- Unutarnje kontrolno okruženje
- Rizici i procjena rizika u području IT-a
- Revizijski univerzum u području IT-a: što je potrebno revidirati?
- Godišnji plan
- Primjeri

Više od 60 % organizacija doživi velik neuspjeh pri kontroliranju sigurnosti i integriteta svojih računalnih sustava

- Informacije su dostupne nikad većem broju radnika.
- Informacije na distribuiranim računalnim mrežama teško je kontrolirati.
- Klijenti i dobavljači imaju pristup sustavima i podacima druge strane.
- Neka društva smatraju gubitak ključnih informacija dalekom i ne posebno izglednom prijetnjom.
- Implikacije prelaska s centraliziranih računalnih sustava na internetske sustave u pogledu kontrole nisu u potpunosti jasne.
- Mnoga društva nisu svjesna činjenice da su informacije strateški resurs i da njihova zaštita mora postati strateški uvjet.
- Produktivnost i troškovni pritisci potiču rukovodstvo da odustane od mjera kontrole koje oduzimaju vrijeme.

PREGLED KONCEPATA UNUTARNJE KONTROLE

Unutarnja kontrola – proces koji se provodi kako bi se u razumnoj mjeri pružilo uvjerenje da su ostvareni sljedeći ciljevi u pogledu kontrole

Zaštita imovine	Održavanje evidencije	Pružanje informacija	Unaprjeđenje efikasnosti	Poticanje politika	Usklađenost s propisima
Sprječavanje ili otkrivanje neovlaštenog stjecanja, upotrebe ili raspolaganja	Dovoljno pojedinosti da bi se o imovini društva moglo izvještavati precizno i pravedno	Precizne i pouzdane	Promicanje i unaprjeđenje operativne efikasnosti	Poticanje poštovanja propisanih politika	Sukladnost s važećim zakonima i propisima

Unutarnja kontrola sastavni je dio aktivnosti upravljanja

VRSTE UNUTARNJIH KONTROLA *(VAŽNE FUNKCIJE)*

Preventivne kontrole

Sprječavanje problema prije nego što se pojave

Primjer:

- ✓ zapošljavanje kvalificiranog osoblja, odvajanje dužnosti zaposlenika,
- ✓ kontrola fizičkog pristupa imovini i informacijama

Detektivne kontrole

Otkrivanje problema koji nisu spriječeni

Primjer:

Dvostruka provjera izračuna te priprema bankovnog poravnanja i mjesečnih bruto bilanci

Korektivne kontrole

Ispravljanje problema te ispravljanje i oporavak od pogrešaka koje uslijede.

Primjer:

održavanje sigurnosnih kopija datoteka, ispravljanje pogrešno unesenih podataka

Opće kontrole

osiguravanje stabilnosti kontrolnog okruženja i dobrog upravljanja njime

Primjer: IT infrastruktura i kontrole kupnje, razvoja i održavanja softvera

Aplikacijske kontrole

sprječavanje, otkrivanje i ispravljanje transakcijskih pogrešaka i prijevare u aplikacijskim programima

kontrole procesa **ulazni podaci – obrada – izlazni podaci**

Primjer: autorizacija ulaznih podataka, provjera valjanosti podataka, postupci uređivanja

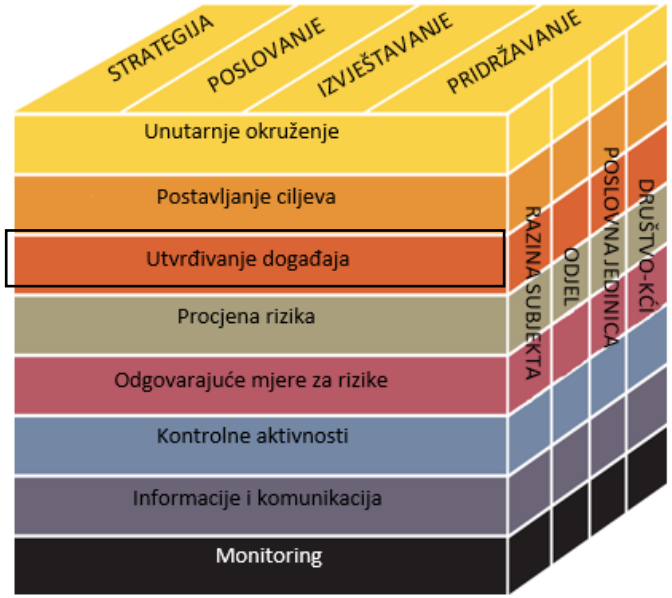
ŠTO JE TO RIZIK?

COSO definira **događaj** kao „**incident** ili pojavu koji nastaju **iz unutarnjih ili vanjskih izvora**, a koji **utječu na provedbu strategije ili ostvarenje ciljeva**.

Događaju mogu imati pozitivan ili negativan utjecaj, ili i jedno i drugo."

Prilika

RIZIK



Rukovodstvo mora pokušati **predvidjeti sve moguće pozitivne** ili **negativne** događaje, **utvrditi koji su od njih najvjerojatniji i najmanje vjerojatni** te **razumjeti odnose između događaja**.

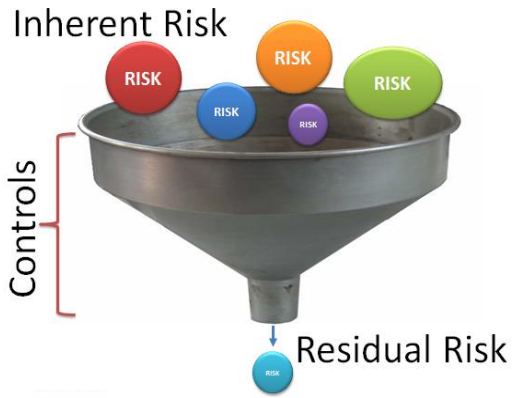
Primjer – zamislimo provedbu sustava elektroničke razmjene podataka (EDI) koji stvara elektroničke dokumente, prenosi ih klijentima i dobavljačima te prima povratne odgovore u elektroničkom obliku.

Neki događaji s kojima bi se društvo moglo suočiti su: odabir neprikladne tehnologije, neovlašteni pristup, gubitak integriteta podataka, nedovršene transakcije, kvar sustava i nekompatibilni sustavi.

PROCJENA RIZIKA I ODGOVOR NA RIZIK

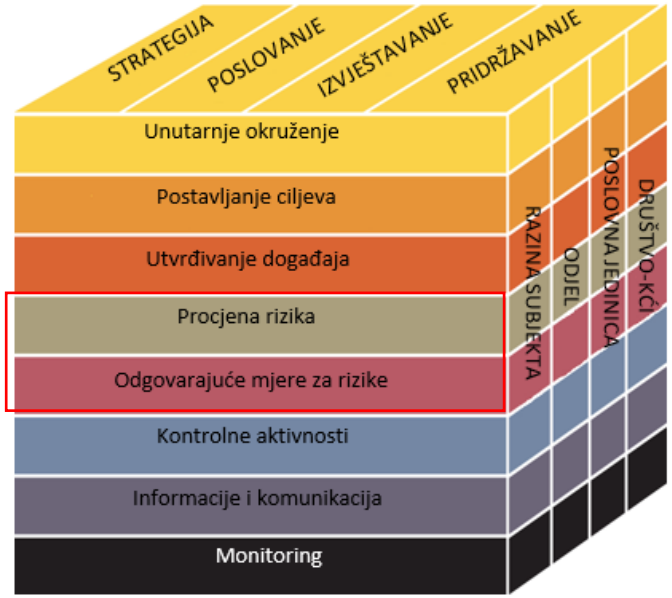
Inherentni rizik

COSO definira inherentni rizik kao:
rizik za subjekt koji nastaje zbog izostanka **bilo kakvih mjera** rukovodstva kojima bi se promijenila **vjerojatnost** ili **utjecaj** rizika.



