HRVATSKA GOSPODARSKA KOMORA
TRIBINA ISO FORUM CROATICUM
Zagreb, 20.04.2017.

IZAZOVI U PRIMJENI NORME ISO 9001:2015

Dr.sc. Zdenko Adelsberger, dipl.inž.
zdenko@bluefield.hr
www.kvalis.com
www.bluefield.hr

Agenda

- Uvod
- Upravljanje dokumentima
- Mjerenja u ISO 9000:2015
- Kontekst
- Zainteresirane strane
- Znanje u organizaciji
- Razmišljanje na temelju rizika
- Zaključak

Neka pitanja tranzicije / implementacije

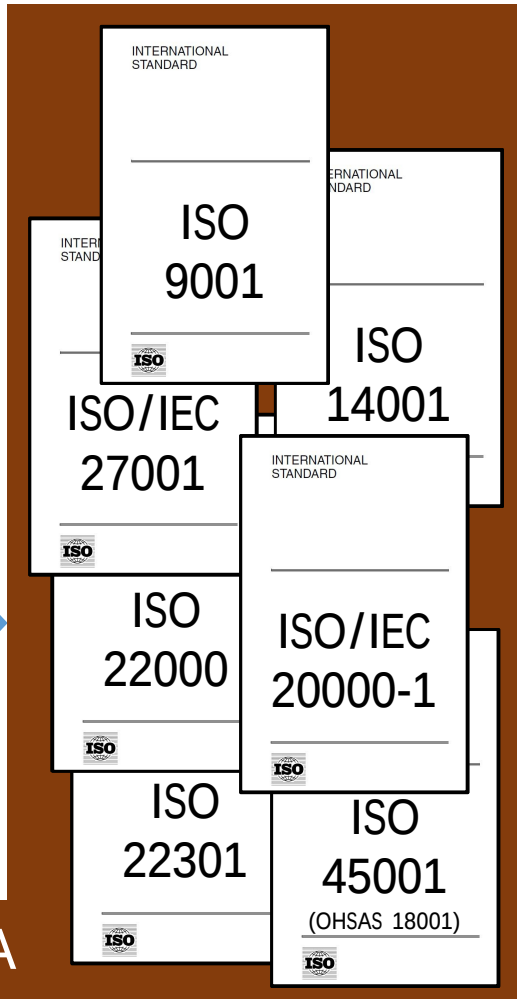
- Da li je lakše raditi tranziciju stare u novu reviziju ili sve ispočetka implementirati?
- Koliko se može iskoristiti od stare implementacije ?
- Da li su tranzicija ili implementacija zahtjevne aktivnosti?
- Koja nova znanja i vještine se treba / mora imati?
- Da li borba za KVALITETU organizacije završava certificiranim SUK-om?
- Što znači SUK u odnosu na druge sustave upravljanja prema ISO normama?

Poslije 2012. SVE specifikacije zahtjeva MORAJU biti u skladu s okvirom definiranim u Annex SL

Jedinstvena terminologija | Jedinstvena struktura | Jedinstvene definicije

Annex SL (2012) - okvir

1. Područje primjene (Scope)
2. Normativne reference (Normative references)
3. Nazivi i definicije (Terms and definitions)
4. **Kontekst organizacije** (Organizational context)
5. **Vodstvo** (Leadership)
6. **Planiranje** (Planning)
7. **Podrška** (Support)
8. **Operacije** (Operation)
9. **Ocjena uspješnosti** (Performance evaluation)
10. **Poboljšanje** (Improvement)



SPECIFIKACIJE ZAHTJEVA

Najznačajnije novosti u ISO 9001:2015

- Koncept rizika je utkan u cijeli SUK
- Naglasak na "razmišljanje na temelju rizika"
- "Proizvodi i usluge" umjesto "proizvoda"
- "Dokumentirane informacije " umjesto "dokumenti " i "zapisi"
- "Priručnik kvalitete" nije zahtjev
- Procesni pristup zahtjeva više propisa uključujući ulaze i izlaze procesa te mjerenja
- "Kontekst Organizacije" je dodan, a podrazumijeva širi pristup dizajnu SUK-a
- „Predstavnik za kvalitetu" nije više zahtjev, ali se mora identificirati osoba(e) za upravljanje SUK-om
- Ciljevi kvalitete moraju biti precizni i uključuju tko, što, gdje, i kako
- "Planiranje promjena" je zahtjev
- "Upravljanje znanjem" je zahtjev
- SUK se seli u opće sustave upravljanja
- Više se temelji na procesima
- Manje dokumentacije ali više i evidentiranih dokaza

Glavne razlike u terminologiji između ISO 9001:2008 and ISO 9001:2015

ISO 9001:2008	ISO 9001:2015
‘Proizvodi’	‘Proizvodi i usluge’
‘Dokumentacija’	‘Dokumentirane informacije’
‘Zapisi’	
‘Radno okruženje’	‘Radno okruženje procesa’
‘Kupljeni proizvodi’	‘Vanjski nabavljeni proizvodi i usluge’
‘Dobavljači’	‘Vanjski dobavljači’
‘Preventivne akcije’	-
‘Isključenja’	-
‘Predstavnik uprave’	-

Principi upravljanja kvalitetom

ISO 9000:2008

1) Usmjerenost na kupca
2) Vodstvo
3) Uključivanje ljudi
4) Procesni pristup
5) Sustavni pristup upravljanju
6) Stalno poboljšanje
7) Činjenični pristup odlučivanju
8) Uzajamno korisni odnosi s dobavljačima

ISO 9000:2015

1) Usmjerenost na kupca
2) Vodstvo
3) Uključivanje ljudi
4) Procesni pristup
5) Poboljšanje
6) Odlučivanje utemeljeno na dokazima
7) Upravljanje odnosima

Usporedba sadržaja normi

ISO 9001:2008	ISO 9001:2015
0. Uvod	0. Uvod
1. Područje primjene	1. Područje primjene
2. Upućivanje na druge norme	2. Upućivanje na druge norme
3. Nazivi i definicije	3. Nazivi i definicije
4. Sustav upravljanja kvalitetom	4. Kontekst organizacije
5. Odgovornost uprave	5. Vodstvo
6. Upravljanje resursima	6. Planiranje
7. Realizacija proizvoda	7. Podrška
8. Mjerenje, analiza, poboljšanje	8. Radni proces
	9. Vrednovanje mjerljivih rezultata
	10.Poboljšavanje

Teme točaka sa specifikacijama u ISO 9001:2015

T	Zahtjev
4	KONTEKST ORGANIZACIJE Uvodi se zahtjev razumijevanja "konteksta organizacije", te očekivanja zainteresiranih strana kao i potencijalnih utjecaja na ciljeve sustava. Postizanje ciljeva je preduvjet za zadovoljstva kupaca.
5	VODSTVO Vodstvo uključuje većinu zahtjeva iz točke "5. Odgovornost uprave (2008)".
6	PLANIRANJE Povećan je naglasak na "planiranje", koje se usredotočuje na identifikaciju rizika i prilika jer oni utječu na područje primjene sustava. Time se uklanja potreba za preventivnim akcijama kao što je definirano u verziji 2008., ali uključuje i pojačava zahtjeve za upravljanje promjenama i upravljanje rizicima.
7	PODRŠKA "Podrška" uključuje većinu zahtjeva iz prethodne revizije točki "6. Upravljanje resursima (2008)", ali uključuje i novi zahtjev upravljanja „organizacionim znanjem".
8	RADNI PROCES "Operacije" zamjenjuju iz prethodne revizije točku "7. Realizacija proizvoda (2008)" i uključuje većinu njenih zahtjeva. Namjera je učiniti zahtjeve više relevantne za servisni sektor.
9	VREDNOVANJE MJERLJIVIH REZULTATA "Ocjena uspješnosti" zamjenjuje iz prethodne revizije točku "8. Mjerenje, analiza, poboljšanje (2008)" iz koje je izbačen zahtjev za preventivnim akcijama u skladu s točkom 6 Planiranje.
10	POBOLJŠAVANJE Povećan je fokus na „Poboljšavanje" a uključuje nesukladnosti i korektivne akcije iz točke "8. Mjerenje, analiza, poboljšavanje (2008)".

ISO 9001:2015 zahtjevi u PDCA krugu

PLAN				DO	CHECK	ACT
4. Kontekst organizacije	5. Vodstvo	6. Planiranje za QMS	7. Podrška	8. Radni proces	9. Vrednovanje mjerljivih rezultata	10.Poboljšavanje
4.1 Razumijevanje organizacije i njezina konteksta	5.1 Vodstvo i opredijeljenost	6.1 Mjere za poduzimanje koraka povezanih s rizicima i prilikama	7.1 Resursi	8.1 Operativno planiranje i nadzor	9.1 Praćenje, mjerenje, analiza i vrednovanje	10.1 Općenito
4.2 Razumijevanje potreba i očekivanja zainteresiranih strana	5.2 Politika kvalitete	6.2 Ciljevi kvalitete i planiranje njihova postizanja	7.2 Osposobljenost	8.2 Zahtjevi za proizvode i usluge	9.2 Interni audit	10.2 Nesukladnost i popravna radnja
4.3 Određivanje područja primjene sustava upravljanja kvalitetom	5.3 Uloge, odgovornosti i ovlaštenja u organizaciji	6.3 Planiranje promjena	7.3 Svjesnost	8.3 Projektiranje i razvoj proizvoda i usluga	9.3 Preispitivanje od rukovodstva	10.3 Trajno poboljšavanje
4.4 Sustav upravljanja kvalitetom i njegovi procesi			7.4 Komunikacija	8.4 Nadzor nad procesima, proizvodima i uslugama pribavljenim od vanjskih dobavljača		
			7.5 Dokumentirane informacije	8.5 Proizvodnja i pružanje usluga		
				8.6 Puštanje proizvoda i usluga u promet		
				8.7 Nadzor nad nesukladnim izlazima		

Odnos između zahtjeva u ISO 9001:2015 i ostalih međunarodnih normi (smjernica)

