UPRAVLJANJE RIZICIMA PREMA ISO 31000

TEMELJNA NORMA ZA SVE ISO SUSTAVE UPRAVLJANJA

Dr.sc. Zdenko Adelsberger
BlueField d.o.o., Zagreb, HR
zdenko@bluefield.hr
www.bluefield.hr

Predavanje u HDK, Zagreb
14.04.2015.

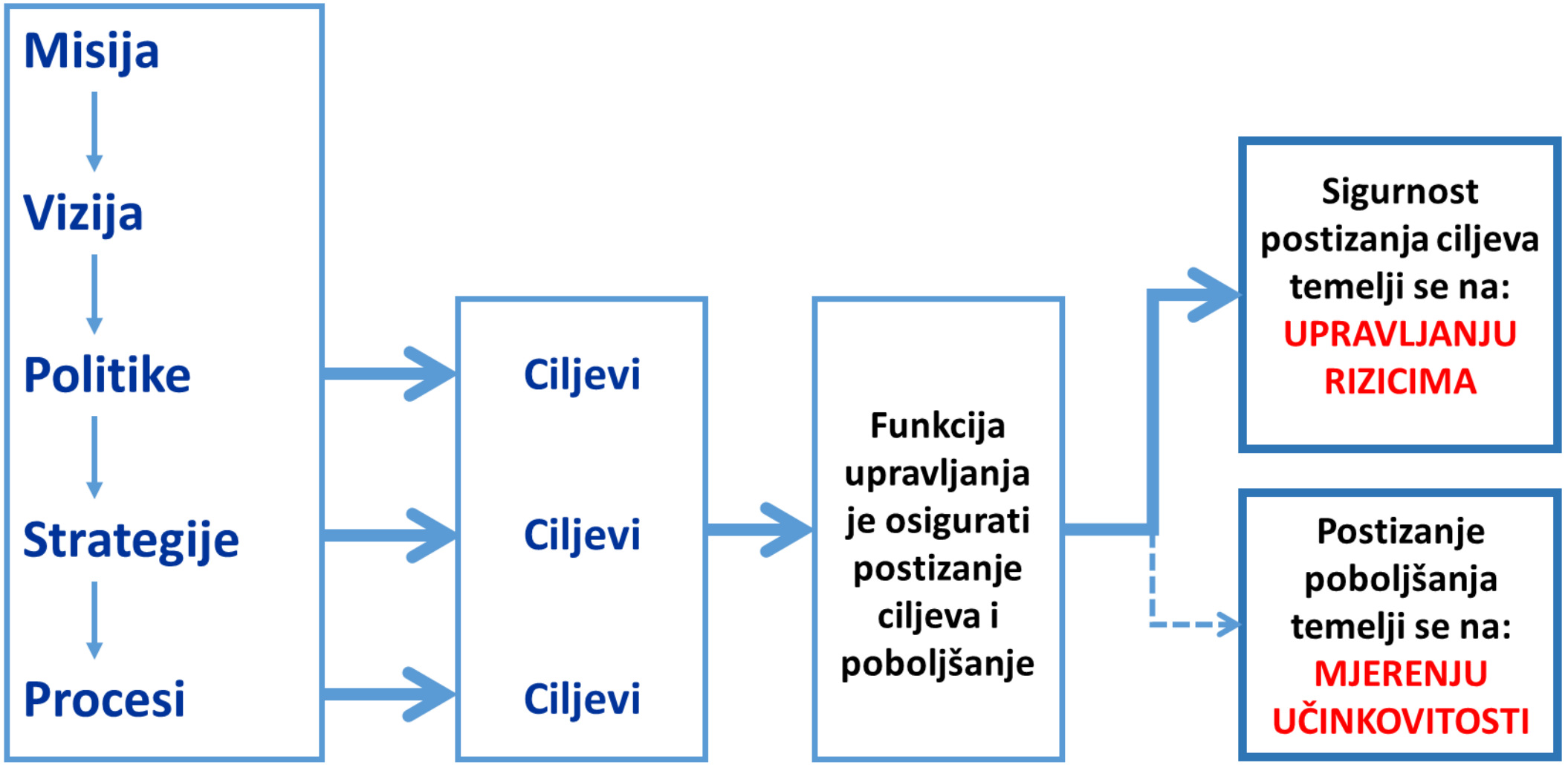
Teme

- Uvod: Pojam rizika i njegovo značenje za sustave upravljanja prema ISO normama
- Norma **ISO 31000:2009** za upravljanje rizicima
- Serija smjernica **ISO Guide 73:2009**, **IEC 31010:2009**, **ISO/TR 31004:2013**
- Praktična implementacija zahtjeva upravljanja rizicima u sustave upravljanja
- Primjer integralne koncepcije upravljanja rizicima, odnosno sigurnošću u kompanijama
- Pitanja i odgovori

Primjeri nekih opasnih (rizičnih) situacija