Rezidualni rizik

Rezidualni rizik je rizik koji preostaje nakon što je rukovodstvo poduzelo odgovarajuće mjere za rizike.

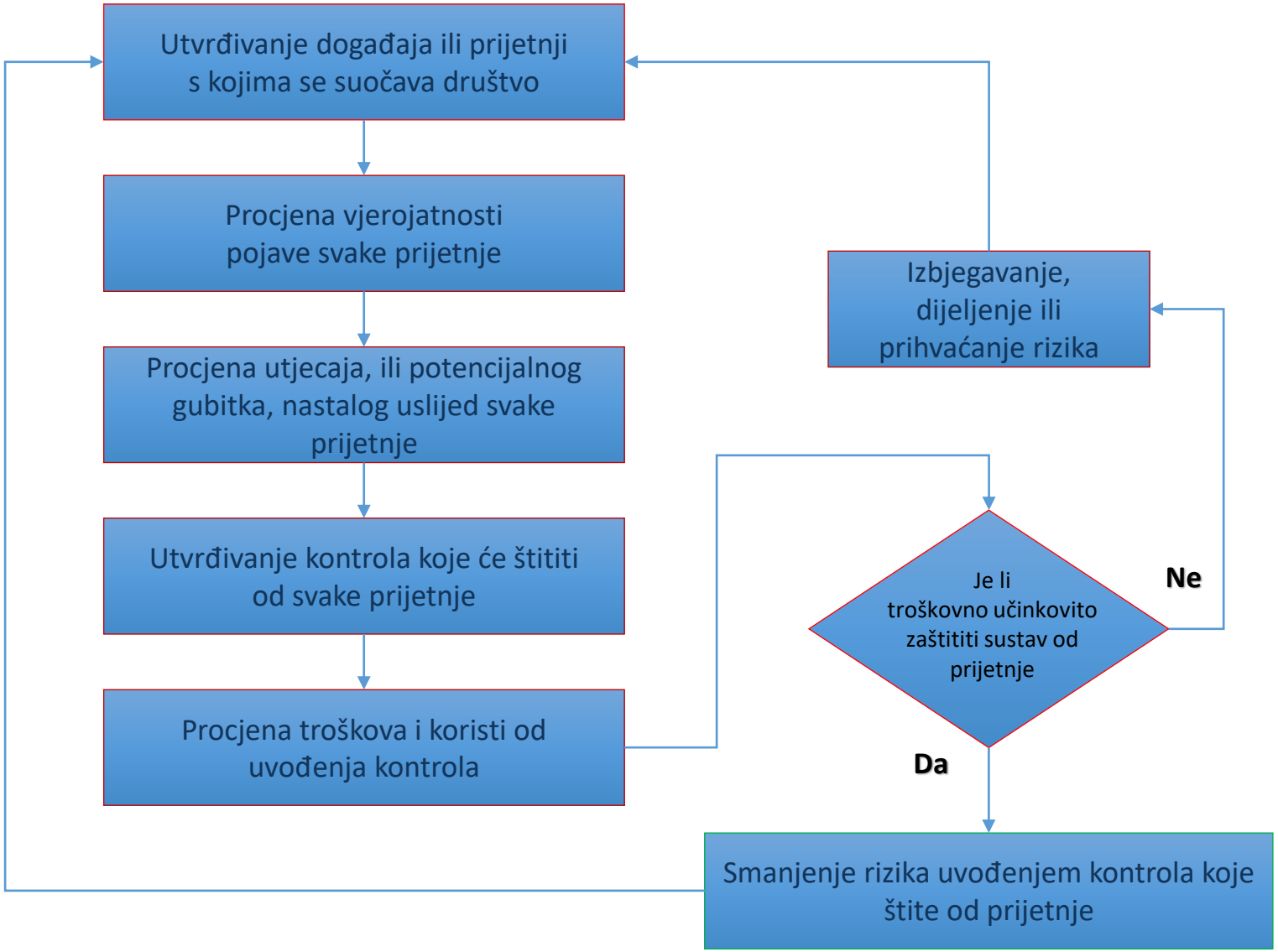


Kako bi se utvrđeni rizici uskladili s tolerancijom društva prema riziku, rukovodstvo mora rizik sagledati na razini cjelokupnog društva. Mora procijeniti vjerojatnost i utjecaj rizika, kao i troškove i koristi alternativnih odgovora na njega.

- **Umanjiti**
- **Prihvatiti**
- **Podijeliti**
- **Izbjeći**

OD PROCJENE RIZIKA DO DIZAJNIRANJA UNUTARNJIH KONTROLA

Rukovodstvo bi trebalo dizajnirati učinkovite sustave unutarnje kontrole kako bi smanjilo inherentni rizik.
Unutarnjom revizijom *(revizijom IT-a)* potrebno je evaluirati sustave unutarnje kontrole kako bi se utvrdilo funkcioniraju li učinkovito.



UTVRĐIVANJE KONTROLA I ANALIZA TROŠKOVA I KORISTI

Rukovodstvo bi trebalo utvrditi kontrole kojima se društvo štiti od svakog događaja

- **Preventivne kontrole**
- **Detektivne kontrole**
- **Korektivne kontrole**

Cilj dizajniranja sustava unutarnje kontrole jest pružanje razumnog uvjerenja da neće doći do događaja

Unutarnje kontrole

Uvođenje previše kontrola preskupo je i negativno utječe na operativnu učinkovitost

Uvođenjem premalo kontrola neće se postići potrebno razumno uvjerenje

Koristi postupka unutarnje kontrole moraju biti veće od troškova takvog postupka!

Kako se mjere koristi?

Kako se mjere troškovi?

Očekivani gubitak = **Vjerojatnost** X **Utjecaj**

Rizik = **Vjerojatnost** X **Utjecaj**

Rizik = prijetnja x ranjivost

Dva je slučaja potrebno imati na umu:

Ako je bilo koji od čimbenika nula, čak i ako su ostali čimbenici visoki ili na kritičnoj razini, rizik će biti nula.