Druge međunarodne norme	Zahtjevi u ISO 9001:2015						
	4	5	6	7	8	9	10
ISO 9000 Quality management systems	SVE	SVE	SVE	SVE	SVE	SVE	SVE
ISO 9004 Managing for the sustained success of an organization	SVE	SVE	SVE	SVE	SVE	SVE	SVE
ISO 10001 Guidelines for codes of conduct for organizations					8.2.2 8.5.1	9.1.2	
ISO 10002 Guidelines for complaints handling in organizations					8.2.1	9.1.2	10.2.1
ISO 10003 Guidelines for dispute resolution external to organizations						9.1.2	
ISO 10004 Guidelines for monitoring and measuring						9.1.2 9.1.3	
ISO 10005 Guidelines for quality plans		5.3	6.1 6.2	SVE	SVE	9.1	10.2
ISO 10006 Guidelines for quality management in projects	SVE	SVE	SVE	SVE	SVE	SVE	SVE
ISO 10007 Guidelines for configuration management					8.5.2		
ISO 10008 Guidelines for business-to-consumer electronic commerce transactions	SVE	SVE	SVE	SVE	SVE	SVE	SVE
ISO 10012 Requirements for measurement processes and measuring equipment				7.1.5			
ISO/TR 10013 Guidelines for quality management system documentation				7.5			
ISO 10014 Guidelines for realizing financial and economic benefits	SVE	SVE	SVE	SVE	SVE	SVE	SVE
ISO 10015 Guidelines for training				7.2			
ISO 10017 Guidance on statistical techniques			6.1	7.1.5		9.1	
ISO 10018 Guidelines on people involvement and competence	SVE	SVE	SVE	SVE	SVE	SVE	SVE
ISO 10019 Guidelines for the selection of QMS consultants and use of their services					8.4		
ISO 19011 Guidelines for auditing management systems						9.2	

„SVE" ukazuje na to da se sve podtočke u određenom zahtjevu odnose se na drugu međunarodnu normu

Pitanja vezana za tranziciju na ISO 9001:2015

Stanje: Imamo uspostavljeni QMS i certificiran je prema ISO 9001:2008

PITANJE	ODGOVOR
Imamo li višak zahtjeva iz revizije 2008 koje treba ukloniti?	Nema, osim zahtjeva za preventivne akcije koji je postao besmislen zbog implementacije kontrola u procjeni rizika. Proceduru za preventivne akcije treba ukloniti. Ostale prema procjeni.
Da li postoje zahtjevi u reviziji 2015 kojih nema u reviziji 2008?	Objektivno samo zahtjevi iz poglavlja 4 (kontekst organizacije) i poglavlja 6 (planiranje) su potpuno novi.
Što je sa zahtjevima koji vrijede u reviziji 2015, a postojali su i u reviziji 2008?	Niz zahtjeva je promijenio poglavlje što dovodi do reorganizacije dokumentacije. Neke zahtjeve iz 2008 treba znatno bolje dokumentirati (zapisi kao dokazi, posebno mjerenja učinkovitosti i djelotvornosti procesa i ciljeva)

Tranzicija ili implementacija ISO 9001:2015

Plan	Dokumenti	Trening	Audit
Definirati plan što sve treba uraditi, na koji način, tko, kada, ...	Izraditi sve planirane (potrebne) dokumentirane informacije	Na temelju dokumentiranih informacija provesti trening svih koji sudjeluju u SUK	Provesti audit prema zahtjevima ISO 9001:2015

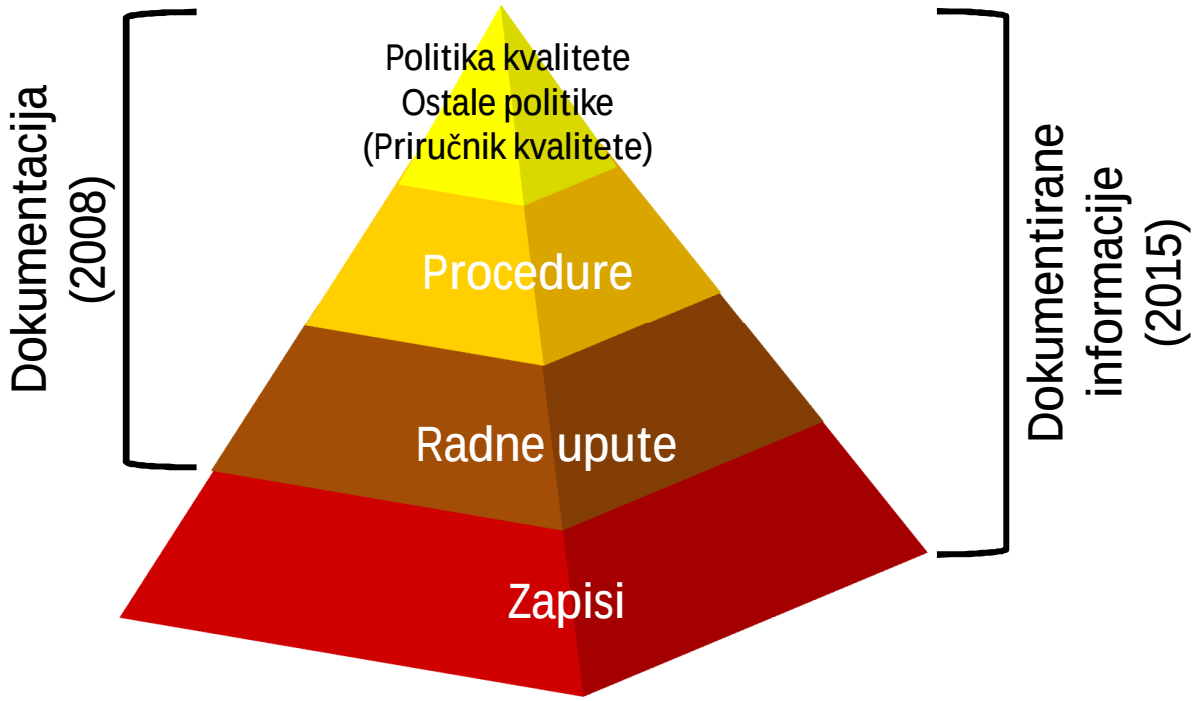
GAP analiza – koraci za provedbu

1. Priprema rasporeda i plana audita za GAP analizu;
2. Pridružiti odgovorne auditore za pojedina područja audita;
3. Kopirati svaku sekciju Check-liste auditorima na koje se odnosi dio;
4. Provedba aktivnosti prema Check-listi
   a. Identificirati područja koja treba razviti.
   b. Napraviti listu procedura ili drugih dokumenta koje imaju ili osiguravaju informacije za novi QMS.
   c. Definirati zabilješke na statuse dokumenata:
      i. Da li trebaju biti revidirani za novu reviziju?
      ii. Ili mogu biti korišteni takvi kavi jesu?
      iii. Ili proces postoji, ali treba biti dokumentiran.

Stupanj promjena u ISO 9001:2015

UPRAVLJANJE DOKUMENTIMA DOKUMENTIRANE INFORMACIJE (7.5)

Dokumentirane informacije ISO 9001:2015



2008 je bio zahtjev: kontrolirana promjena za dokumentaciju i apsolutna nepromjenjivost za zapise → 2015 SE NIŠTA PROMIJENILO NIJE

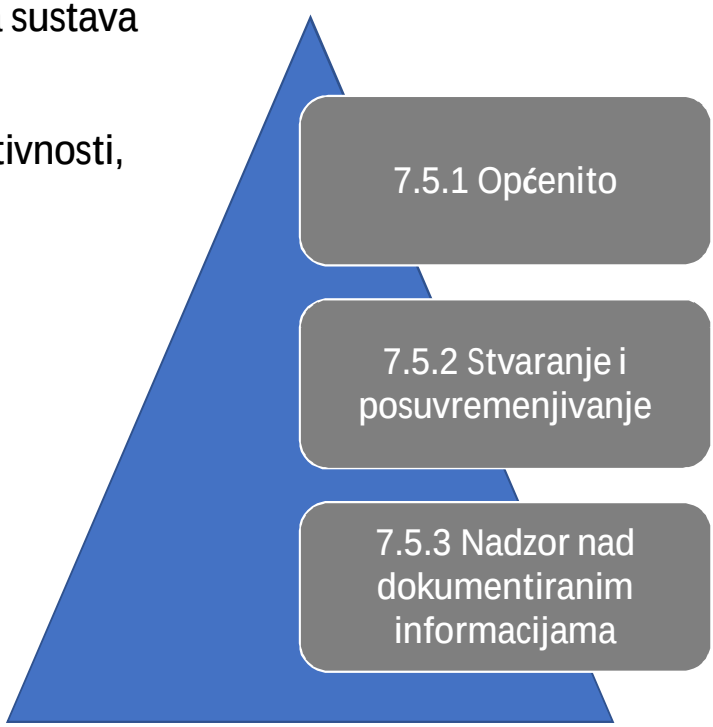
7.5 Dokumentirane informacije

Opseg dokumentiranih informacija sustava upravljanja kvalitetom određen je:

- veličinom organizacije, vrstom aktivnosti, procesa, proizvoda i usluga;
- složenosti procesa i njihovih međudjelovanja;
- osposobljenosti osoba.

