IT Audit

19.-20. travnja/aprila
Virtualno
osposobljavanje

Komitas Stepanyan
Dr.sc., CRISC, CRMA, CobitF

REVIZIJA IT-A

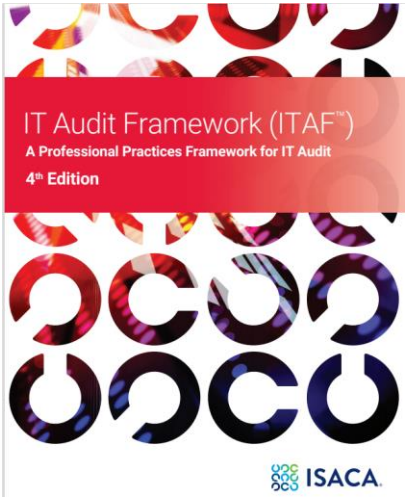
Sadržaj

- ✓ Unutarnja revizija i revizija IT-a
- ✓ Standardi, okviri i najbolje prakse revizije IT-a
- ✓ Odgovornosti, ciljevi i potrebne vještine za provođenje revizija IT-a
- ✓ Primjeri

ONO ŠTO IMAMO

The Institute of Internal Auditors

ISACA



Izjave o standardima revizije i uvjerenja IT-a

Opći standardi

1001 Povelja o reviziji

1001.1 Funkcija revizije i uvjerenja IT-a prikladno dokumentira funkciju revizije u povelji o reviziji, navodeći **svrhu**, **odgovornosti**, **ovlasti** i **dužnosti**

1004 Opravdana očekivanja

1004.1 Praktičari revizije i uvjerenja IT-a imaju opravdana očekivanja da angažman može biti izvršen u skladu s primjenjivim standardima revizije i uvjerenja IT-a te, po potrebi, drugim standardima industrije ili primjenjivim zakonima i propisima koji će dovesti do stručnog mišljenja ili zaključka.

Izjave o standardima revizije i uvjerenja IT-a

Opći standardi

1006 Stručnost

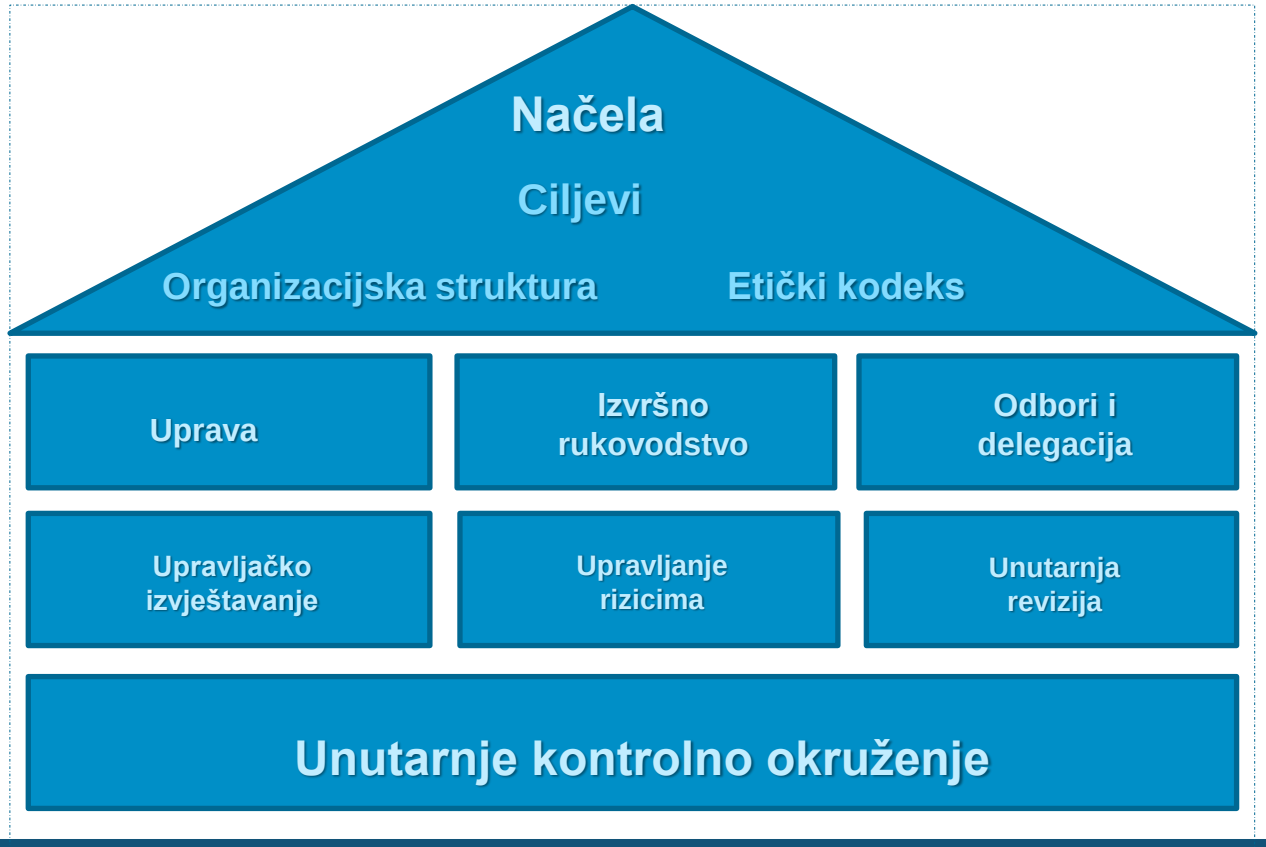
1006.1 Praktičari revizije i uvjerenja IT-a, zajedno s drugima koji pomažu u pogledu angažmana s revizijom i izražavanjem uvjerenja, imaju stručne kompetencije za obavljanje potrebnog rada.