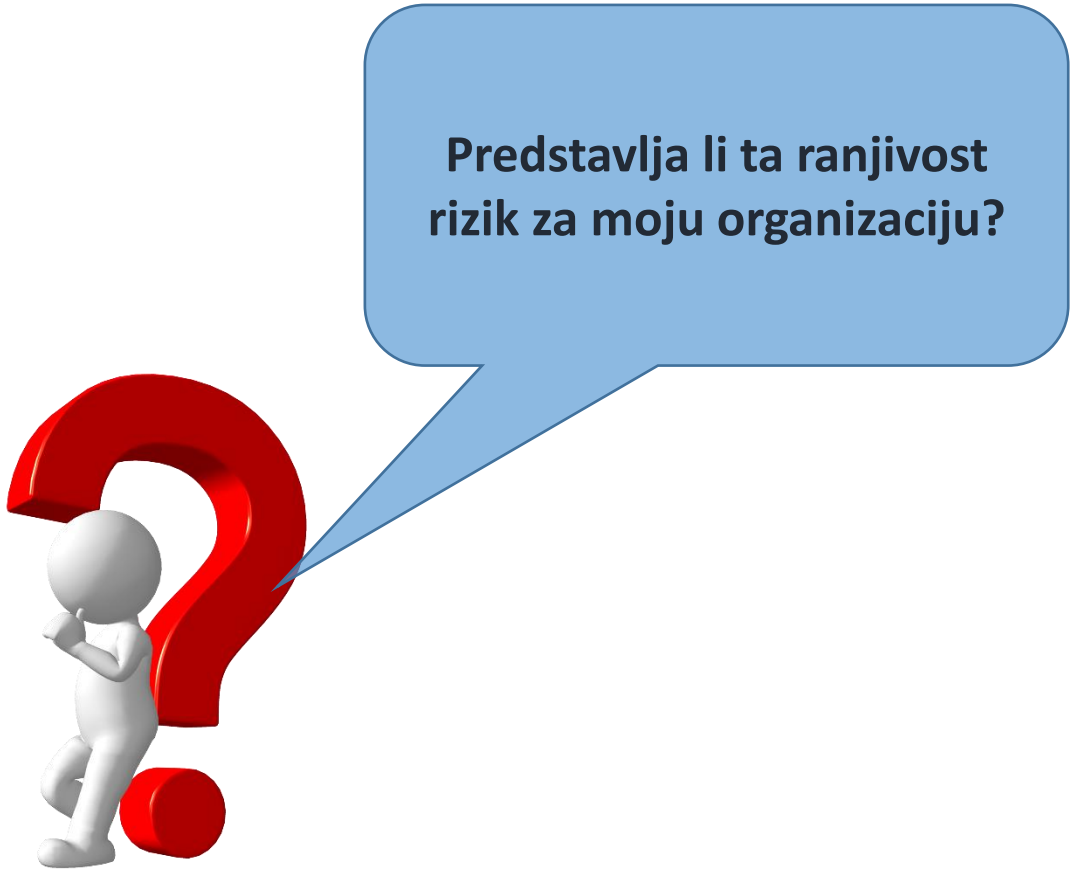
Rizik podrazumijeva nesigurnost. Ako će se nešto sasvim sigurno dogoditi, to ne predstavlja rizik.

PRIMJER

Ranjivost uslijed povećanja ovlasti postoji u sustavu Windows u slučaju u kojem komponenta Win32k ne uspije pravilno obraditi objekte u memoriji, što je takozvana „ranjivost uslijed povećanja ovlasti u Win 32k".
Toj su pogrešci izloženi sustavi

- Windows 7,
- **Windows Server 2012 R2**,
- Windows RT 8.1,
- **Windows Server 2008**,
- **Windows Server 2019**,
- **Windows Server 2012**,
- Windows 8.1,
- Windows Server 2016,
- **Windows Server 2008 R2**,
- Windows 10

Jedinstvena CVE oznaka ove ranjivosti jest CVE-2018-8641.



Godišnja procjena rizika

Procjena rizika na temelju šest kriterija

- Strategija
- Reputacija
- Financije
- Složenost procesa
- Upravljanje IT-em i informacijama
- Ljudski resursi

Br.	Proces	Rizici												
		Strategija	Reputacija	Financije	Složenost procesa	Upravljanje IT-em i informacijama	Ljudski resursi	Ukupno za unutarnju reviziju 2018.	Ukupno za unutarnju reviziju 2017.	Ukupno za unutarnju reviziju 2016.	Rukovodstveni prosjek 2018.	Rukovodstveni prosjek 2017.	Rukovodstveni prosjek 2016.	Razlika
Temeljni proces								a			b			c = a - b
A.1 – Financijsko upravljanje	Planiranje proračuna Kontrola i izvještavanje	4	4	2	4	3	3	20	20	20	22	20,5	15,3	(2)
A.2 – Mikroekonomska politika	Razvoj Provedba	4	4	4	4	4	4	24	24	24	23	23,5	17,3	1
A.3 – Politika računovodstva i revizije	Razvoj i provedba	4	4	4	3	2	2	19	19	17	19	16,4	17,3	0
A.4 – Informacijska sigurnost	Upravljanje informacijskom sigurnosti	4	4	2	4	4	4	22	22	22	22	23,0	16,3	(0,5)

Ocjena rizika		Ukupno	Učestalost revizije
Visok	4	21.-24.	Svaka kalendarska godina
Srednje visok	3	17.-20.	Svake 2 godine
Srednji	2	13.-16.	Svake 3 godine
Nizak	1	6.-12.	Odluka glavnog direktora za reviziju, Revizorskog ili Upravnog odbora

Godišnja procjena IT rizika, na temelju Cobita

	Proces br.	Procesi	Inherentni rizik (V, S, N)	Unutarnja kontrola (V, S, N)	Rezidualni rizik (V, S, N)	ZBROJ za inherentni rizik	Является ли упомянутая операция критической для ЦБ	Влияют ли ошибки и потери на авторитет ЦБ	Ведут ли к нарушению законодательства допущение ошибок и понесении потерь?	Имеет ли финансовое воздействие допущении ошибок и понесении потерь	Насколько реализация операции зависит от внешних факторов?	ZBROJ za unutarnju kontrolu	Присущий внутреннему контрольно уровень механизма по отношению к операции	Были ли прежде выявлены ошибки и пробелы	Насколько состоящийся этот аспект?	Насколько урегулировано этого процесса	Зависит ли ализация процесса от одного специалиста?	ZBROJ za rezidualni rizik	Učestalost ispitivanja
			Odgovorite na svako pitanje ocjenom od 1 do 4 *(1-nije važno, 4-vrlo važno)*																
			Inherentni rizik									Unutarnja kontrola							
		Procesi					25	25	15	25	10		25	25	20	15	15		
	Planiranje i organizacija (PO)																		
7	PO 1	Definirati strateški plan za IT.	V	V	V	400	4	4	4	4	4	400	4	4	4	4	4	16,0	1 godina
8	PO 2	Definirati informacijsku arhitekturu.	N	N	N	0						0						0,0	5 godina
9	PO 3	Utvrditi tehnološki smjer.	N	N	N	0						0						0,0	5 godina
10	PO 4	Definirati procese, organizaciju i odnose za IT.	N	N	N	0						0						0,0	5 godina
11	PO 5	Upravljati investicijama u IT.	N	N	N	0						0						0,0	5 godina
12	PO 6	Obavijestiti osoblje o ciljevima i smjeru rukovodstva.	N	N	N	0						0						0,0	5 godina
13	PO 7	Upravljati ljudskim resursima u području IT-a.	N	N	N	0						0						0,0	5 godina
14	PO 8	Upravljati kvalitetom.	N	N	N	0						0						0,0	5 godina
15	PO 9	Procijeniti rizike IT-a i i upravljati njima.	N	N	N	0						0						0,0	5 godina

REVIZIJSKI UNIVERZUM U PODRUČJU IT-A

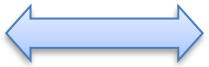
- Na temelju rizika

- Sistematski i sveobuhvatno *(ne bi trebalo postojati nijedno poslovno, administrativno ili IT područje koje se nikad ne revidira)*