Kroz cjelokupnu povijest ljudi su živjeli, radili, stvarali, proizvodili u nesigurnim okolnostima. **Jedino je sigurno da ništa nije sigurno.**

Elementi sustava upravljanja



Zašto je potrebno upravljati rizicima?

Svrha upravljanja rizicima je povećanje vjerojatnosti da će organizacije ostvariti svoje ciljeve kroz upravljanje prijetnjama i nepovoljnim situacijama, te biti spremne iskoristiti mogućnosti koje se mogu pojaviti.

Što je rizik ?

Rizik je efekt neizvjesnosti za ciljeve.

(Prema ISO 31000:2009)

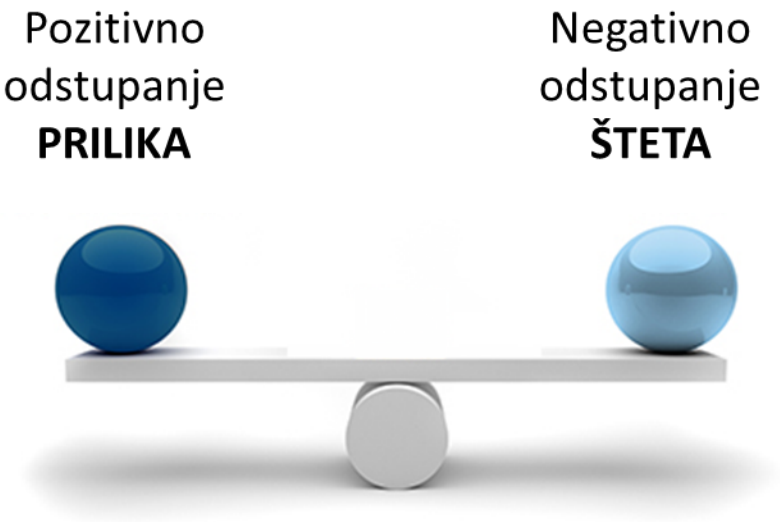
NAPOMENA 1: pod efektom se smatra odstupanje od očekivanog — pozitivno i/ili negativno.

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).