1006.2 Praktičari revizije i uvjerenja IT-a imaju primjerenu razinu znanja o tom području za ispunjavanje svojih uloga u angažmanu s revizijom i izražavanjem uvjerenja.

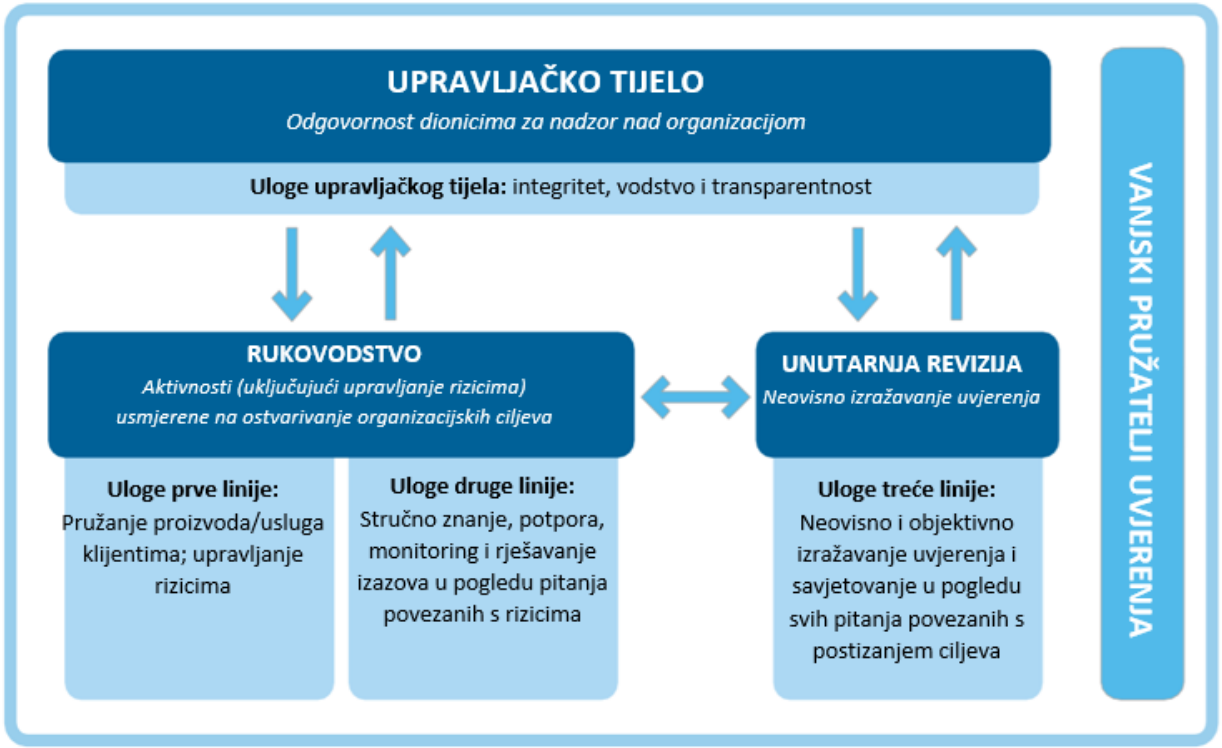
1008 Kriteriji

1008.1 Praktičari revizije i uvjerenja IT-a odabiru kriterije prema kojima će se predmet procjenjivati, a ti su kriteriji objektivni, potpuni, relevantni, pouzdani, mjerljivi, razumljivi, nadaleko poznati, mjerodavni te su razumljivi ili dostupni svim čitateljima i korisnicima izvještaja.

