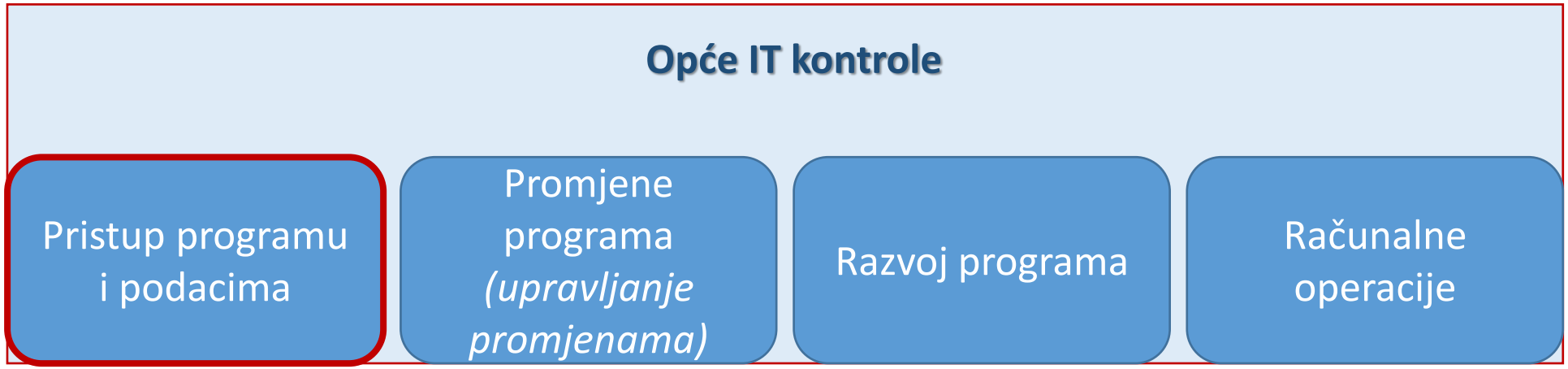
Opće
kontrole informacijske tehnologije *(ITGC-i)*

PRIMJER

PREGLED OPĆIH IT KONTROLA – PROCES REVIZIJE

- ❑ Razumjeti i utvrditi IT okruženje i sustave koje je potrebno pregledati
- ❑ Provesti intervjue, dati pojašnjenja i pregledati dokumentaciju kako bi se bolje razumjeli procesi
- ❑ Razumjeti i utvrditi IT okruženje i sustave koje je potrebno pregledati
- ❑ Ocijeniti primjerenost postojećeg kontrolnog okruženja (dizajn kontrole)
- ❑ Potvrditi postojeće kontrole kako bi se ocijenila operativna učinkovitost kontrola

PREGLED OPĆIH IT KONTROLA – PRISTUP PROGRAMIMA I PODACIMA



Ciljevi:

Pristup programu i podacima pravilno je ograničen samo na ovlaštene osobe

Rizik:

Neovlašteni pristup programu i podacima može dovesti do neprimjerenih izmjena podataka ili uništenja podataka.