REVIZIJSKI UNIVERZUM U PODRUČJU IT-A, PRIMJER

Subjekti revizije IT-a

- Planiranje i upravljanje IT-om
- Mreže, operativni sustavi, DBMS
- Stjecanje i razvoj IT-a
- Upravljanje rizicima i upravljanje kontinuitetom poslovanja (BCP)
- Fizička i tehnička sigurnost



Procesi COBIT

- Planiranje i organizacija
- Stjecanje i provedba
- Isporuka i podrška
- Monitoring i evaluacija

Jedinica za reviziju	Jedinica za reviziju po COBIT-u	Zakazano za 2018.	Zakazano za 2019.	Zakazano za 2020.
Planiranje i upravljanje IT-om	PO1.		X	
	PO2.		X	
	PO3.		X	
	PO4.		X	
	DS3.		X	
Planiranje i upravljanje IT-om – monitoring	PO8.			X
	M1.			X
	M2.			X
	M3.			X
	M4.			X
Mreže	DS9.	X		X
	DS10.	X		X
	DS13.	X		X
	AI6.	X		X
Baza podataka	DS9.	X		X
	DS10.	X		X
	DS11.	X		X
	DS13.	X		X
	AI6.	X		X
	AI7.	X		X
Operativni sustavi	DS9.		X	
	DS10.		X	
	DS13.		X	
	AI6.		X	
	AI7.		X	
Stjecanje i razvoj IT aplikacija	AI1.	X		X
	AI2.	X		X
	AI3.	X		X
	PO10.	X		X
Planiranje poslovnog kontinuiteta	DS1.		X	
	DS2.		X	
	DS4.		X	
	DS8.		X	
Informacijska sigurnost prema normi ISO27001:2013	DS5.	X	X	X
Fizička i tehnička sigurnost	DS12.	X		X

IT ODJEL

- **IT infrastruktura**
  - Podatkovni centri
  - Mrežna oprema
  - Poslužitelji *(Linux i Windows)*
  - Operativni sustavi
  - Aplikacije
- **Osoblje**
  - Zaposlenici

PREDMETI REVIZIJE IT-A

- Aplikacije:
  skupovi međusobno povezanih računalnih programa i relevantnih podataka za podršku jednog poslovnog procesa *(ili više njih)*.

- Često se revidiraju uz poslovni proces kojem pružaju podršku *(integrirana revizija)*

PREDMETI REVIZIJE IT-A

IT infrastrukture:

- hardverska i/ili softverska oprema kojom se podržava jedan aplikacijski sustav ili više njih
- Može ih se smatrati posebnim predmetima revizije ili ih se može revidirati uz aplikacijski sustav koji podržavaju

Primjeri:

- ✓ Sigurnost mreže
- ✓ Sustav e-pošte
- ✓ Intranet
- ✓ Operativni sustavi
- ✓ Sustav upravljanja bazom podataka

PREDMETI REVIZIJE IT-A

- Postupci upravljanja IT-om:

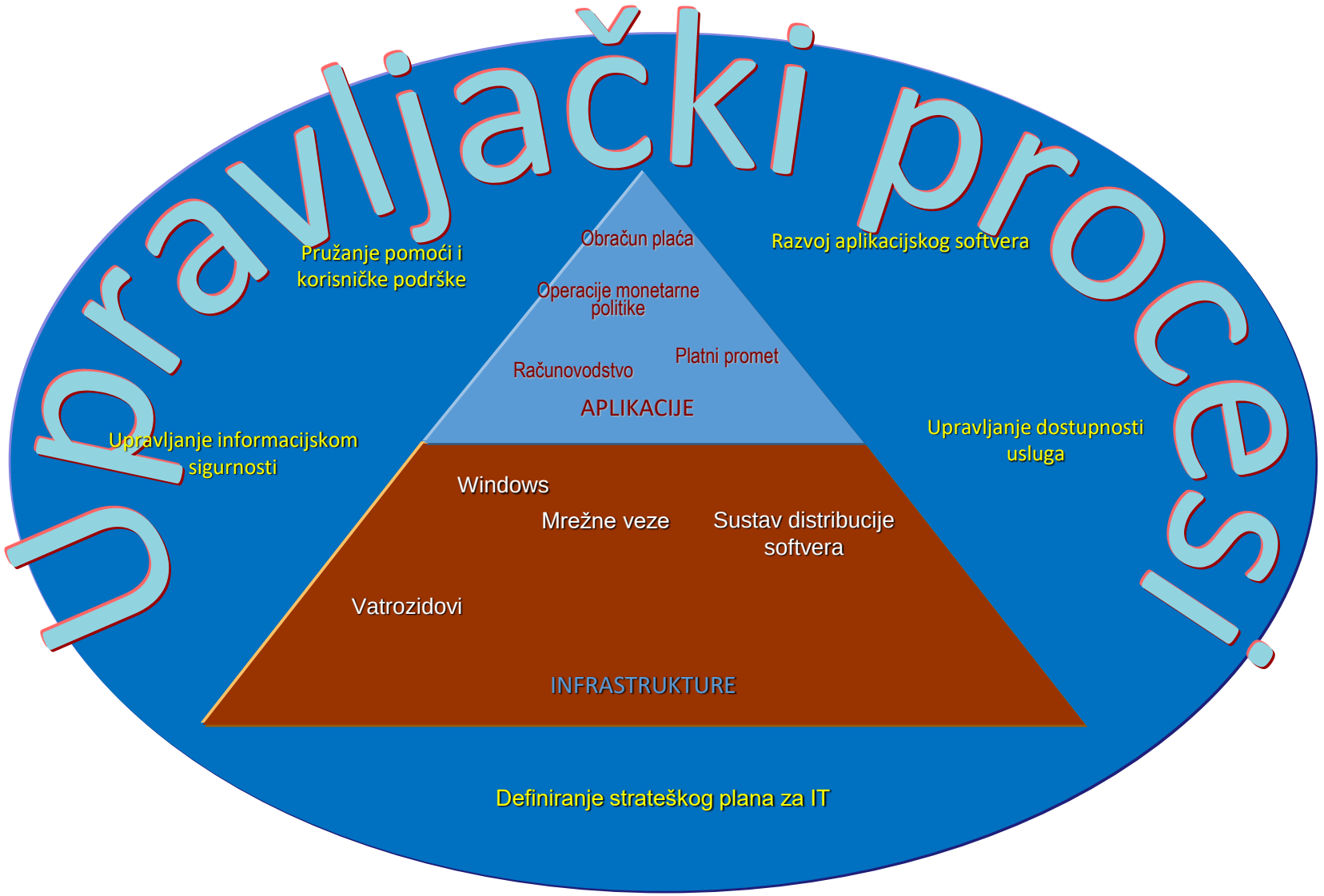
  Ljudske aktivnosti u odjelu za IT, kako je opisano u COBIT-u i ITIL-u