ONO ŠTO IMAMO



Model triju linija

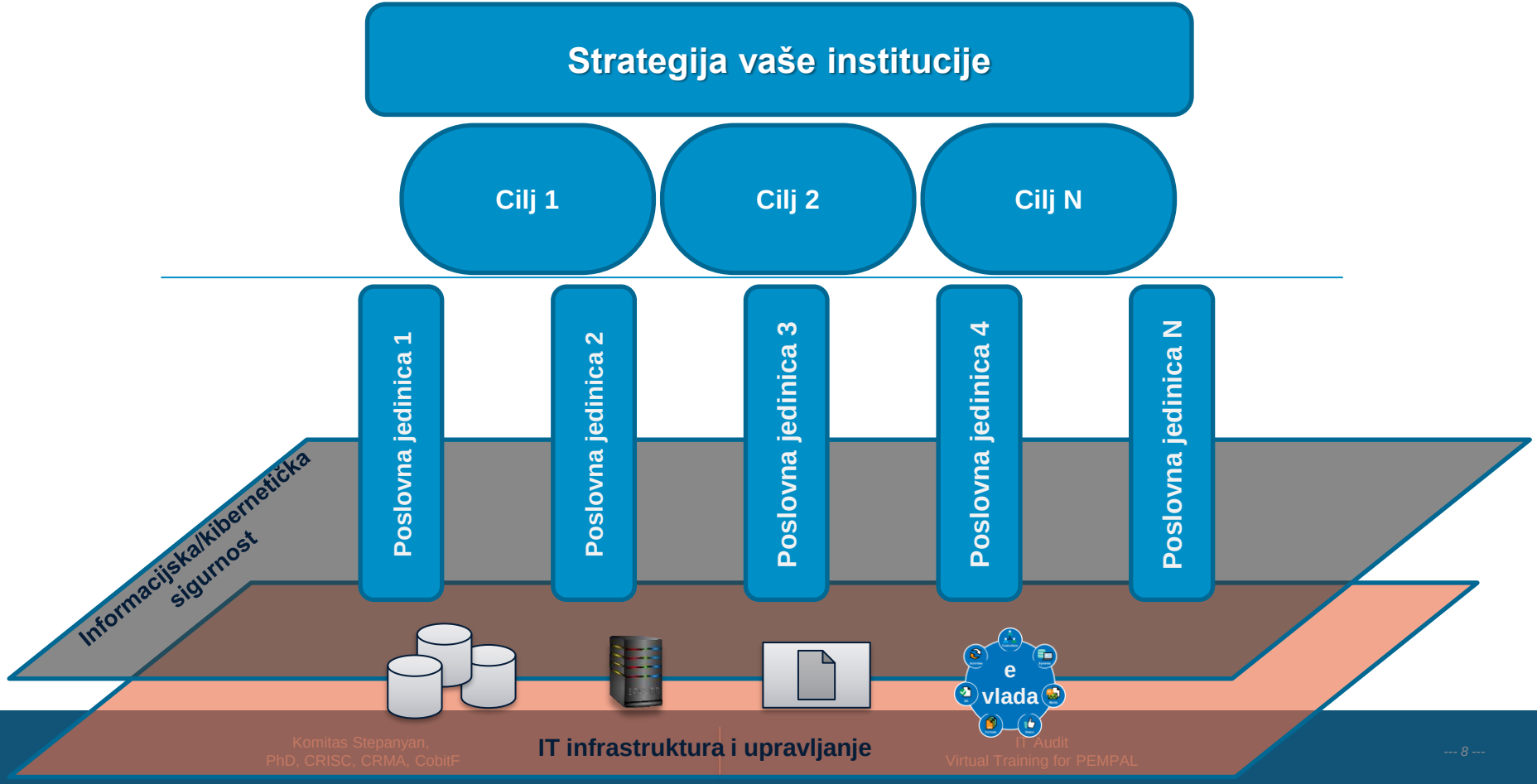


Odgovornost, izvještavanje

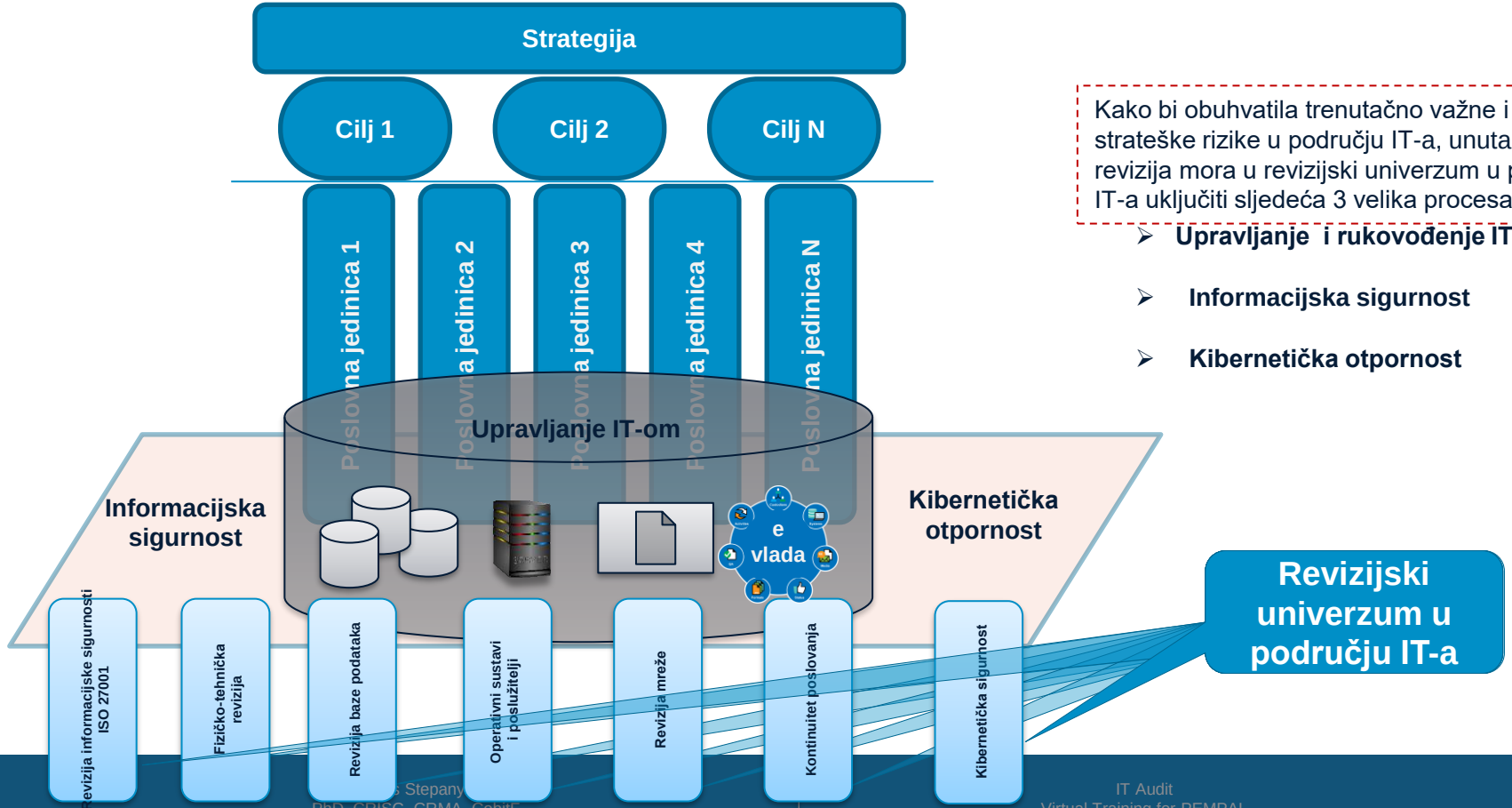
Delegacija, smjer, sredstva, nadzor

Usklađivanje, koordinacija komunikacije, suradnja

Pristup revizije IT-a i revizijski univerzum u području IT-a



Pristup revizije IT-a i revizijski univerzum u području IT-a



Kako bi obuhvatila trenutačno važne i strateške rizike u području IT-a, unutarnja revizija mora u revizijski univerzum u području IT-a uključiti sljedeća 3 velika procesa