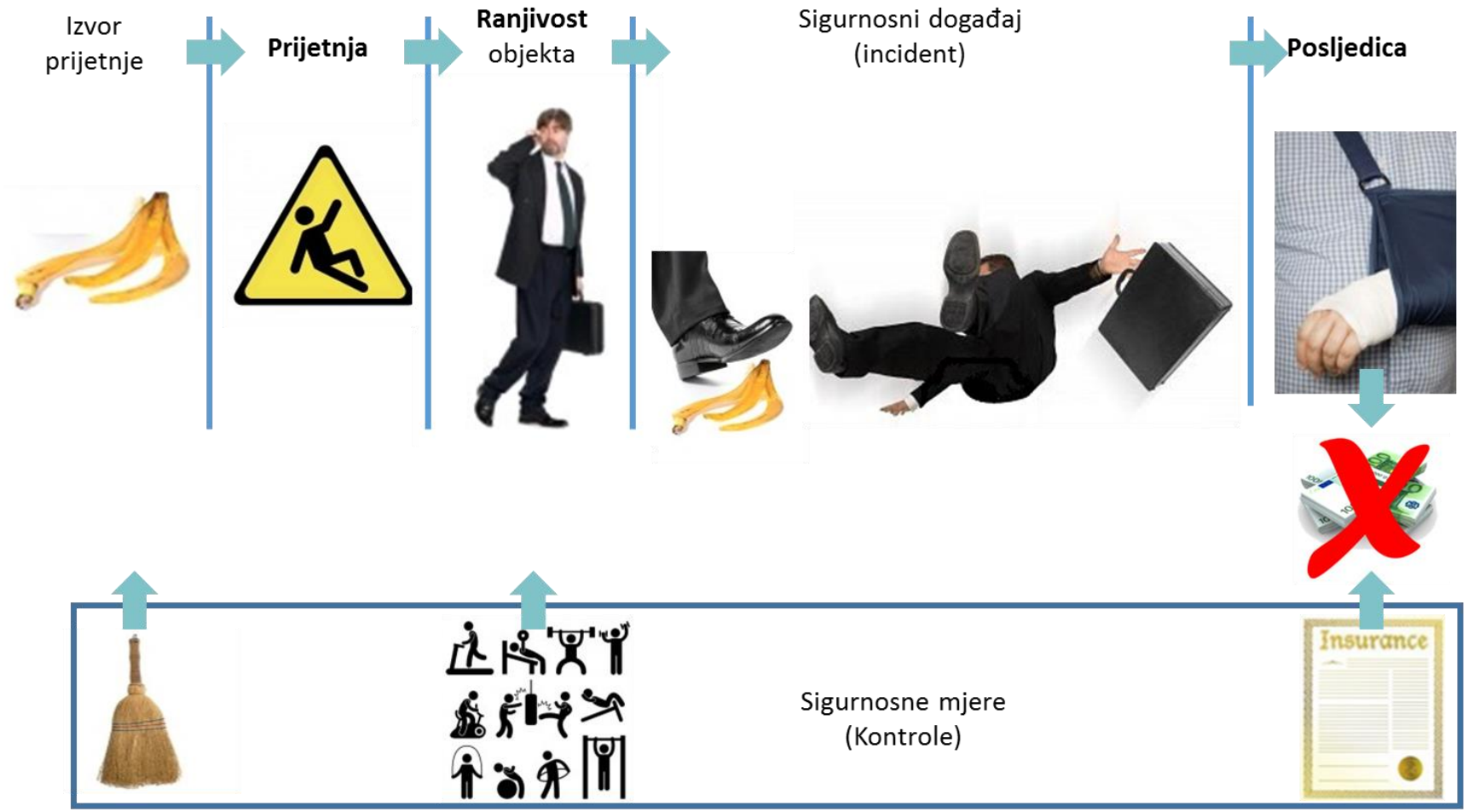
NAPOMENA 3: rizik je često karakteriziran u odnosu na kombinaciju potencijalnih događaja i posljedica koje se mogu dogoditi.

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.