- Opće kontrole *(primjenjivo na nekoliko infrastruktura i aplikacija)*

PREDMETI REVIZIJE IT-A

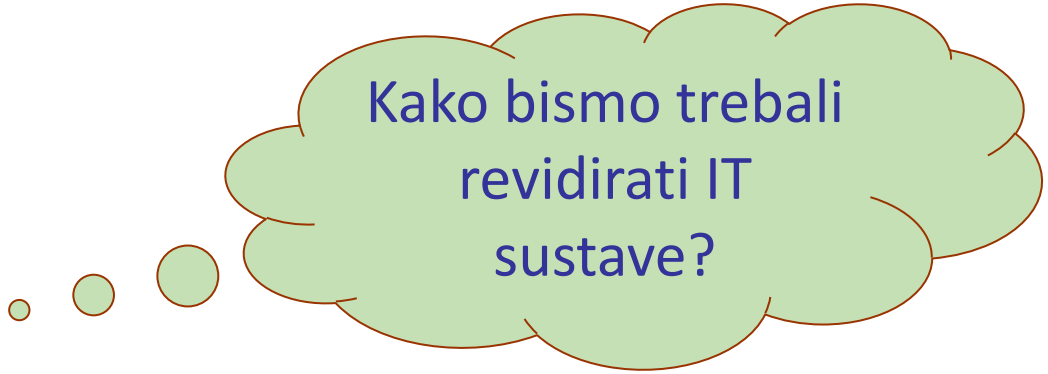
- Procesi upravljanja IT-om – primjeri:
  - Upravljanje incidentima
  - Upravljanje promjenama
  - Upravljanje konfiguracijama
  - Upravljanje razinom usluge
  - Upravljanje sigurnosti
  - Upravljanje kapacitetima