PITANJA:

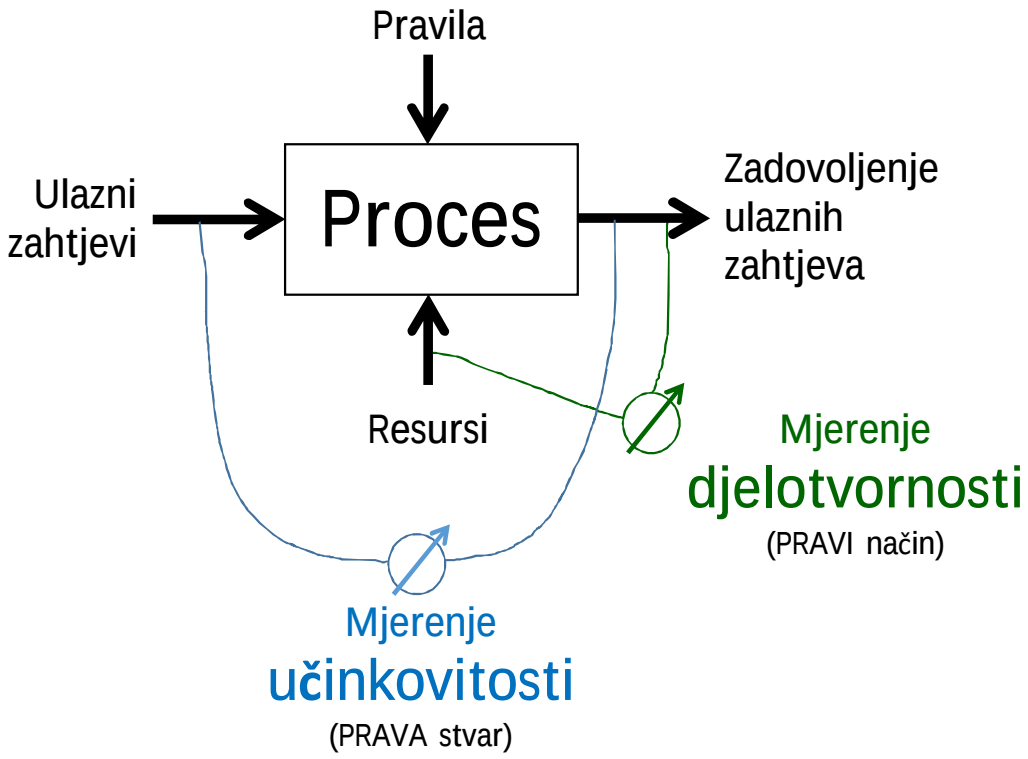
- Za čega raditi dokumentirane informacije?
- Što je kriterij za nepostojanje određenih dokumentiranih informacija?



MJERENJA U ISO 9001:2015 (9.1)

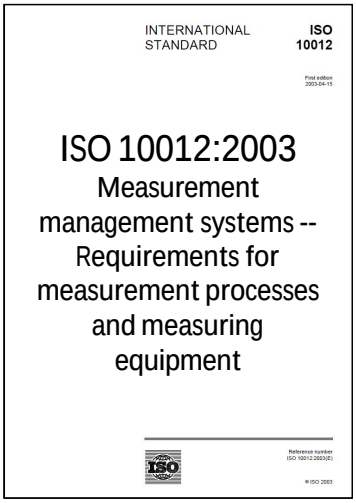
Mjerenja: zahtjev u ISO 9001:2015

Mjerenjem se osigurava ideal: Radi PRAVU stvar na PRAVI način !

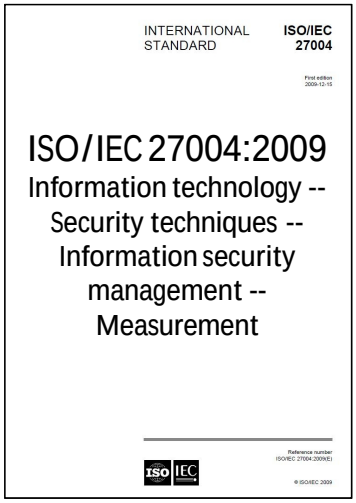


Mjerenja na procesu

Učinkovitost (effectiveness): mjera za postizanje planiranih rezultata
Djelotvornost (efficiency): odnos između postignutih rezultata i upotrijebljenih resursa



+



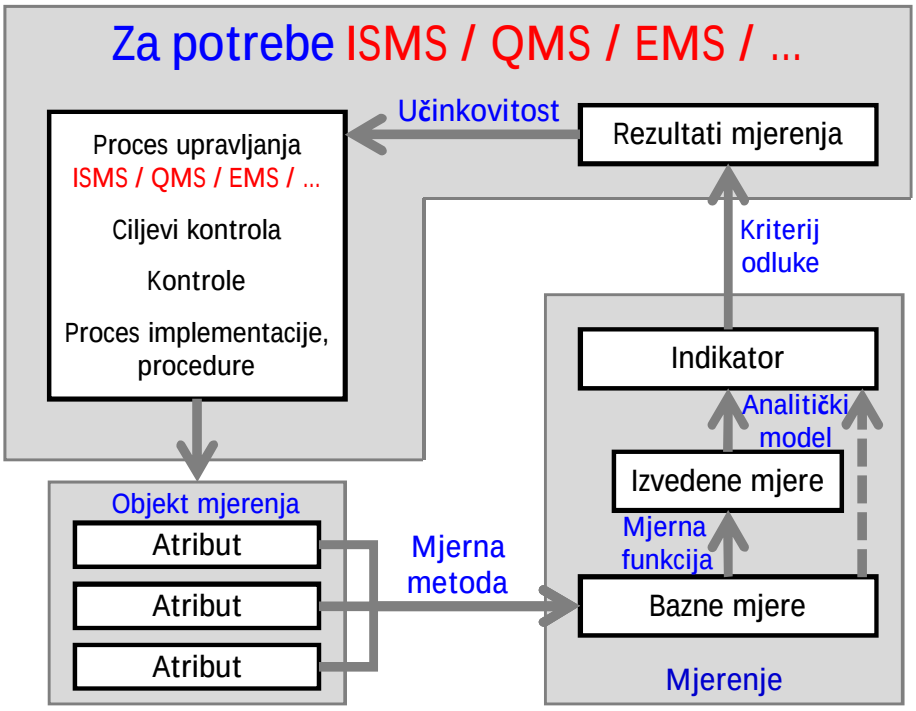
=

NAPOMENA za primjenu u QMS-u

- 'information security' čitaj 'quality'
- 'ISMS' čitaj 'QMS'
- 'information' čitaj 'quality'

Model mjerenja sustava upravljanja

(prema ISO/IEC 27004)



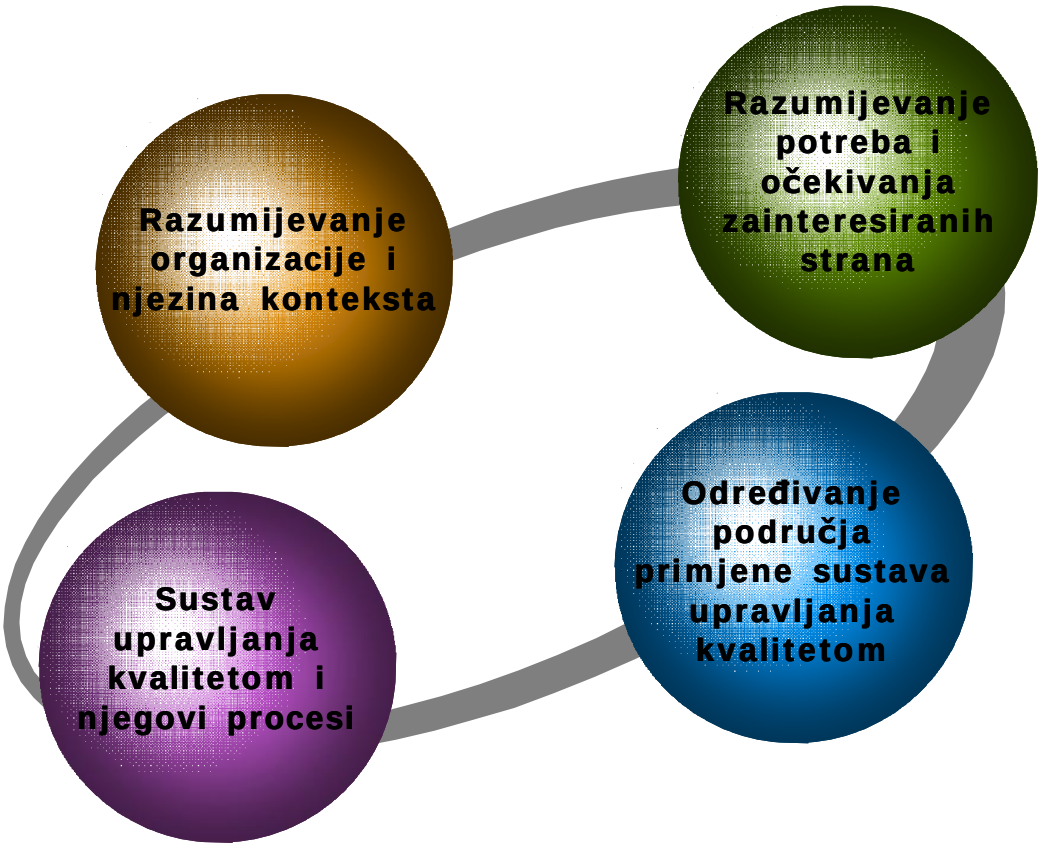
Sadržaj radne upute za mjerenje učinkovitosti

(Primjer prema ISO/IEC 27004)

Identifikacija mjerenja	Naziv mjerenja, ID mjerenja, svrha mjerenja, primjena na koje procese
Objekt mjerenja i atributi	Objekt mjerenja, Atributi
Osnovne specifikacije za mere (za svaku baznu meru [1...n])	Bazno mjerenje, metoda mjerenja, vrste metode mjerenja, mjerna skala, tip skale, mjerna jedinica
Specifikacija izvedene mjere	Izvedena mjera, funkcija mjerenja
Specifikacija pokazatelja (indikatora)	Pokazatelj, analitički model
Specifikacija kriterija za odluku	Kriteriji za odluku
Rezultati mjerenja	Interpretacija pokazatelja, forme izvještavanja
Zainteresirane strane	Korisnici mjerenja, recenzent mjerenja, vlasnik informacije, skupljač informacija, komunikator informacija
Frekvencija/Period	Frekvencija prikupljanja podataka, frekvencija analiziranja podataka, frekvencija izvještavanja rezultata mjerenja, revizija mjerenja, period mjerenja

KONTEKST (4)

4. Kontekst organizacije



Kontekst organizacije – naglasci

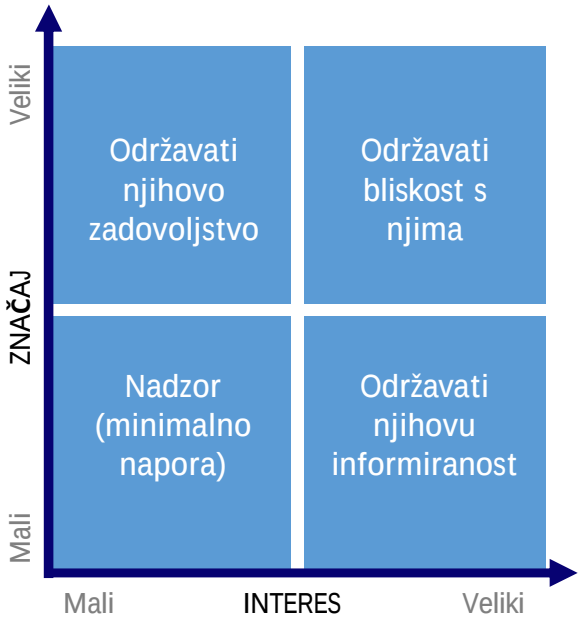
Zahtijeva se od organizacije da procjeni sebe i svoj kontekst, te odredi učinke različitih elemenata na nju. Drugim riječima, treba odrediti kako unutarnji i vanjski problemi utječu na kulturu organizacije, njene ciljeve, proizvode, tijek procesa, tržišta, kupaca itd. Definiranjem konteksta organizacija čini prvi korak za otkrivanje rizika i mogućnosti u poslovnom kontekstu.