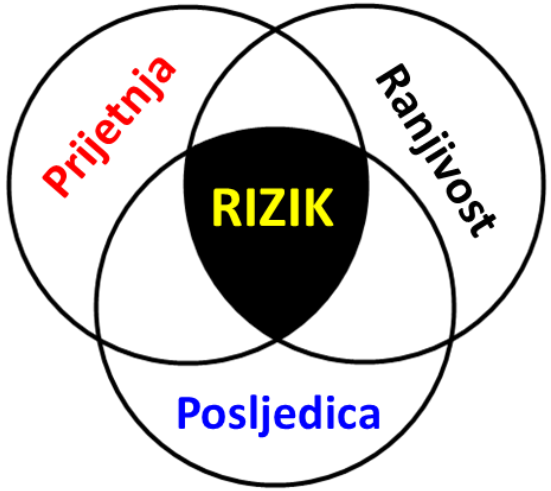


Ilustracija mehanizma rizika

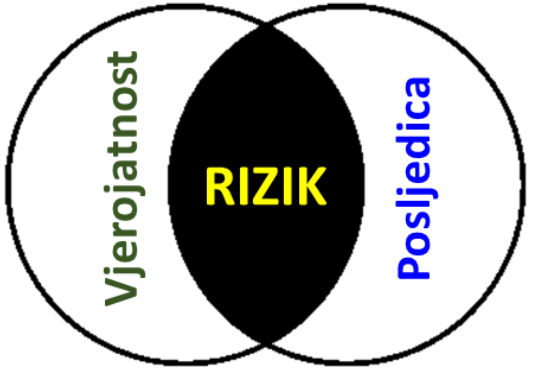


Ako prijetnja iskoristi ranjivost i zbog toga dođe do posljedica, kaže se da je došlo sigurnosnog događaja (incidenta).
Svaka posljedica s točke gledišta upravljanja rizicima, iskazuje se kroz gubitak novca.