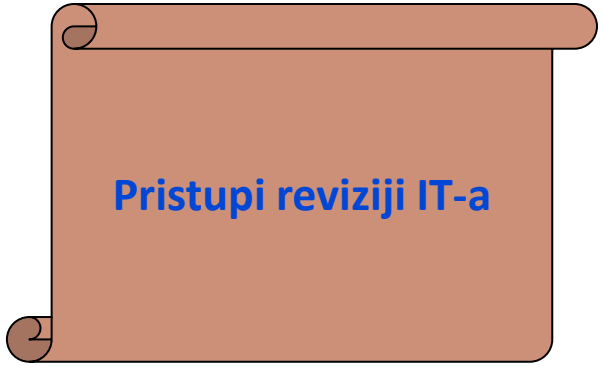
PREDMETI REVIZIJE IT-A



1. dan, 3. prezentacija

PRISTUPI REVIZIJI IT-A

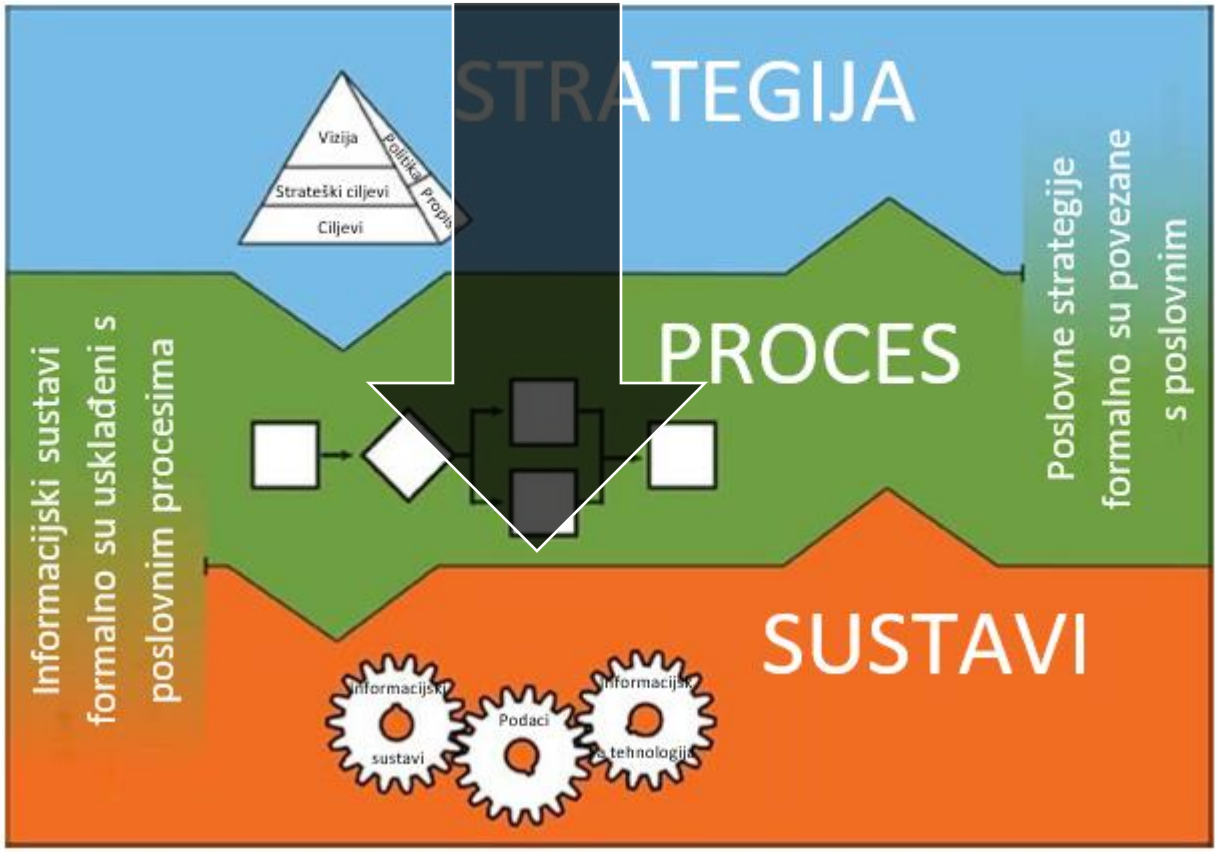




PRISTUPI REVIZIJI IT-A

1 Vertikalno

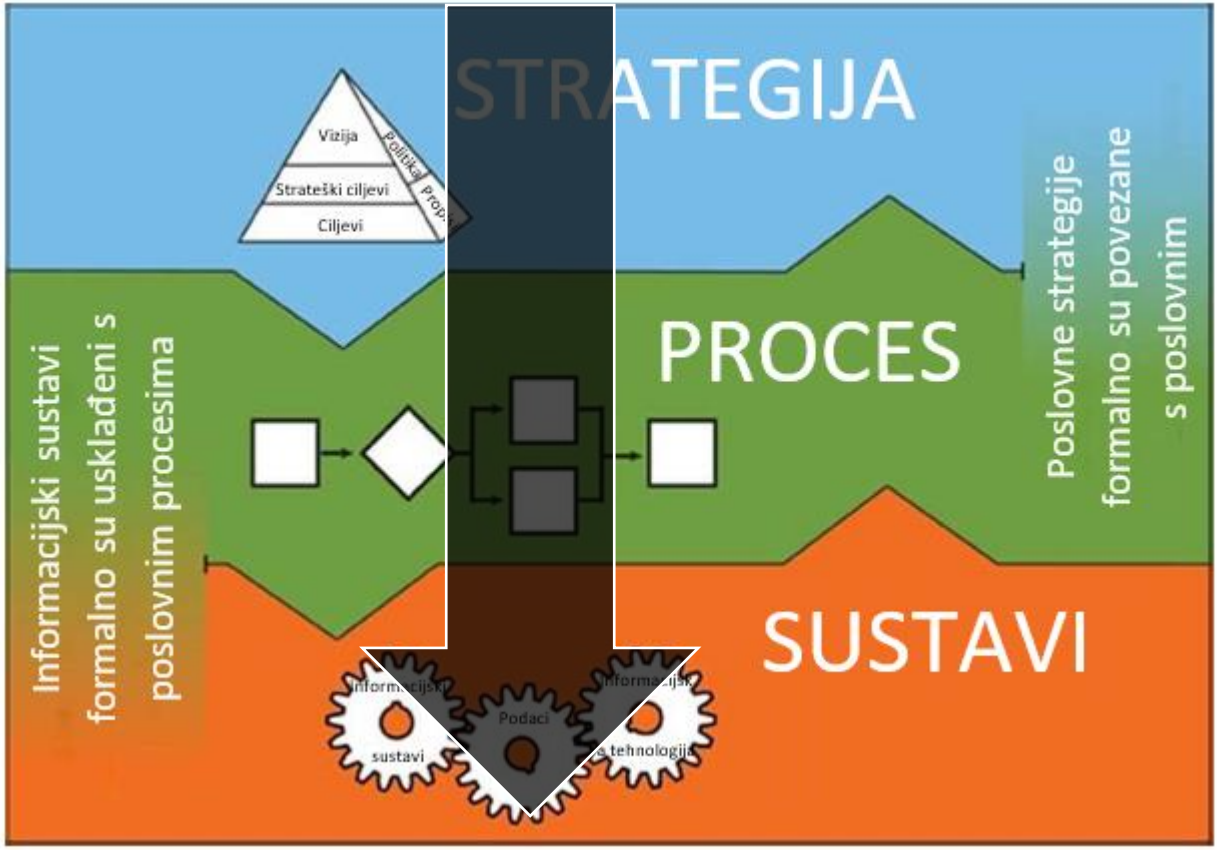
Opće IT kontrole u poslovnom procesu



PRISTUPI REVIZIJI IT-A

2 Duboko vertikalno

- ✓ Opće IT kontrole
- ✓ Aplikacijske kontrole



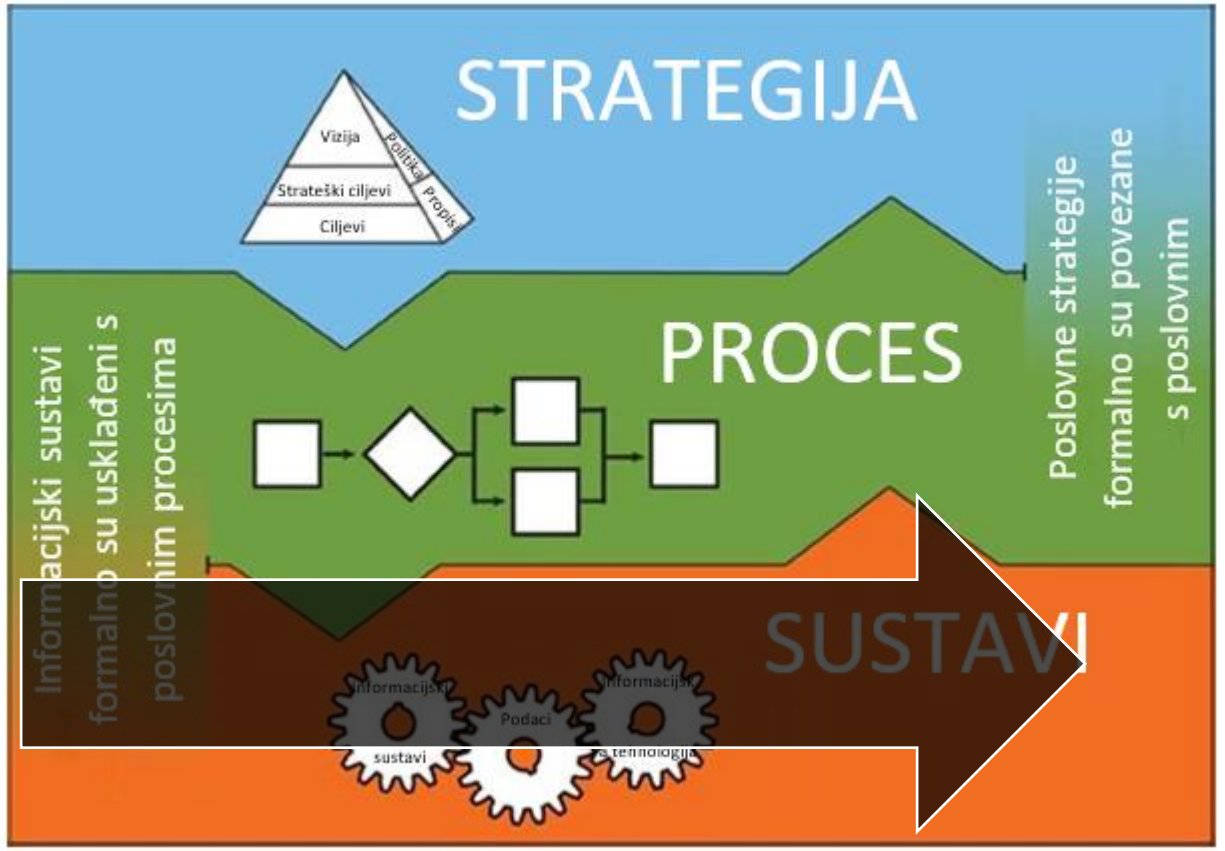
PRISTUPI REVIZIJI IT-A

3 Horizontalno

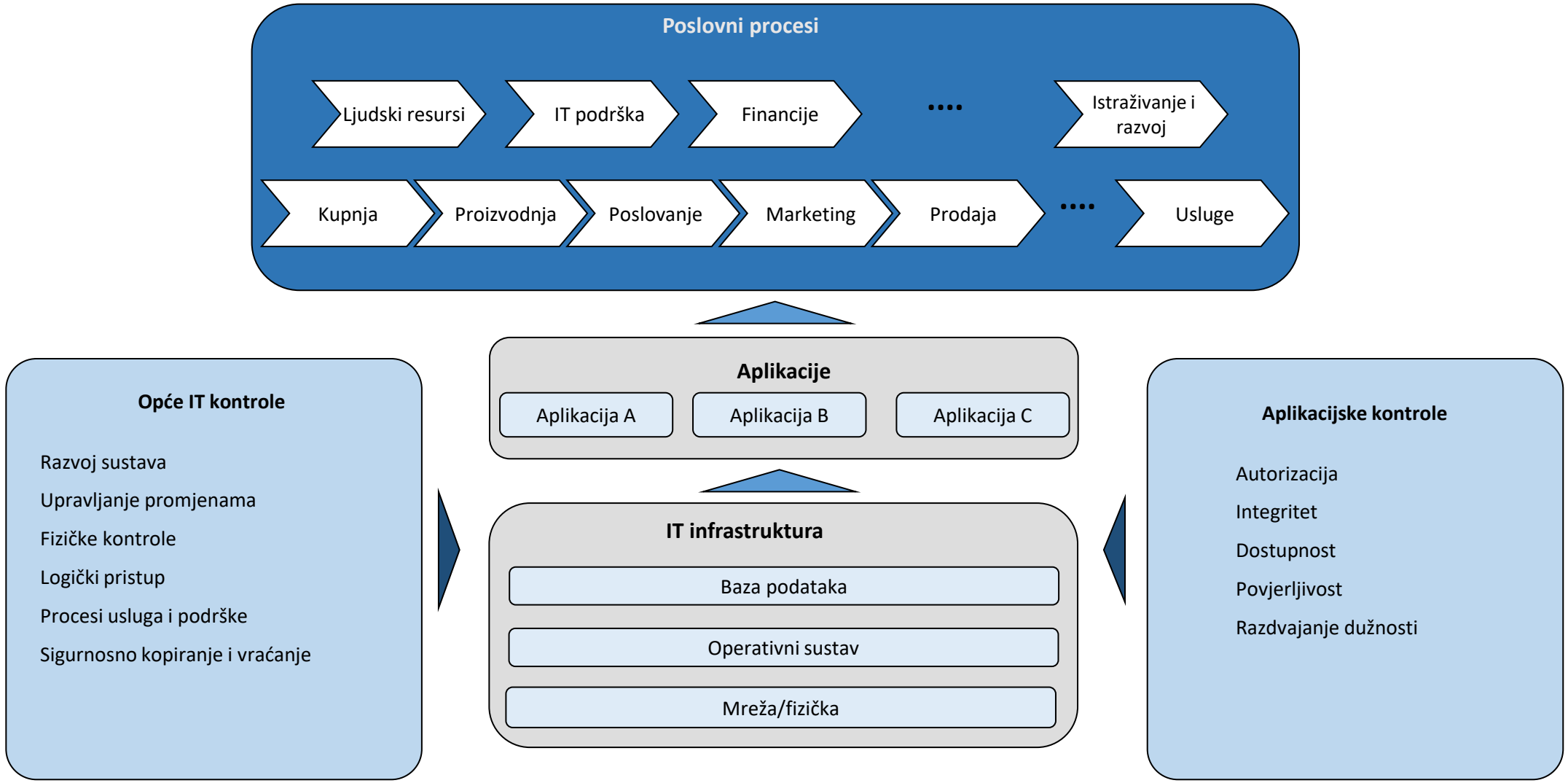
Sve relevantne IT kontrole

Primjeri:

- ✓ Informacijska sigurnost
- ✓ Upravljanje bazom podataka
- ✓ Služba za podršku



PRISTUPI REVIZIJI IT-A, OPĆE IT KONTROLE



Što još?

- **Revizija prije uvođenja**
  - Tijekom faze dizajniranja i uvođenja novih aplikacija, infrastruktura ili IT procesa, ili bilo kakvih značajnih promjena postojećih elemenata
- **Revizija nakon uvođenja**
  - Kada su aplikacije, infrastrukture ili IT procesi u pogonu

UPRAVLJANJE NEOVISNOSTI

- Izbjegavati sudjelovanje u samoj aktivnosti dizajniranja