ZAINTERESIRANE STRANE (4.2)

ISO 9001:2015 – Neke od najznačajnijih zainteresiranih strana

Zainteresirana strana je osoba ili organizacija koja može utjecati, da bude pod utjecajem, ili smatraju da na njih utječe odluka ili aktivnost.

PROCES za mapiranje ZAINTERESIRANIH STRANA



Identificirati relevantne zainteresirane strane
Savjet: stvoriti tablicu ili tablice s kolonama zainteresiranih strana, dodajte stupce za potrebe i očekivanja, Značaj / Interes i ciljevi.

Odredite njihove potrebe i očekivanja.
Savjet: istražite njihove potrebe i sumarne rezultate dodati u odgovarajuće stupcu u tablici zainteresiranih strana.

Rangirati ih i smislu značaja interesa
Savjet: analizirati svoje značaje i interese te dodati rang u relevantnom stupcu u tablici zainteresiranih strana.

Prepoznati ciljeve i prioritete
Savjet: postavljanje SMART* ciljeva gdje god je to moguće, te ih dokumentirati u tablici zainteresiranih strana.

* SMART
S - specifični, značajni, prilagodljivi
M - mjerljivi, smisleni, motivacijski
A - dogovoreni, dostižni, ostvarivi, prihvatljivi, usmjereni na djelovanje
R - realistični, relevantni, razumni, nagrađivani, orijentirani na rezultate
T – vremenski utemeljeni, vremenski ograničeni, pravovremeni, opipljivi, može ih se pratiti

Elementi opsega sustava upravljanja kvalitetom

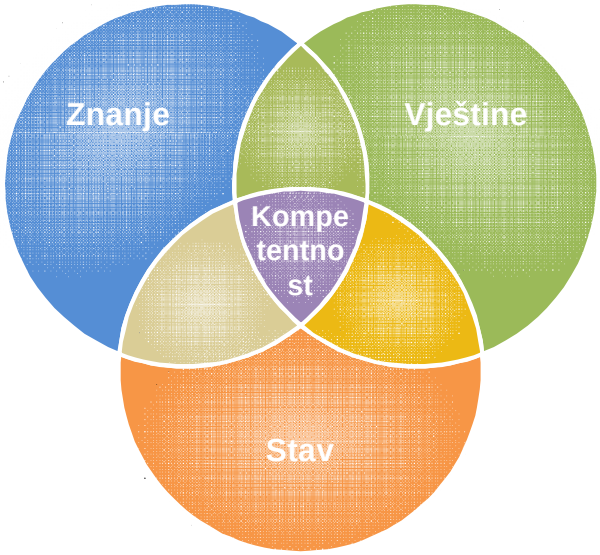
ZNANJE U ORGANIZACIJI (7.1.6)

Cilj je u definiranju kompetentnosti

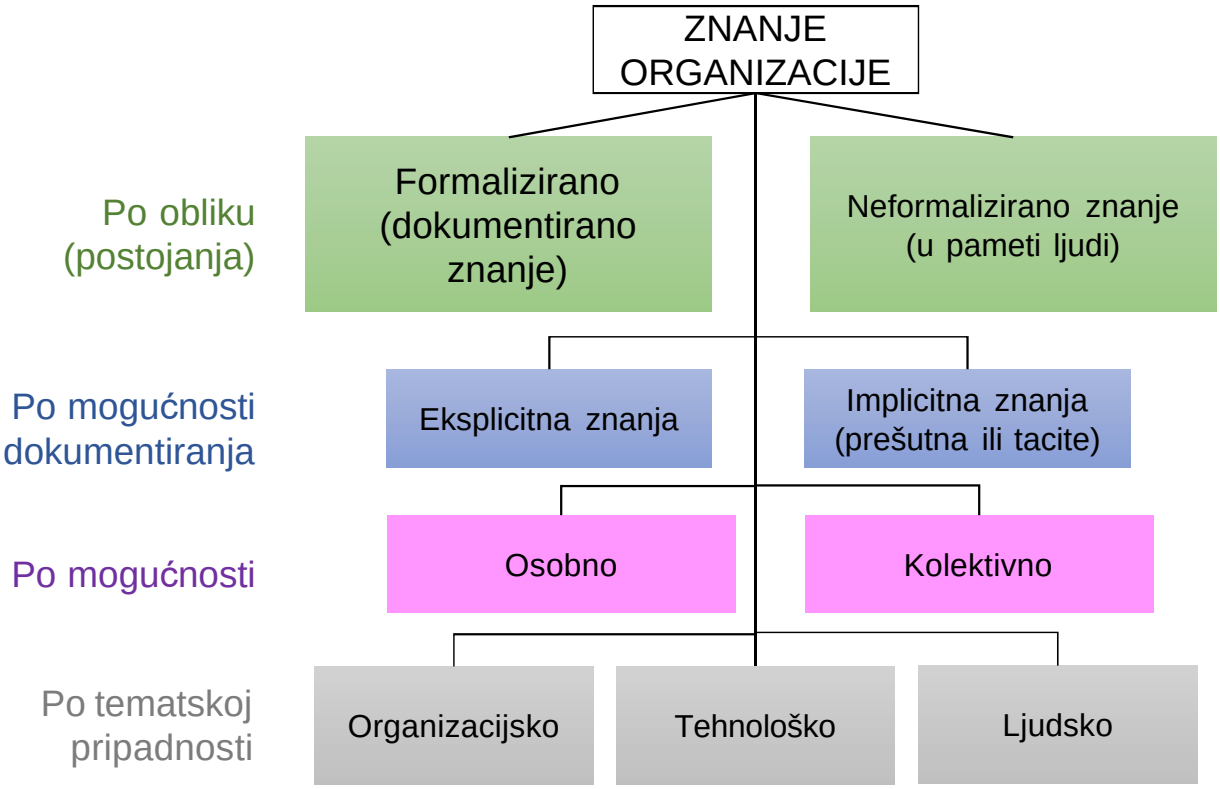
Organizacija mora odrediti znanje potrebno za odvijanje svojih procesa i postizanje sukladnosti proizvoda i usluga.

To se znanje mora održavati i mora biti raspoloživo u potrebnom opsegu.

Organizacija mora razmotriti svoje sadašnje znanje i odrediti kako steći ili ostvariti pristup potrebnom dodatnom znanju i obnoviti postojeće.



Klasifikacija znanja



Razmišljanje na temelju rizika (Risk-Based Thinking)

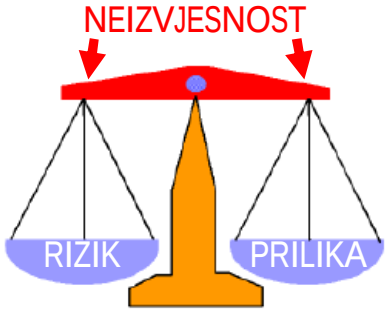
Razmišljanje na temelju rizika (Risk-Based Thinking)

ISO 9001:2015 A.4

Činjenice:

- Razmišljanje na temelju rizika je nešto što svi provode automatski, često pod-svjesno
- Koncept rizika uvijek je bio implicitno u ISO 9001, ali u reviziji 2015 je eksplicitno ugrađen u cijeli sustav upravljanja
- Razmišljanje na temelju rizika je dio procesnog pristupa
- Razmišljanje na temelju rizika čini da je preventivno djelovanje dio rutine

O riziku se često razmišlja samo u negativnom smislu. Razmišljanje na temelju rizika može pomoći identificirati mogućnosti. To se može smatrati da je pozitivna strana rizika.



Kako se definiraju zahtjevi prema rizicima u ISO 9001:2015

0.1.c) poduzimanje koraka povezanih s rizicima i prilikama vezanim uz kontekst i ciljeve organizacije;
0.1 Ova međunarodna norma primjenjuje procesni pristup koji objedinjuje ciklus „planirati – provesti – provjeriti – djelovati“ (Plan-Do-Check-Act – PDCA) i pristup utemeljen na rizicima.
0.3.2. Planirati (Plan): ustanoviti ciljeve sustava, njegove sastavne procese i resurse potrebne za postizanje rezultata u skladu sa zahtjevima kupaca i organizacijskim politikama te utvrditi rizike i prilike i poduzeti korake povezane s njima
4.4.1.f) poduzeti korake povezane s rizicima i prilikama utvrđenim u skladu sa zahtjevima iz 6.1;
5.1.1.d) promicanjem primjene procesnog pristupa i pristupa utemeljenog na rizicima;
5.1.2.b) da se utvrde rizici i prilike koji mogu utjecati na sukladnost proizvoda i usluga i na sposobnost povećanja zadovoljstva kupaca i da se poduzmu koraci povezani s tim rizicima i prilikama;
6.1 Mjere za poduzimanje koraka povezanih s rizicima i prilikama

6.1 Mjere za poduzimanje koraka povezanih s rizicima i prilikama

6.1.1 Prilikom planiranja sustava upravljanja kvalitetom, organizacija mora razmatrati pitanja iz 4.1 i zahtjeve iz 4.2 i odrediti rizike i prilike s obzirom na koje treba poduzeti korake kako bi se:

a) zajamčilo da sustav upravljanja kvalitetom može ostvariti predviđene rezultate;
b) poboljšali poželjni učinci;
c) spriječile ili umanjile neželjene posljedice:
d) postigla poboljšanja.

