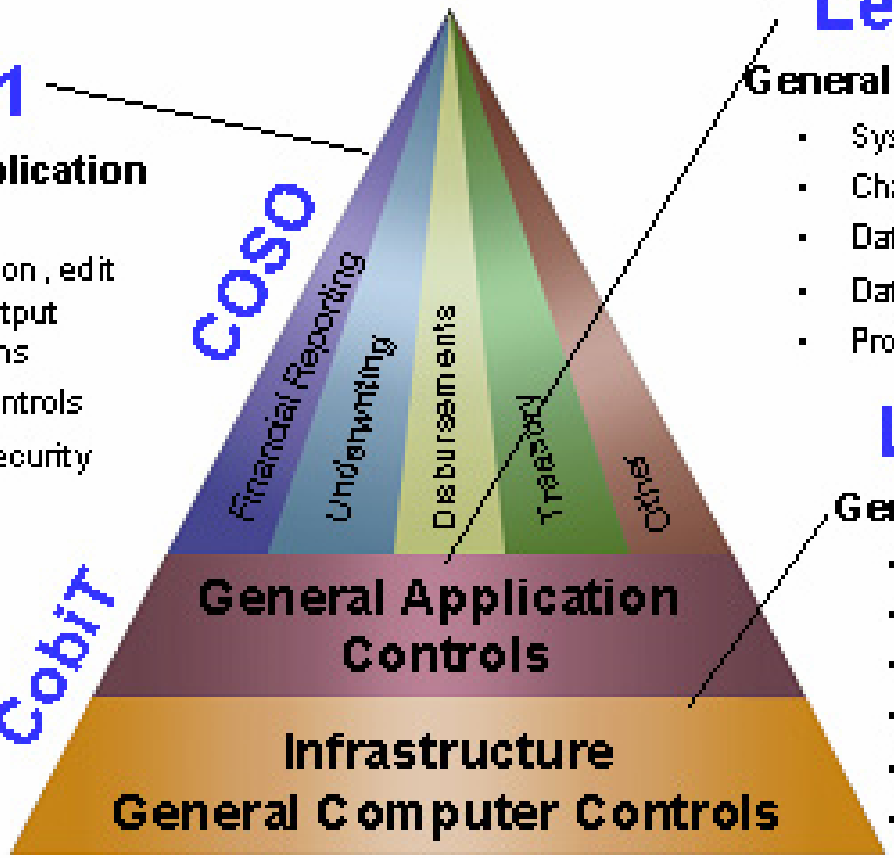
Kako bi osigurali ostvarenje ciljeva, kontrole moraju biti u skladu sa

→ COSO, CobiT, ITIL

Interne kontrole mogu biti podjeljene u dvije kategorije:

- Generalne IT kontrole
- Kontole na aplikativnom nivou

Interne Kontole



Level 1

Automated Application Controls

- Data validation, edit checks & output reconciliations
- Interface Controls
- End User Security

Level 2

General Application Controls

- System development
- Change control
- Data Recovery
- Database management
- Programmer security

Level 3

General Computer Controls

- Change and configuration management
- Network Administration
- Security Administration
- Data center operations
- Database Administration
- Disaster Recovery
- O/S Administration

Interne Kontole

Generalne IT kontrole

- Kontrole koje su validne za sve sisteme
- Generalne kontrole nemaju direktni uticaj na transakcije
- Kontole ugrađene u IT proces
  - Razvoj
  - Change Management
  - Operacije
  - Incident Management
  - IT Security

→ Dobro uspostavljene generalne kontrole su preduslov za edektivne kontole na aplikativnom nivou

Interne Kontrole

Kontrole aplikativnog nivoa

- Mogu biti direktno povezane sa procesiranjem transakcija u sistemu
- Specifične su samo za jednu aplikaciju/sistem
- Kontrole su ugnježdene u poslovni proces upotrebom aplikacija
  - Unos podataka
  - Verifikacija / Odobrenje
  - Procesiranje
  - Izlaz

Interne Kontrole

Kontrole aplikativnog nivoa:

Kriterij podataka nije direktno primjenjiv za slijedeće ciljeve

Efektivnost, Efikasnost, Pouzdanost, Integritet, Dostupnost, Pouzdanost

→ U tu svrhu se koristi različit set :

Kao direktni link procesiranim transakcijama ukoliko je moguće, tvrdnje se koriste za obezbjeđivanje ispravnog procesiranja.

Interne Kontole

Tvrdnje: SAMO for Transakcioni nivo kotnrola

Tvrdnje	**Potpunost (Completeness)**	**Potpunost osigurava da su sve transakcije procesirane.**
	Tačnost (Accuracy)	**Tačnost osigurva da su transakcije procesirane u korektnoj formi (npr.kalkulacije se izvršavaju korektno)**
	Validnost / Pridržavanje (Validity / Compliance)	**Validnost transakcija osigurava da je izrada, modifikacija i izdanje odobreno i autorozovano. Ovo takođe osiguravna usaglašenost za regulatornim zahtjevima.**
	Pravovremenost (Timeliness)	**Pravovremenost osigurava provođenje transakcija u skladu sa vremenskim okvirom.)**
	Ograničen pristup (Restricted access)	**Ograničen pristup osigurava da samo autorizovane osobe mogu ostvariti pristup procesiranju informacija (kreiranje, modifikacija, čitanje).**

Interne Kontole

Pitanja?

Da li možete popuniti atribute koji nedostaju na primjerima kontrola?

Interne Kontole

Control Nr.	Control Objective	Control Description	Responsible	Control Attributes	Assertions				
					C	A	V	T	R
x.1	Invoices are not uploaded more than once.	The system prohibits double uploads of invoices by checking invoice nr., supplier, date and amount with processed records.		Preventive Automatic Continuous	X				

Internal Controls

Control Nr.	Control Objective	Control Description	Responsible	Control Attributes	Assertions				
					C	A	V	T	R
x.2	All necessary fields in the records are filled.	All customer related fields are mandatory and have to be filled. This is enforced by the system further processing is not possible.		Preventive Automatic Continuous		X			

Internal Controls

Control Nr.	Control Objective	Control Description	Responsible	Control Attributes	Assertions				
					C	A	V	T	R
x.3	All payments are authorized.	All payments are authorized according to an approval matrix. The authorization is documented by signatures on printouts. Once a week XYZ is checking if all approvals were made accordingly.		Detective Manual Weekly			X		

Internal Controls

Control Nr.	Control Objective	Control Description	Responsible	Control Attributes	Assertions				
					C	A	V	T	R
x.4	The system is kept to current patch level.	Recommended patches are installed as soon as possible after they are released by the vendor. Tests are performed prior to installation.		General IT Control					

Internal Controls

Control Nr.	Control Objective	Control Description	Responsible	Control Attributes	Assertions				
					C	A	V	T	R
x.5	Employee's accounts are protected.	Accounts of employees are marked with a special flag. Additional permissions are necessary to access these accounts. All accesses (incl. read) to these accounts are logged.		Preventive Automatic Continuous					X