Odnos rizika i elemenata koji dovode do rizika



a



b

Rizik = Prijetnja & Ranjivost & Posljedica

Funkcionalna relacija

Rizik = Vjerojatnost & Posljedica

Rizik = Prijetnja * Ranjivost * Posljedica

Matematička relacija

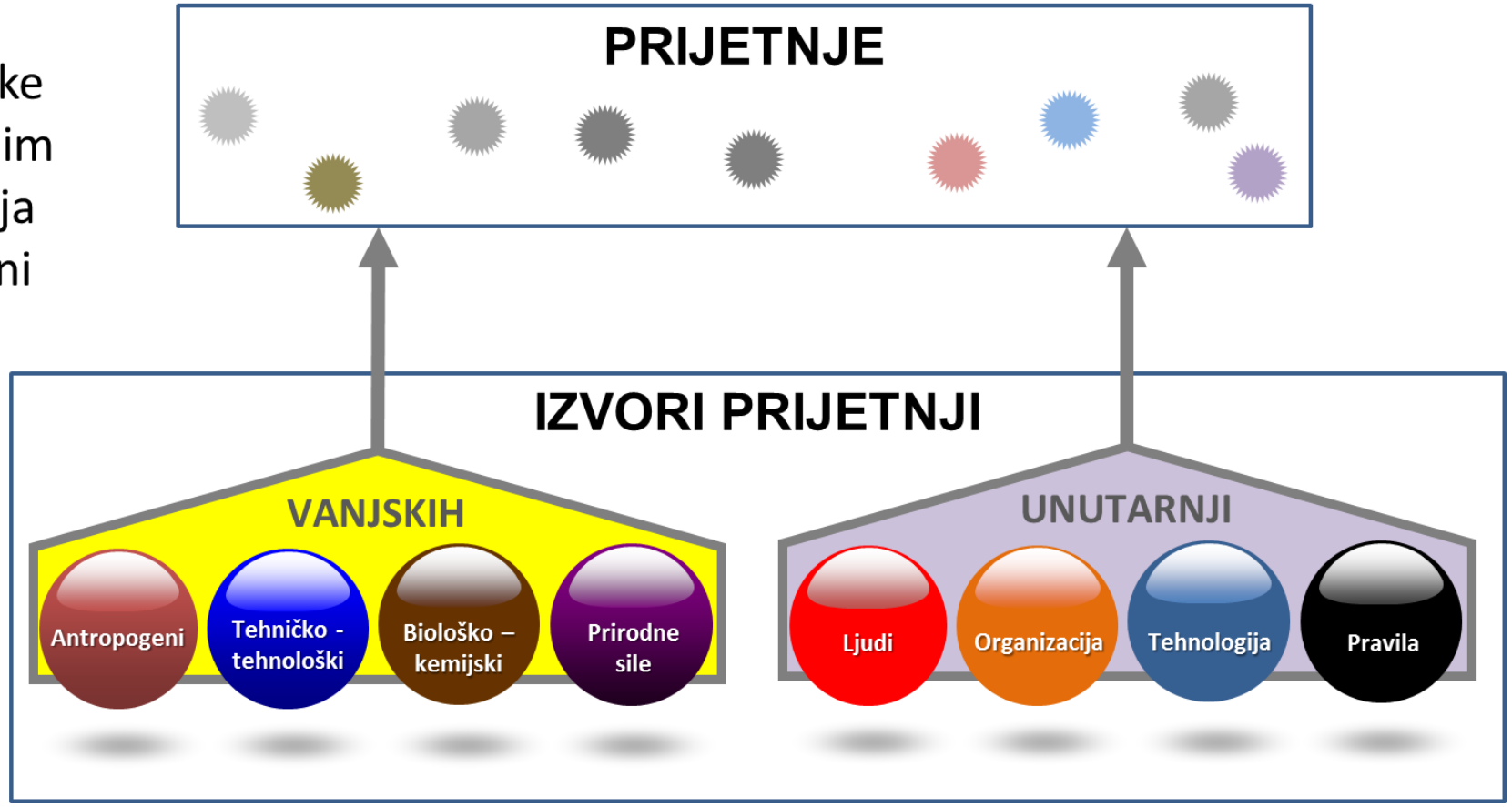
Rizik = Vjerojatnost * Posljedica

Napomena: Vjerojatnost ≠ Prijetnja * Ranjivost

Izvori prijetnji - Prijetnje

Potencijalan uzrok incidenta koji mogu naškoditi ciljevima (funkciji) objekta.

Objekti relevantni za rizike stalno su podložni mnogim vrstama prijetnji. Prijetnja može uzrokovati neželjeni događaj koji može imati štetne posljedice za organizaciju i njena sredstva.
Prijetnje mogu nastati iz **slučajnih** ili **namjernih** izvora / događaja.



Primjeri nekih prijetnji

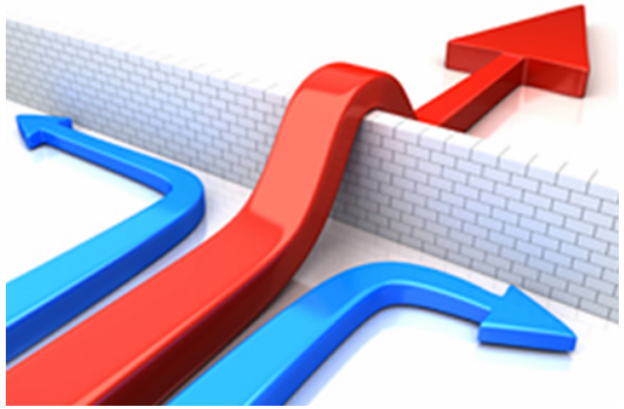
- teroristička djelovanja;
- kvar klimatizacije;
- čestice/prašina iz zraka;
- bombaški napad;
- povreda zakonodavnih ili nadzornih odredaba;
- povreda ugovornih obveza;
- ugrožavanje sredstava;
- ugrožavanje sigurnosti;
- šteta nastala uslijed provjere upada;
- šteta nastala uslijed trećih strana;
- uništenje zapisa;
- uništenje planova kontinuiteta poslovanja;
- propadanje medija;
- katastrofe (prirodne ili od ljudi);
- krivotvorenje zapisa;
- požar;
- poplava;
- prijevara;
- kvar hardvera;
- orkan;
- ilegalni uvoz/izvoz softvera;
- ilegalna upotreba softvera;
- industrijska akcija;
- curenje informacija;
- slučajevi informacijske sigurnosti;
- presretanje;
- ometanje;
- prekid poslovnih aktivnosti i procesa;
- munja;
- gubitak zapisa;
- gubitak usluga;
- greška održavanja;

Ranjivost

Ranjivosti su sigurnosne slabosti povezane sa imovinom organizacije.