PREGLED OPĆIH IT KONTROLA – PRISTUP PROGRAMIMA I PODACIMA

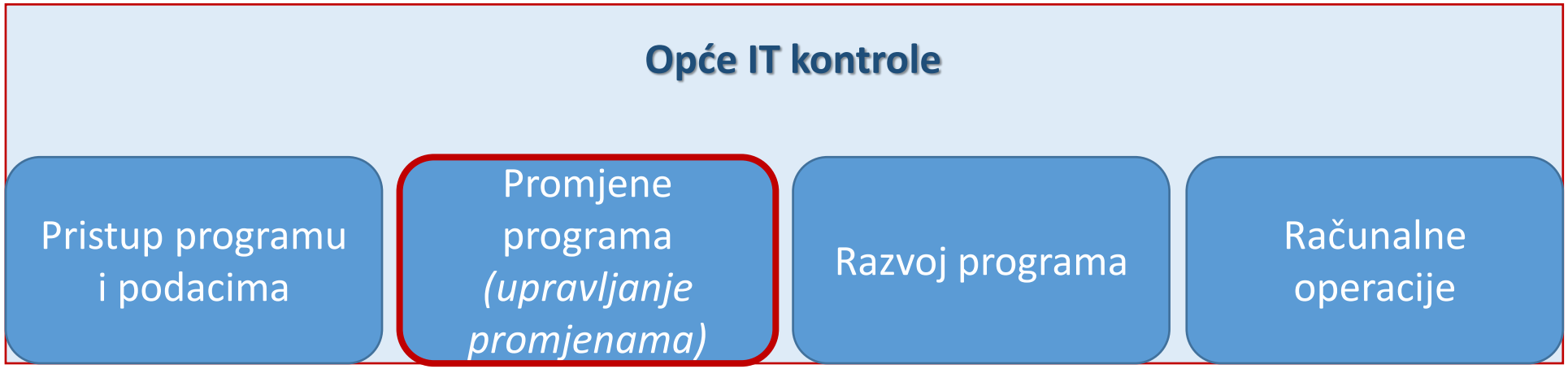
Komponente pristupa programima i podacima koje treba uzeti u obzir:

- Politike i postupci
- Dodjela privilegija za korisnički pristup i onemogućavanje korisničkog pristupa
- Periodični pregledi dozvole za pristup
- Zahtjevi za lozinku
- Upravljanje privilegiranim korisničkim računima
- Fizički pristup
- Primjerenost pristupa/raspodjele dužnosti
- Autentifikacija sustava
- Zapisnik revizija

PREGLED OPĆIH IT KONTROLA – PRISTUP PROGRAMIMA I PODACIMA, PRIMJER

Područje	Dizajn postojeće kontrole	Kako ispitati/potvrditi
Dodjela privilegija za korisnički pristup	U primjeni je formalan proces odobravanja ili mijenjanja pristupa sustavu (na temelju odgovarajuće razine odobrenja).	Pregled dokaza o odobrenju
Onemogućavanje korisničkog pristupa	U primjeni je formalan proces onemogućavanja pristupa korisnicima koji su preneseni ili odvojeni.	Usporediti postojeće korisničke račune s popisom korisnika koji su
Periodični pregledi dozvole za pristup	Provode se periodični pregledi dozvole za pristup korisnika, administratora i dobavljača trećih strana.	Pregled dokaza o periodičnim pregledima
Zahtjevi za lozinku	Upotrebljavaju se jedinstvene (pojedincu) i snažne lozinke.	Procijeniti jesu li provedena pravila za lozinku
Privilegirani korisnički računi	Računi koji imaju privilegirana prava na pristup sustavu (npr. poslužitelji, baze podataka, aplikacije i infrastruktura) dostupni su samo ovlaštenom osoblju.	Pregledati račune s privilegiranim pravima na pristup
Fizički pristup	Pristup zaštićenim područjima i računalnoj opremi dopušten je samo ovlaštenom osoblju.	Vodič kroz područja (npr. podatkovni centar, pohrana sigurnosnih kopija, itd.)

PREGLED OPĆIH IT KONTROLA – PROMJENE PROGRAMA



Ciljevi:

Sve promjene u postojećim sustavima pravilno su ovlaštene, ispitane, potvrđene, provedene i dokumentirane.

Rizik:

Neprimjerene promjene u sustavima ili programima mogu dovesti to netočnih podataka