6.1.2 Organizacija mora planirati:

a) mjere za poduzimanje koraka povezanih s tim rizicima i prilikama;
b) način na koji će:
   1) integrirati i uvesti mjere u svoje procese sustava upravljanja kvalitetom (vidi 4.4);
   2) vrednovati djelotvornost tih mjera.

Mjere za poduzimanje koraka povezanih s rizicima i prilikama moraju biti razmjerne mogućem utjecaju na sukladnost proizvoda i usluga.

Formalni i neformalni pristup rizicima

Nastavak točke 6.1.

NAPOMENA 1: Mogućnosti za poduzimanje koraka povezanih s rizicima mogu biti: izbjegavanje rizika, preuzimanje rizika kako se ne bi propustila prilika, uklanjanje izvora rizika, mijenjanje vjerojatnosti za rizik ili njegovih posljedica, dijeljenje rizika ili zadržavanje rizika nakon odlučivanja, uz sagledavanje problema.

OVO SE NE MOŽE PROVESTI BEZ FORMALNE METODOLOGIJE

NAPOMENA 2: Prilike mogu dovesti do usvajanja novih postupaka, lansiranja novih proizvoda, otvaranja novih tržišta, obraćanja novim kupcima, uspostave partnerskih odnosa, korištenja novih tehnologija i drugih poželjnih i ostvarivih mogućnosti poduzimanja koraka povezanih s potrebama organizacije i njezinih kupaca.

NEDOPUSTIVO JE ODLUČIVANJE NA TEMELJU RIZIKA BEZ FORMALNE METODOLOGIJE

A.4 Pristup utemeljen na rizicima

. . .

Iako se u 6.1 određuje da organizacija mora planirati mjere za poduzimanje koraka povezanih s rizicima, ne postoji zahtjev za formalne metode upravljanja rizicima ili dokumentirani proces upravljanja rizicima.

. . .

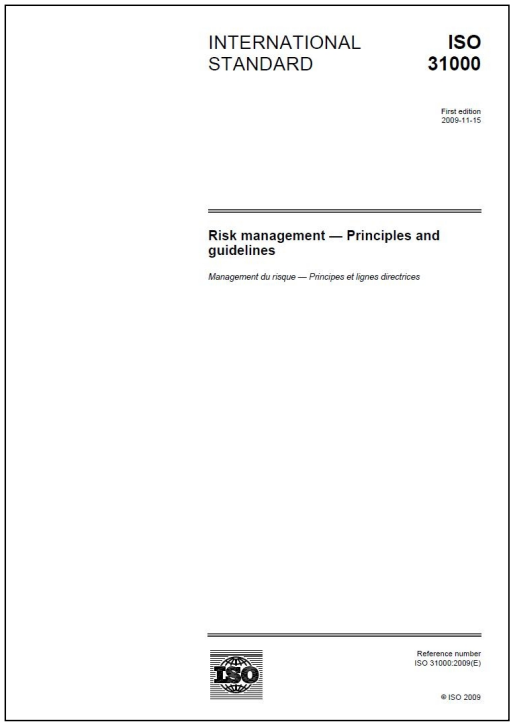
Organizacije mogu odlučiti hoće li ili ne razviti opsežniju metodologiju upravljanja rizicima nego što to zahtijeva ova međunarodna norma, npr. kroz primjenu drugih smjernica ili normi.

. . .

ISO 31000:2009
Risk management – Principles and guidelines

ISO je objavio međunarodnu normu ISO 31000 kojom se definira generički proces upravljanja rizicima za sva područja primjene.

Norma nije obvezna za primjenu – spada u kategoriju smjernica. Međutim, u praksi se pokazala kao sveobuhvatna i prihvaćena od strane apsolutne većine koji se bave sistemski problemima upravljanja rizicima.


INTERNATIONAL STANDARD

ISO 31000

First edition 2009-11-15

Risk management — Principles and guidelines

Management du risque — Principes et lignes directrices

Reference number ISO 31000:2009(E)

© ISO 2009

Principi upravljanja rizicima

(Prema ISO 31000)

a) Upravljanje rizikom stvara vrijednost
b) Upravljanje rizikom je integralni dio organizacijskih procesa
c) Upravljanje rizikom je dio donošenja odluka
d) Upravljanje rizikom se eksplicitno odnosi na neizvjesnost
e) Upravljanje rizikom je sistematsko, strukturirano i blagovremeno
f) Upravljanje rizikom se temelji na najbolje dostupnim informacijama
g) Upravljanje rizikom je prilagođeno danoj situaciji
h) Upravljanje rizikom vodi računa o ljudskim i kulturnim faktorima
i) Upravljanje rizikom je transparentno i uključivo
j) Upravljanje rizikom je dinamično, ponovljivo i osjetljivo na promjene
k) Upravljanje rizikom olakšava kontinuirano poboljšanje i unaprjeđenje organizacije

Definicija rizika prema ISO GUIDE 73:2009

Rizik je efekt neizvjesnosti za ciljeve

NAPOMENA 1 pod efektom se smatra odstupanje od očekivanog — pozitivno i/ili negativno.

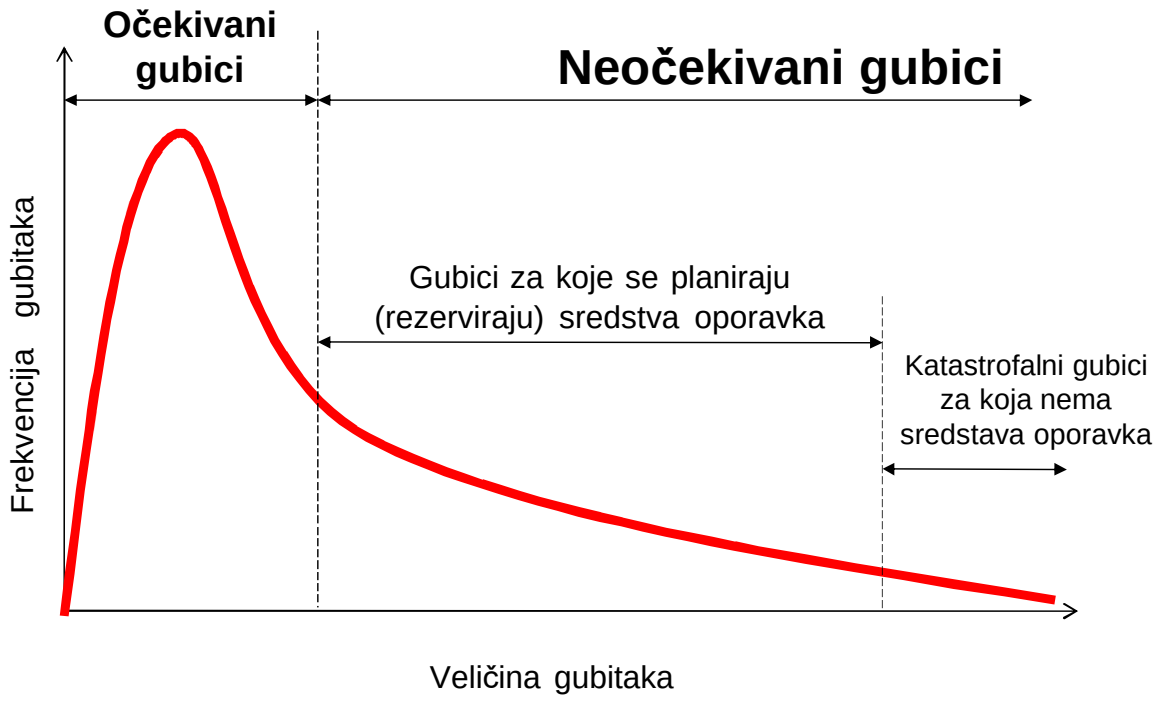
NAPOMENA 2 ciljevi mogu imati različite aspekte (npr. financijske, na zdravlje i sigurnost, ciljevi zaštite okoliša, informacijska sigurnost, itd.) i mogu imati različite razine (npr. strateški, organizacijski, projektni, produkata, procesni).

NAPOMENA 3 rizik je često karakteriziran u odnosu na kombinaciju potencijalnih događaja i posljedica koje se mogu dogoditi.

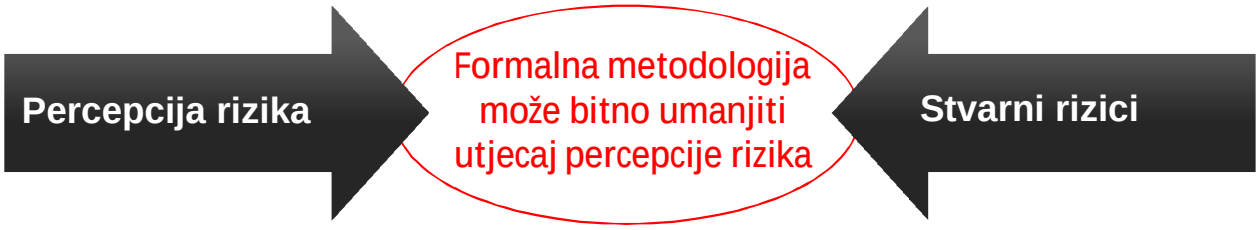
NAPOMENA 4 rizik je često izražen u iznosima kombinacije posljedice događaja (uključujući promjene uvjeta) i pridruženog ponavljanja (frekvencije) događaja.