- Odrediti potrebu za „ključnim kontrolama”, no ne i oblik koji bi trebale imati
- Prethodno postići dogovor o osnovnim pravilima sudjelovanja
- Odvajanje timova za reviziju prije i poslije uvođenja

PREDUVJETI ZA USPJEH

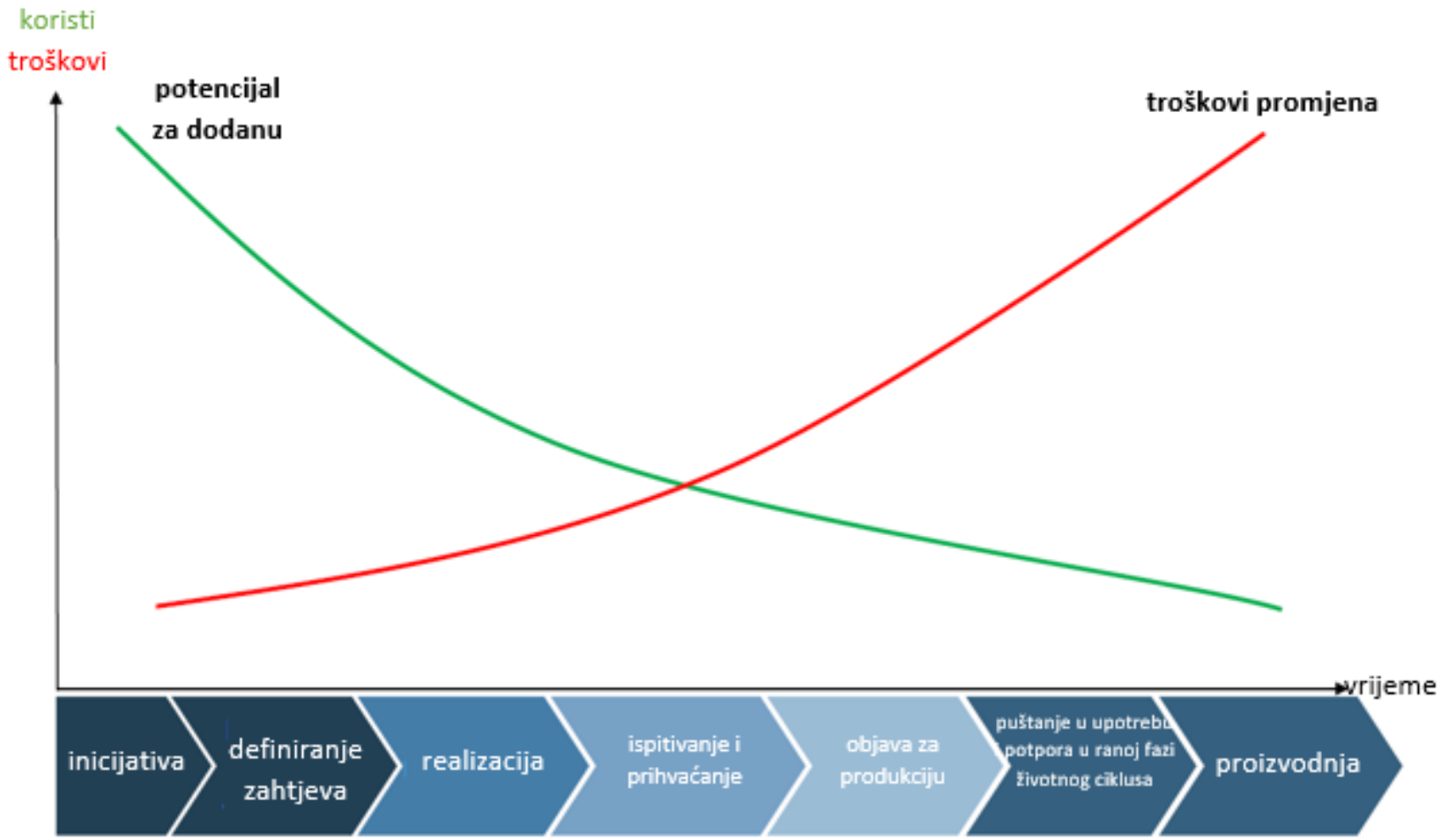
PREDUVJETI ZA USPJEH

- Potrebno je početi u fazi pokretanja projekta
- Potrebna je dobra koordinacija između voditelja projekta i revizora
- Mora se provoditi usporedno s projektom
- O rezultatima je potrebno podnijeti pravovremeni izvještaj

Izazovi

- Revizori se mogu smatrati članovima projektnog tima
- Provođenje revizija prije uvođenja može narušiti neovisnost revizora
- Tijekom revizije prije uvođenja revizor obično prima samo nacrte dokumenata koje pregledava

REVIZIJAMA PRIJE UVOĐENJA NASTAJE DODANA VRIJEDNOST



POTREBNE VJEŠTINE

Opće revizorske vještine i iskustvo

Opće poznavanje procesa kojima će aplikacija u razvoju pružati podršku

Vještine upravljanja projektima

Znanje i iskustvo revizora IT-a

OSTALA RAZMATRANJA

Potrebno je razmotriti...