PREGLED OPĆIH IT KONTROLA – PROMJENE PROGRAMA

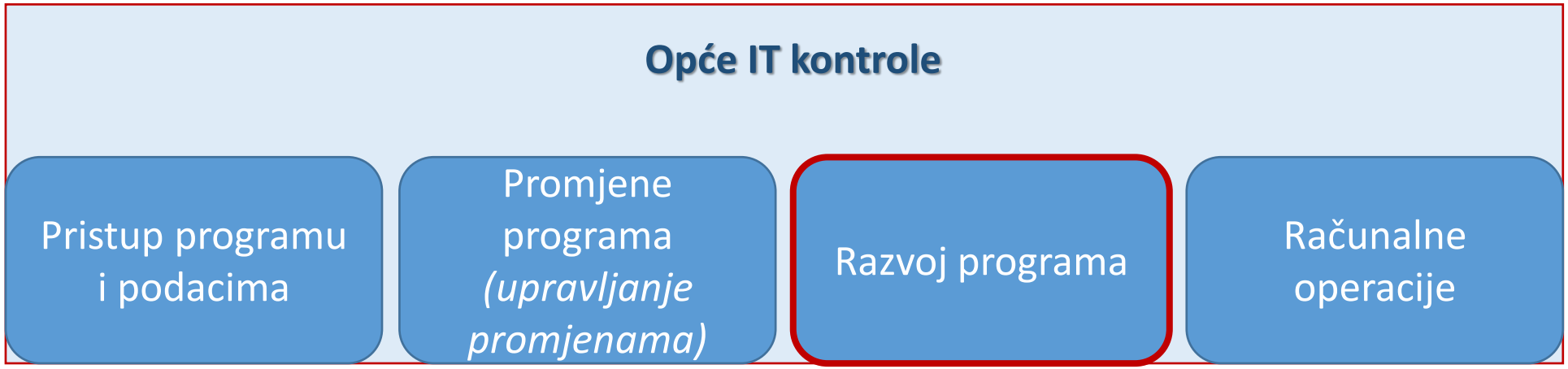
Komponente promjene programa i razvoja koje treba uzeti u obzir:

- Postupci upravljanja promjenama i metodologija razvoja sustava
- Autorizacija, razvoj, provedba, ispitivanje, odobrenje i dokumentacija
- Migracija u produkcijsko okruženje (odvajanje dužnosti)
- Konfiguracijske promjene
- Hitne promjene
- Migracija podataka i kontrole verzije
- Ispitivanje i pregledi nakon promjene/provedbe

PREGLED OPĆIH IT KONTROLA – PROMJENE PROGRAMA, PRIMJER

Područje	Dizajn postojeće kontrole	Kako ispitati/potvrditi
Kontrole upravljanja promjenama	U primjeni je formalni proces za ispravno upravljanje promjenama.	Pregledati/ocijeniti postupke upravljanja promjenama i potvrditi pridržavanje postupaka
Dokumentacija o promjenama	Sve promjene na *sustavima (npr. poslužitelji, baze podataka, aplikacije, skupni poslovi i infrastruktura)* dokumentiraju se i prate.	Pregledati zapisnike o promjenama
Ispitivanje	Provodi se odgovarajuća razina ispitivanja.	Pregledati dokaz o planovima i rezultatima ispitivanja
Odobrenje	Potrebno je odgovarajuće odobrenje prije migracije u produkciju.	Pregled dokaza o odobrenju
Migracija	Pristup za migraciju promjena u produkciju ograničen je na odgovarajući način.	Provjeriti postoji li odvajanje dužnosti između razvojnih inženjera i operatora (= koji unosi izmjene)

PREGLED OPĆIH IT KONTROLA – RAZVOJ PROGRAMA



Ciljevi:

Novi sustavi/aplikacije koji se razvijaju ili provode pravilno su ovlašteni, ispitani, potvrđeni, provedeni i dokumentirani

Rizik:

Neprimjeren razvoj ili provedba sustava ili programa mogu dovesti do netočnih podataka, financijskih gubitaka, itd.