Sama po sebi, ranjivost ne nanosi štetu, to je samo stanje ili niz stanja koje mogu prijetnji dozvoliti uzrokovanje štete na imovini ili poslovima koje ta imovina obavlja. Utvrđivanje ranjivosti bi trebalo odrediti slabosti koje se odnose na imovinu u:

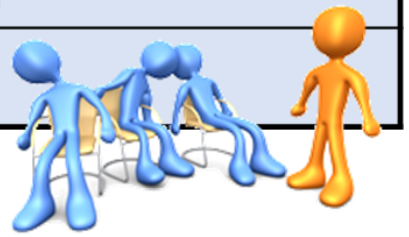
- fizičkom okruženju;
- kadrovskim, upravnim i administrativnim postupcima i kontrolama; poslovnim postupcima i uslugama koje pružaju;
- hardveru, softveru ili komunikacijskim uređajima i opremi.



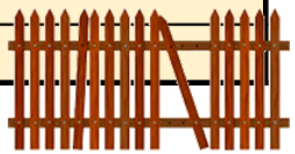
Ranjivosti uvijek treba promatrati vezano za prijetnje, jer ranjivost bez prijetnje, kao i prijetnja bez ranjivosti nema nikakvog značenja za rizike.

Primjeri nekih ranjivosti

PRIMJERI RANJIVOSTI VEZE ZA LJUDSKE RESURSE	
RANJIVOST	**PRIJETNJA KOJA MOŽE ISKORISTITI RANJIVOST**
Nedovoljno sigurnosno obučavanje	Greška osoblja pratećih funkcija
Nedostatak svjesnosti o sigurnosti	Korisnička greška
Nedostatak mehanizma praćenja	Upotreba softvera na neovlašteni način
Nedostatak politika za ispravnu upotrebu telekomunikacijskih medija i slanje poruka	Upotreba mrežne opreme na neovlašteni način
Neuklanjanje prava pristupa nakon prestanka rada	Neovlašteni pristup
Nikakav postupak koji osigurava povratak sredstava nakon prestanka rada	Krađa
Nemotivirano ili nezadovoljno osoblje	Zloporaba opreme za obradu informacija
Nenadzirani rad vanjskog osoblja ili osoblja koje radi prekovremeno	Krađa



PRIMJERI RANJIVOSTI VEZANIH ZA SIGURNOST OKRUŽENJA	
RANJIVOST	**PRIJETNJA KOJA MOŽE ISKORISTITI RANJIVOST**
Neodgovarajuća ili nebrižna upotreba kontrole fizičkog pristupa zgradama, prostorijama i uredima	Namjerna šteta
Nedostatak fizičke zaštite zgrada, vrata i prozora	Krađa
Lokacija u području podložnom poplavi	Poplava
Nedovoljno održavanje/neispravna ugradnja medija za pohranjivanje	Greška održavanja
Nedostatak rasporeda periodičke zamjene opreme	Propadanje medija za pohranjivanje
Osjetljivost opreme na vlagu, prašinu, prljavštine	Čestice / prašina iz zraka
Osjetljivost opreme na temperaturne promjene	Ekstremne temperature
Nestabilna električka mreža	Njihanje napona



Posljedice

Rezultat interakcije prijetnje i ranjivosti, odnosno stanje kada je prijetnja iskoristila ranjivost i time dovela do pojave štete za organizaciju.

Šteta se uvijek mora izraziti u financijskim iznosima.