- **Upravljanje i rukovođenje IT-om**
- **Informacijska sigurnost**
- **Kibernetička otpornost**

Vještine potrebne za provođenje revizija IT-a

Revizija ITGC-a

Kontrole ITGC-a primijenjene na sve aktivnosti IT usluge

- ✓ Upravljanje pristupom
- ✓ Upravljanje promjenama
- ✓ Upravljanje sigurnosnom kopijom
- ✓ Upravljanje incidentima

Svi unutarnji revizori

Detaljnija revizija IT-a

- ✓ Revizija mreže
- ✓ Revizija sustava za upravljanje bazom podataka (DBMS)
- ✓ Revizija alata Active Directory
- ✓ Revizija virtualizacije
- ✓ Revizija kibernetičke sigurnosti

Revizori za IT

Primjer, šest glavnih kontrola koje su često dio revizije ITGC-a

1. kontrola: Fizička sigurnost i sigurnost okoliša

- ✓ Prostorija s poslužiteljem zaključana je sustavom pristupa karticom.
- ✓ Ograničeni broj zaposlenika ima pristup prostoriji s poslužiteljem putem kartice.
- ✓ Podatkovni centar ima povišene podove i detektore za vodu ispod podova.
- ✓ Alarm sustava grijanja, ventilacije i hlađenja šalje e-poruke i pokreće zvučne signale ako dođe do pogreške sustava.
- ✓ Vatrogasni aparati u prostoriji s poslužiteljem provjeravaju se kvartalno.

Primjer, šest glavnih kontrola koje su često dio revizije ITGC-a

2. kontrola: Logička sigurnost

- ✓ Novim zaposlenicima omogućuje se pristup sredstvima sustava nakon što ih odobri odjel za ljudske resurse.
- ✓ Vjerodajnice za pristup zaposlenika s kojima je raskinut radni odnos brišu se u roku od 15 minuta od obavještavanja odjela za ljudske resurse.
- ✓ Za provjeru autentičnosti korisnika koji zatraže sredstva sustava upotrebljava se Windows Active Directory.

Primjer, šest glavnih kontrola koje su često dio revizije ITGC-a

3. kontrola: Upravljanje promjenama

- ✓ Okruženje za ispitivanje i produkcijsko okruženje odvojeni su jedno od drugoga.
- ✓ Produkcijske promjene i sigurnosne zakrpe se ispituju, dokumentiraju i odobravaju prije početka uporabe.

Primjer, šest glavnih kontrola koje su često dio revizije ITGC-a

4. kontrola: Sigurnosna kopija i oporavak

- ✓ Podaci se svakodnevno sigurnosno kopiraju prema dokumentiranom procesu i rasporedu.
- ✓ Postoje planovi za oporavak u slučaju katastrofe za kritične sustave te se oni ispituju svake godine.

Primjer, šest glavnih kontrola koje su često dio revizije ITGC-a

5. kontrola: Upravljanje incidentima

- ✓ Svakodnevno se izrađuju izvještaji o aktivnostima koje pregledava IT rukovodstvo.
- ✓ Proces odgovora na incidente dokumentira se i redovno upotrebljava prilikom odgovaranja na abnormalne situacije.

Primjer, šest glavnih kontrola koje su često dio revizije ITGC-a

6. kontrola: Informacijska sigurnost

- ✓ Za zaštitu dosega mreže od sumnjivih aktivnosti upotrebljavaju se vatrozidi.
- ✓ Za sprječavanje štete od virusa upotrebljava se antivirusni softver.
- ✓ 24/7 provodi se monitoring ulaznog i izlaznog podatkovnog prometa kako bi se prepoznali mogući napadi krađe identiteta, distribuirani napadi uskraćivanjem resursa i drugi pokušaji prodiranja u doseg mreže.
- ✓ Dvaput godišnje provode se penetracijski testovi kojima se provjerava postoje li slabe točke.

Provođenje revizije ITGC-a

Tijekom provođenja revizije ITGC-a ispitajte svaku kontrolu koristeći se kombinacijom sljedećih tehnika:

1. Intervjui sa zaposlenicima *(i njihovim rukovoditeljima)* koji su za njih odgovorni
2. Pregled dokumentacije *(kao što su pisani postupci, politike i tehnički priručnici)*
3. Osobna zapažanja *(primjerice promatranje kako pojedinac obavlja zadatke povezane s kontrolom)*


How?
Where?
When?
Why?
Which?
What?
Who?
Why?