NAPOMENA 5 neizvjesnost je stanje, čak i djelomičnog, nedostatka informacija o događajima, posljedicama i frekvenciji.

Distribucija frekvencije pojave i veličine gubitaka

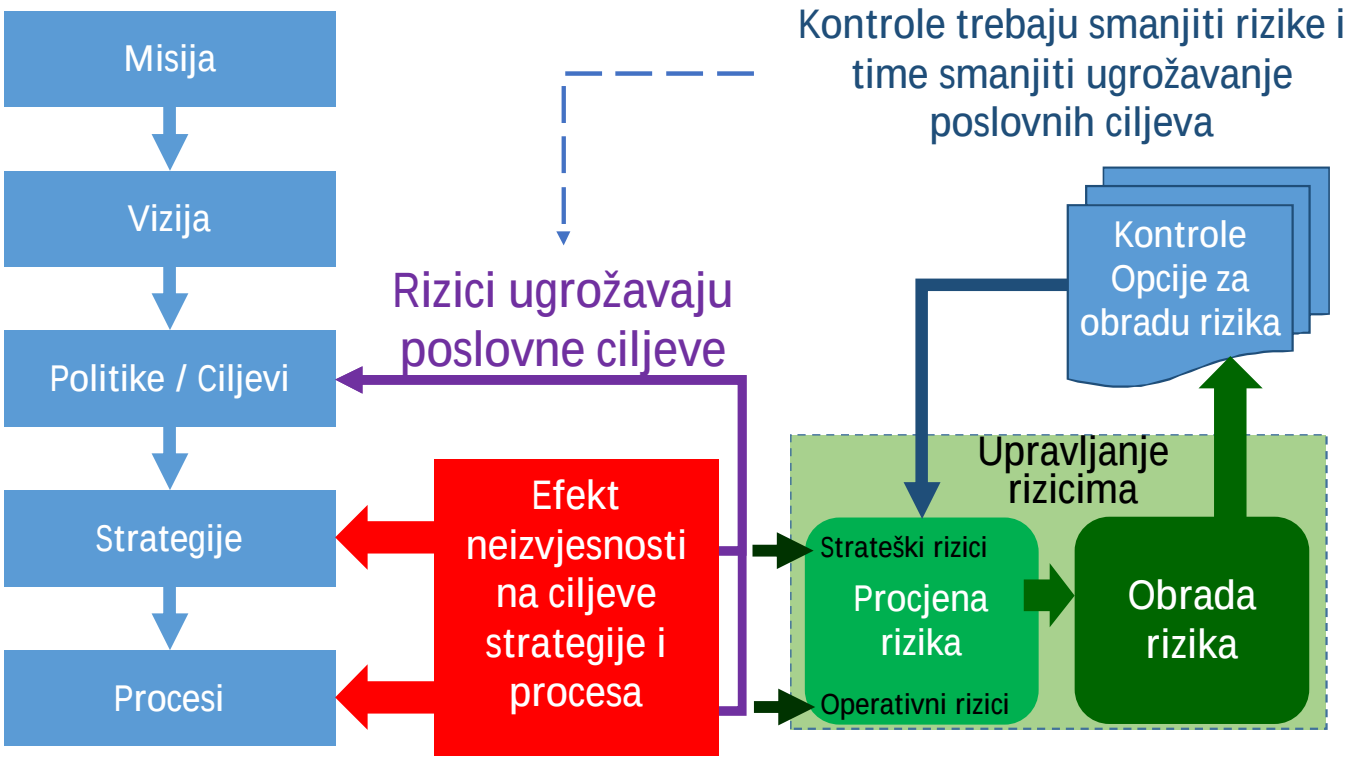


Percepcija rizika



Transportna sredstva	Poginulih putnika Na 100 milijuna putnika-kilometara (2001-2002)
Motocikl	13.8
Pješačenje	6.4
Bicikl	5.4
Automobil	0.7
Autobus	0.07
Avion (civilni)	0.035

Upravljanje sistemima, rizici i kontrole



Tipovi upravljanja rizicima u organizaciji

Glavni zadatak upravljanja rizicima je stvaranje sigurnosnog okruženja.

BASEL II: definicija operativnog rizika

Operativni rizik je definiran kao rizik od gubitka koji proističe iz neadekvatnih ili neuspješnih internih procesa, ljudi i sistema ili iz vanjskih događaja.

Ova definicija uključuje zakonski rizik ali isključuje strateški i reputacijski rizik.

Zakonski rizik uključuje, ali nije ograničen na, izloženost globama, kaznama, kaznenim odštetama proisteklim iz aktivnosti supervizije kao i iz privatnih izvršenja.

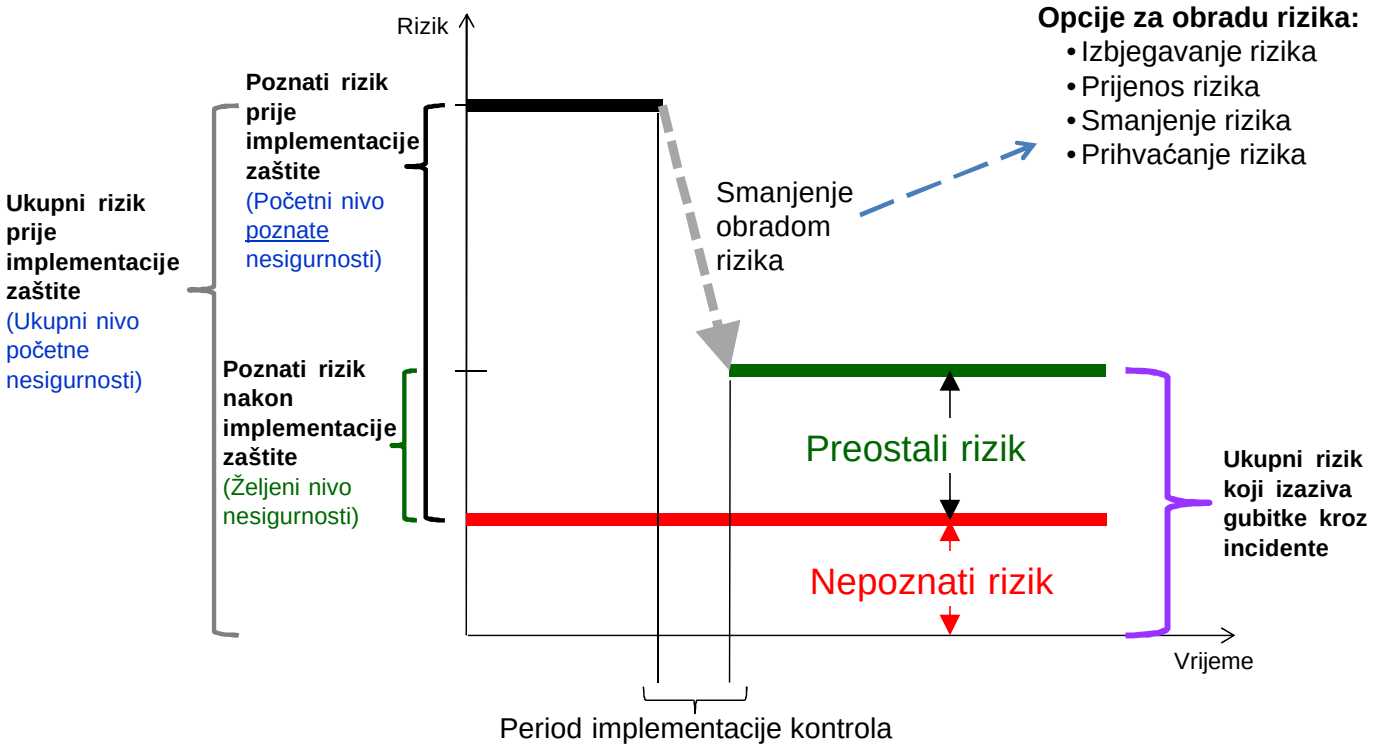
Pojam "operativni rizik" – prvi puta je korišten 1995. godine (bankrot Baringsa)

BASEL II (2004) je sporazum koji se odnosi prvenstveno na banke i financijske institucije u smislu rangiranja prema nivou poslovnih rizika.

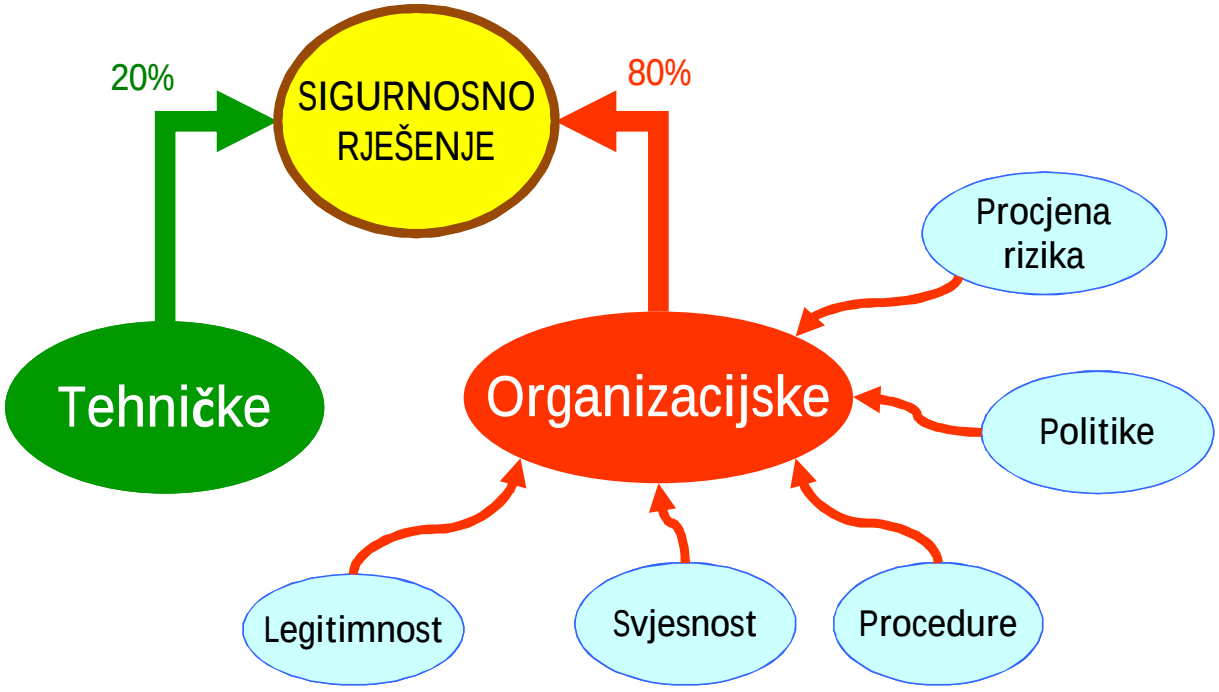
Operativni rizici po vrstama uzroka (prema BASEL II)