Dodjeljuje se višim revizorima u skupini koji imaju najvišu razinu relevantne stručnosti.

Angažman revizora trebao bi započeti istovremeno s početkom sastavljanja razvojnog tima, a najkasnije pri utvrđivanju zahtjeva korisnika.

Vjerojatno neće zahtijevati puno radno vrijeme, već rad pri ključnim točkama tijekom razvojnog procesa.

Prva revizija nakon uvođenja provodi se najkasnije šest mjeseci nakon predaje projekta korisniku/operateru


Standardi,
metode i alati

STANDARDI, METODE I ALATI

- ✓ **GTAG 11** – praktični vodič(i), pruža(ju) smjernice za glavnog izvršnog revizora i timove za unutarnju reviziju o načinima izrade plana IT revizije na temelju rizika.
- ✓ **GAIT** – metodologija procjene opsega rada općih IT kontrola na temelju rizika

- ✓ **COBIT** – okvir, ciljevi kontrola, modeli zrelosti i vodič za osiguravanje IT procesa

- ✓ ISO 27002 *(Kodeks postupaka za upravljanje informacijskom sigurnošću)*
  - ✓ Smjernice, kontrole i tehnike za upravljanje informacijskom sigurnosti
- ✓ Smjernice za reviziju sustava za upravljanje informacijskom sigurnosti

- ✓ **PMBOK** (uz mapiranje COBIT-a i PMBOK-a) – može se upotrijebiti za razvoj revizijskog univerzuma i općih IT kontrola za procese upravljanja projektima.

KORACI U POSTUPKU PRUŽANJA UVJERENJA

Za svaki proces potrebno je provjeriti korake u postupku pružanja uvjerenja

1. korak: Provjeriti jesu li definirani opći i specifični ciljevi

2. korak: Provjeriti je li definirano vlasništvo procesa

3. korak: Provjerit jesu li definirane uloge i odgovornosti

4. korak: Provjerit jesu li definirane politike, planovi i postupci

5. korak: Provjeriti je li poboljšan učinak procesa

Način služenja Cobitom za planiranje i provedbu revizije IT-a

Struktura je sljedeća za svaki proces

Specifični cilj kontrola

Specifični ciljevi kontrola su zahtjevi visoke razine koje je potrebno razmotriti kako bi se mogla provesti učinkovita kontrola svakog procesa IT-a. Sročene su kao kratke prakse u pogledu upravljanja usmjerene na djelovanje.

Pokretači vrijednosti

Pokretači vrijednosti daju primjere prednosti za poslovanje koje mogu proizaći iz dobrih kontrola,

Pokretači rizika

pokretači rizika daju primjere rizika koje je potrebno izbjeći ili umanjiti

Ispitivanje dizajna kontrola

Pruža smjernice na razini objektivne kontrole za profesionalce u pružanju uvjerenja koji provode postupak pružanja uvjerenja u IT-u. Koraci su izvedeni iz kontrolnih praksi, koje su pak izvedene iz svakog specifičnog cilja kontrole.
Koraci ispitivanja uvjerenja:
– Procijenite dizajn kontrola
– Provjerite funkciju kontrola
– Procijeniti operativnu učinkovitost kontrole

PRIMJER – DS5 OSIGURATI SIGURNOST SUSTAVA

Cilj kontrole	Pokretači vrijednosti	Pokretači rizika
DS5.1 Upravljanje sigurnošću IT-a Upravljati sigurnošću IT-a na najvišoj odgovarajućoj organizacijskoj razini kako bi upravljanje sigurnosnim radnjama bilo u skladu sa zahtjevima poslovanja	• Kritična IT imovina je zaštićena • Strategija IT sigurnosti podržava potrebe poslovanja • Strategija IT sigurnosti usklađena je sa sveukupnim poslovnim planom • Odgovarajuće provedene i održavane sigurnosne prakse u skladu su s primjenjivim zakonima i propisima	• Nedostatak upravljanja IT sigurnošću • Neusklađenost ciljeva IT-a i poslovanja • Nezaštićeni podaci i informacijska imovina

Ispitivanje dizajna kontrole

- Utvrditi postoji li upravni odbor za sigurnost s predstavništvom u ključnim funkcionalnim područjima, uključujući unutarnju reviziju, ljudske resurse, operacije, IT sigurnost i pravni odjel
- Utvrditi postoji li proces kojim se daje prednost predloženim sigurnosnim inicijativama, uključujući potrebnu razinu politika, standarda i postupaka
- Ispitati i potvrditi postoji li povelja o informacijskoj sigurnosti.
- Pregledati i analizirati povelju kako bi se ustanovilo odnosi li se na organizacijsku sklonost preuzimanju rizika u odnosu na informacijsku sigumost te uključuje li povelja jasno sljedeće:
  - Opseg i ciljeve funkcije upravljanja sigurnošću
  - Odgovornosti funkcije upravljanja sigurnošću
  - Usklađenost i pokretače rizika
- Ispitati i potvrditi pokriva li politika informacijske sigumosti odgovornosti odbora, izvršnog rukovodstva, neposrednog rukovodstva, članova osoblja i svih korisnika IT infrastrukture poduzeća te odnosi li se na detaljne sigurnosne standarde i postupke.
- Ispitati i potvrditi postoje li detaljna sigurnosna politika, standardi i postupci. Primjeri politika, standarda i postupaka uključuju:
  - Politiku usklađenosti sigurnosti
  - Prihvaćanje rizika u upravljanju (potvrda o sigurnosnoj neusklađenosti)
  - Sigurnosnu politiku vanjske komunikacije
  - Politiku vatrozida
  - Sigurnosnu politiku e-pošte
  - Dogovor o usklađenosti s politikama informacijskog sustava
  - Sigurnosnu politiku prijenosnog/stolnog računala
  - Politiku uporabe interneta

ZAVRŠNE NAPOMENE

Nema jednog rješenja koje svima odgovara. **Međutim, ključni čimbenici su**:

Učinkoviti revizijski univerzumi **obuhvaćaju pristup utemeljen na riziku koji odgovara svakoj IT stavci u poslovnom procesu**, što je u skladu s određenim strateškim ciljem.

Glavni izvršni revizori trebali bi **pokazati višem rukovodstvu** kako će IT univerzum stvoriti dodanu vrijednost svakom procesu koji se revidira te kako svaki proces moće utjecati na strateške ciljeve i svrhe organizacije.

Glavni izvršni revizori trebaju se pobrinuti da je rukovodstvo **uključeno i, ako je moguće, da pruža odgovore** tijekom utvrđivanja i potvrđivanja revizijskog univerzuma IT-a.

Slijedom toga, angažman i podrška rukovodstva omogućuju glavnim izvršnim revizorima i unutarnjim revizorima IT-a da učinkovitije prenose svoje preporuke.


Thank You