PREGLED OPĆIH IT KONTROLA – RAZVOJ PROGRAMA

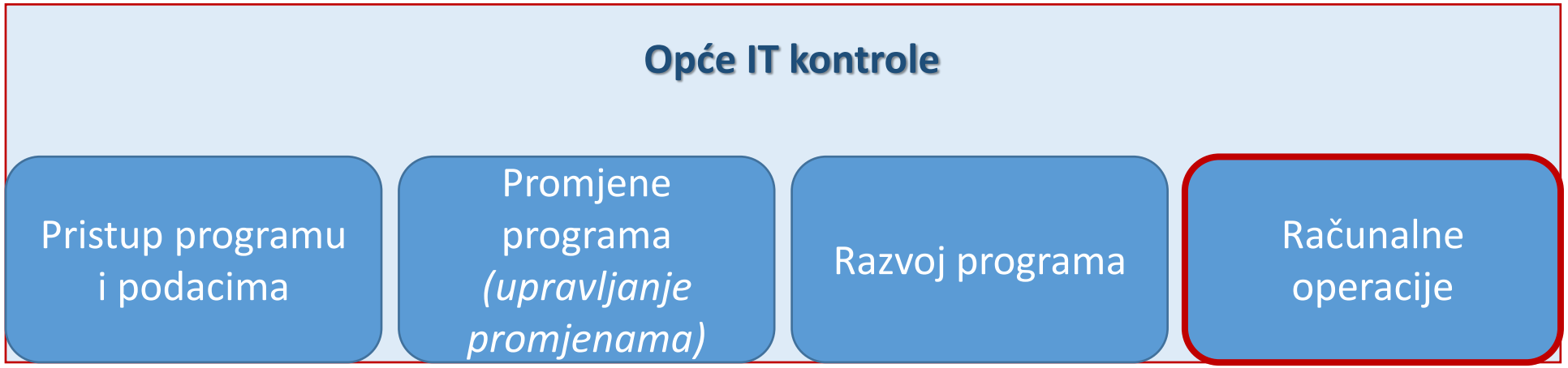
Komponente razvoja programa koje treba uzeti u obzir:

- Korisnički zahtjevi, TOR
- Dizajn
- Izgradnja/kodiranje
- Ispitivanje
- Provedba
- Evaluacija
- Održavanje

PREGLED OPĆIH IT KONTROLA – ŽIVOTNI CIKLUS RAZVOJA SUSTAVA, PRIMJER

Područje	Dizajn postojeće kontrole	Kako ispitati/potvrditi
Korisnički zahtjevi	Postoji dokumentirani postupak za odobrenje korisničkih zahtjeva	Pregledati i osigurati da postoje dokumentirani i odobreni korisnički zahtjevi
Dizajn i kodiranje	????	????
Ispitivanje	????	????
Provedba	????	????
Evaluacija i prihvaćanje	????	????
Održavanje	????	????

PREGLED OPĆIH IT KONTROLA – RAČUNALNE OPERACIJE



Ciljevi:

Sustavi i programi su dostupni i obrađuju pravilno

Rizik:

Sustavi ili programi možda nisu dostupni korisnicima ili ne obrađuju pravilno

PREGLED OPĆIH IT KONTROLA – RAČUNALNE OPERACIJE

Komponente računalnih operacija koje treba uzeti u obzir:

- Obrada skupnih poslova
- Monitoring poslova (uspjeh/neuspjeh)
- Postupci izrade sigurnosne kopije i oporavka
- Rješavanje incidenata i upravljanje problemima
- Promjene u rasporedu skupnih poslova
- Kontrole okoliša
- Plan oporavka u slučaju katastrofe i Plan kontinuiteta poslovanja
- Upravljanje sigurnosnim zakrpama

PREGLED OPĆIH IT KONTROLA – RAČUNALNE OPERACIJE, PRIMJER

Područje	Dizajn postojeće kontrole	Kako ispitati/potvrditi
Obrada skupnih poslova	Skupni poslovi odgovarajuće su zakazani, obrađeni, s odgovarajućim monitoringom i praćenjem	Pregledati/ocijeniti postupke za obradu i monitoring skupnih poslova i potvrditi pridržavanje postupaka
Monitoring poslova	Neuspjeli poslovi naknadno se prate i dokumentiraju (uključujući uspješna rješenja i objašnjenja)	Potvrditi da se neuspjeli poslovi naknadno prate i dokumentiraju
Sigurnosna kopija i oporavak	Sigurnosne kopije za ključne podatke i programe dostupne su u slučaju izvanredne situacije.	Pregledati/ocijeniti postupke za sigurnosnu kopiju i oporavak te potvrditi pridržavanje postupaka
Upravljanje problemima/poteškoćama	U primjeni je formalni proces za rješavanje problema/poteškoća kako bi osigurao pravovremenu identifikaciju, eskalaciju, rješavanje i dokumentaciju problema.	Pregledati/ocijeniti postupke za upravljanje problemima/poteškoćama te potvrditi pridržavanje postupaka

OSIGURANJE KVALITETE


Thank You