Uzrok	Kategorija događaja
Ljudski faktor	Neovlaštene aktivnosti Krađe i prevare zaposlenih Unutrašnji sistem sigurnosti Odnosi prema zaposlenima Različitost i diskriminacija Ne odgovarajuća poslovna ili tržišna praksa
Procesi	Sigurnost radnog okruženja Prikladnost, transparentnost i povjerljivost Greške u proizvodima i uslugama Selekcija, sponzorstvo i izloženost prema klijentu Savjetodavne aktivnosti Nezgode i opća sigurnost Upravljanje procesima, obuhvaćanje i izvršenje transakcija Nadzor i izvještavanje Prijem klijenata i adekvatnost dokumentacije
Sistemi	Neadekvatnost, neefikasnost, loše funkcioniranje ili pad IT sistema
Eksterni faktori	Krađe i prijevare (od strane trećih lica) Vanjski sistem Sigurnosti Druge namjerne aktivnosti Prirodne nepogode Katastrofe prouzrokovane ljudskim faktorom Politički i zakonski rizik (Javne usluge/informacije) neraspoloživost dobavljača Poslovni partneri Prodavači i dobavljači

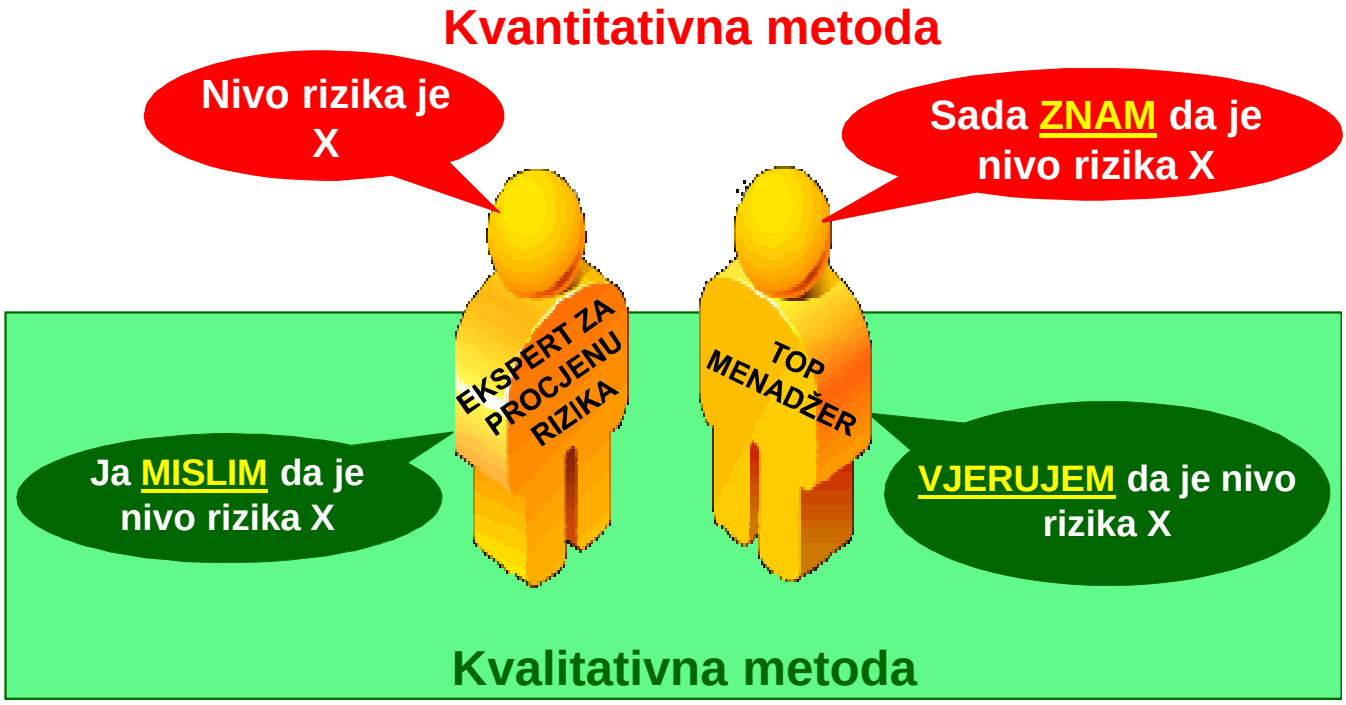
Koncepcija upravljanja rizicima



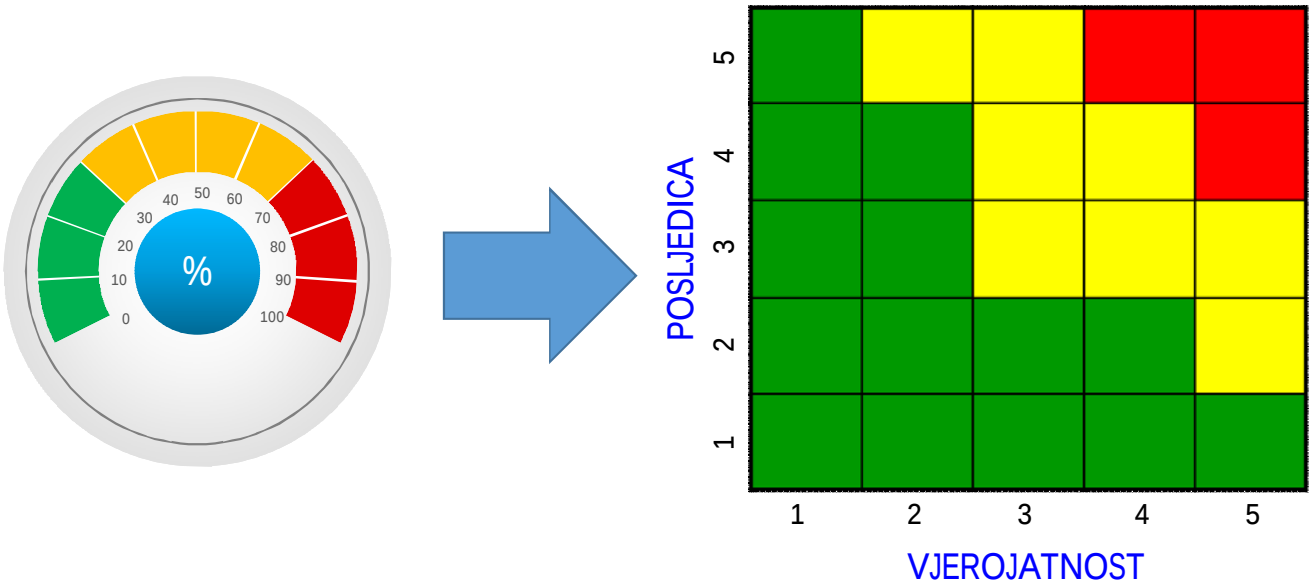
Komponente sigurnosnog rješenja



Razlika između kvantitativne i kvalitativne metode procjene rizika



Rangiranje rizika – POLITIKA SIGURNOSTI KOMPANIJE



Rang rizika → Matrica prihvatljivosti rizika

Koja sigurnosna politika pruža veću poslovnu sigurnost: A ili B?

5	10	15	20	25
4	7	12	16	20
3	6	9	12	15
2	4	6	8	10
1	2	3	4	5

A

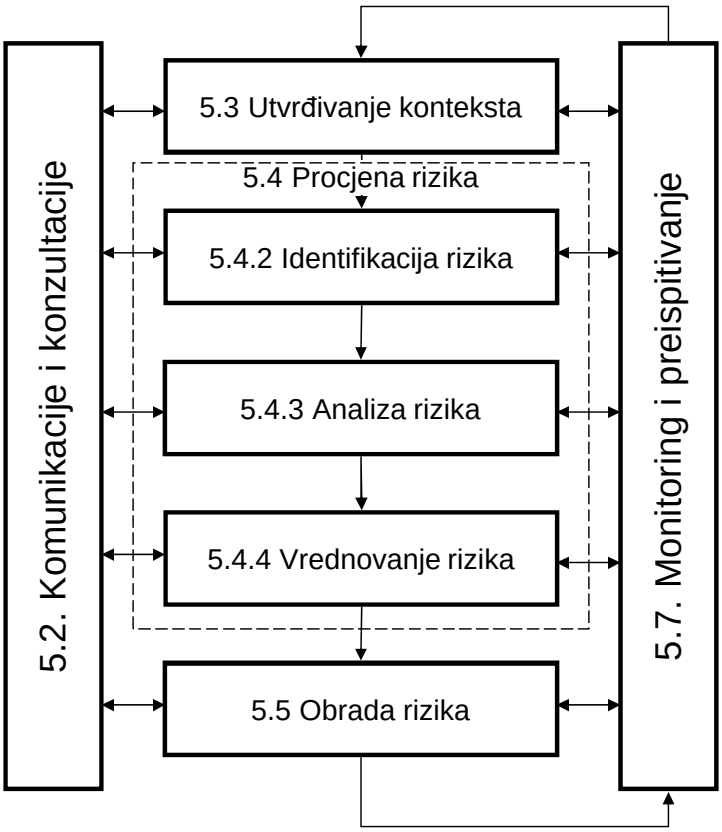
5	10	15	20	25
4	7	12	16	20
3	6	9	12	15
2	4	6	8	10
1	2	3	4	5

B

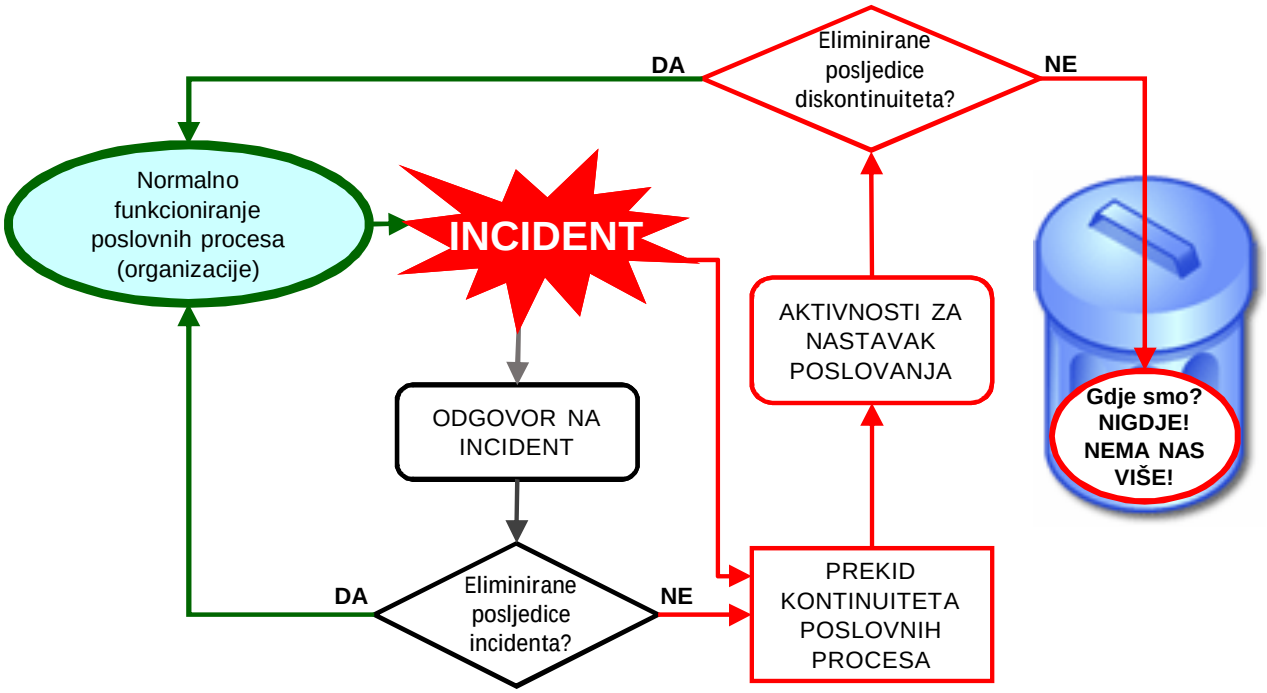
Prihvatljivi rizici

Neprihvatljivi rizici

Procedura upravljanja rizicima prema ISO 31000:2009



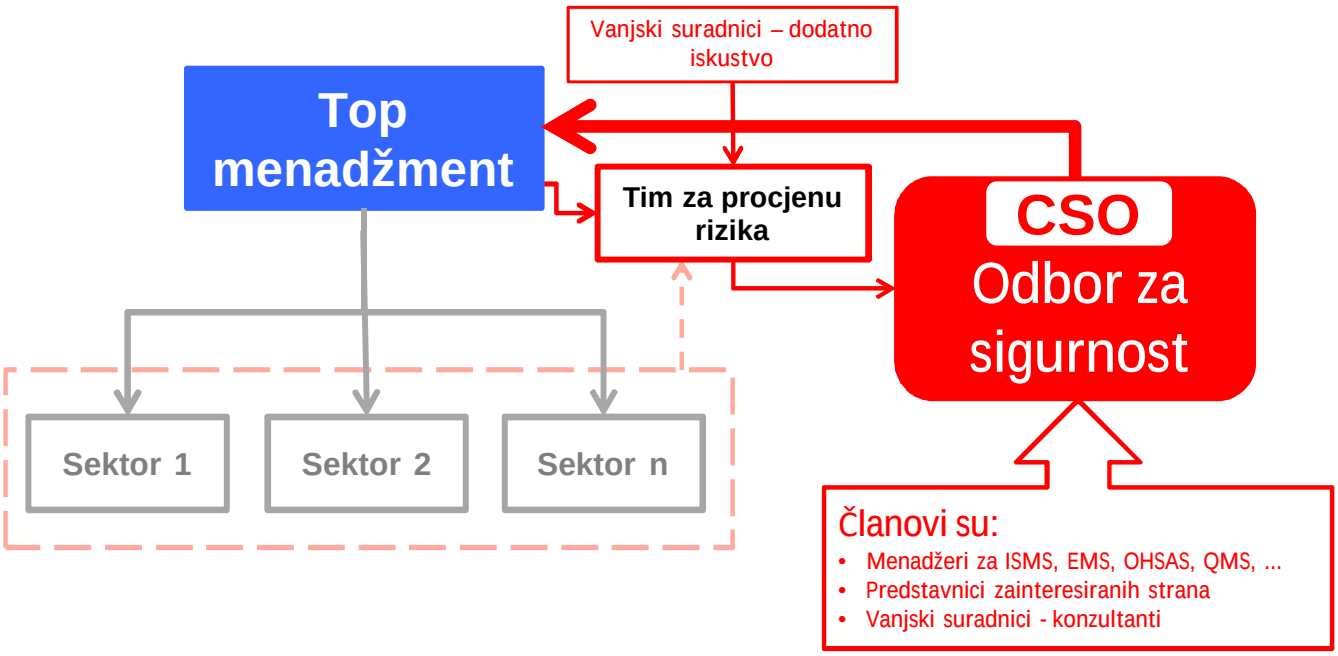
Mehanizam djelovanja incidenata na poslove procese



Svaki incident ima tendenciju da preraste u katastrofu.
Svaki incident može nositi disciplinsku, pa i krivičnu odgovornost.

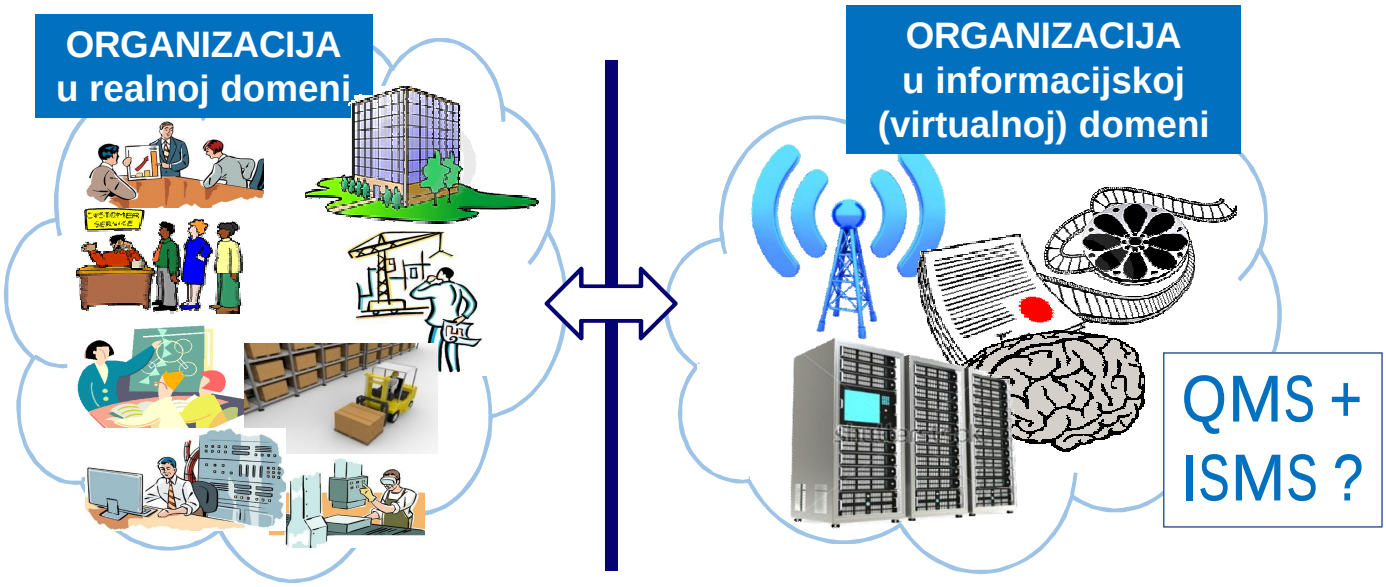
Kako se nositi s rizicima u organizaciji i tko se treba brinuti o njima?

Integracija sigurnosti u kompaniju



CSO (Chief Security Officer) – je najviša izvršna korporacijska funkcija odgovorna vrhovnoj upravi za sigurnost. CSO je direktno odgovoran za identifikaciju, razvoj, implementaciju i održavanje procesa sigurnosti kroz postupke smanjivanja rizika, odgovore na incidente, smanjenje izloženosti svim oblicima rizika, uspostavu politike i procedura sigurnosti.

Gdje je SUK? U realnoj ili virtualnoj domeni?



Svako djelovanje, aktivnosti, planiranje, odlučivanje i upravljanje u kompaniji se provodi ISKLJUČIVO na temelju informacija (generiranih, obrađivanih, spremljenih i distribuiranih) unutar informacijske domene. Pitanje:

KAKO IMATI POVJERENJE U ORGANIZACIJU I NJEN SUK AKO NEMA IMPLEMENTIRANU I INFORMACIJAKU SIGURNOST ?

Zaključak

Ključna novost i doprinos ISO 9001:2015 za veći značaj SUK-a u organizaciji je uvođenje pristupa utemeljenom na rizicima.

Ne optimalni procesi i ostale ne optimalnosti su problem i teškoće za organizaciju, ali incidenti u nekontroliranoj neizvjesnosti su realna i očekujućaKATASTROFA.

IZAZOVI U PRIMJENI NORME ISO 9001:2015