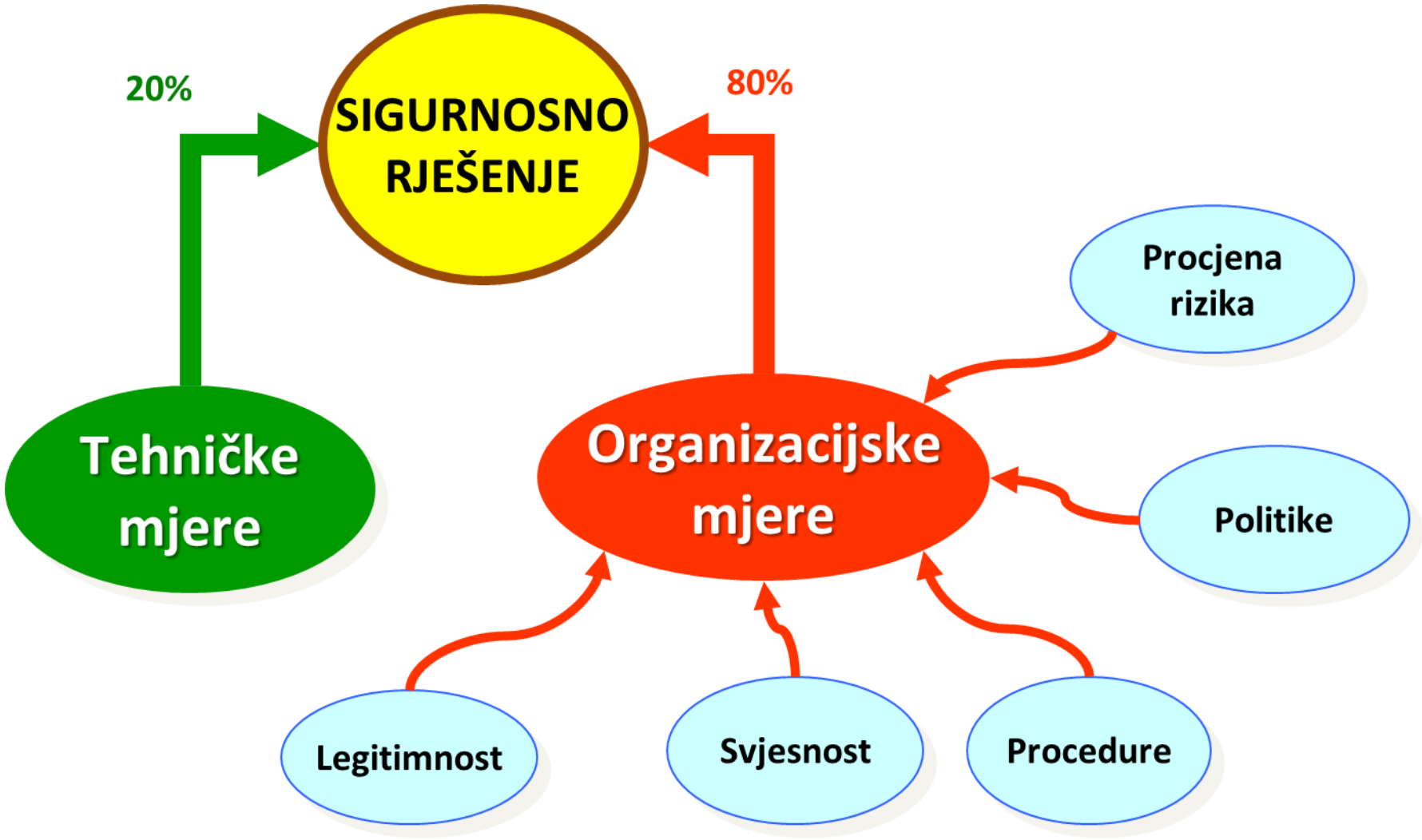
Primjeri posljedica:

- Gubitak profita
- Gubitak ugleda (image)
- Negativni utjecaj na okoliš
- Gubitak podataka
- Gubitak tržišta
- Krađa podataka
- Gubitak C-I-A (za ISMS)
- Itd.

Neki tipovi upravljanja rizicima u kompaniji

Glavni zadatak upravljanja rizicima je stvaranje sigurnosnog okruženja.

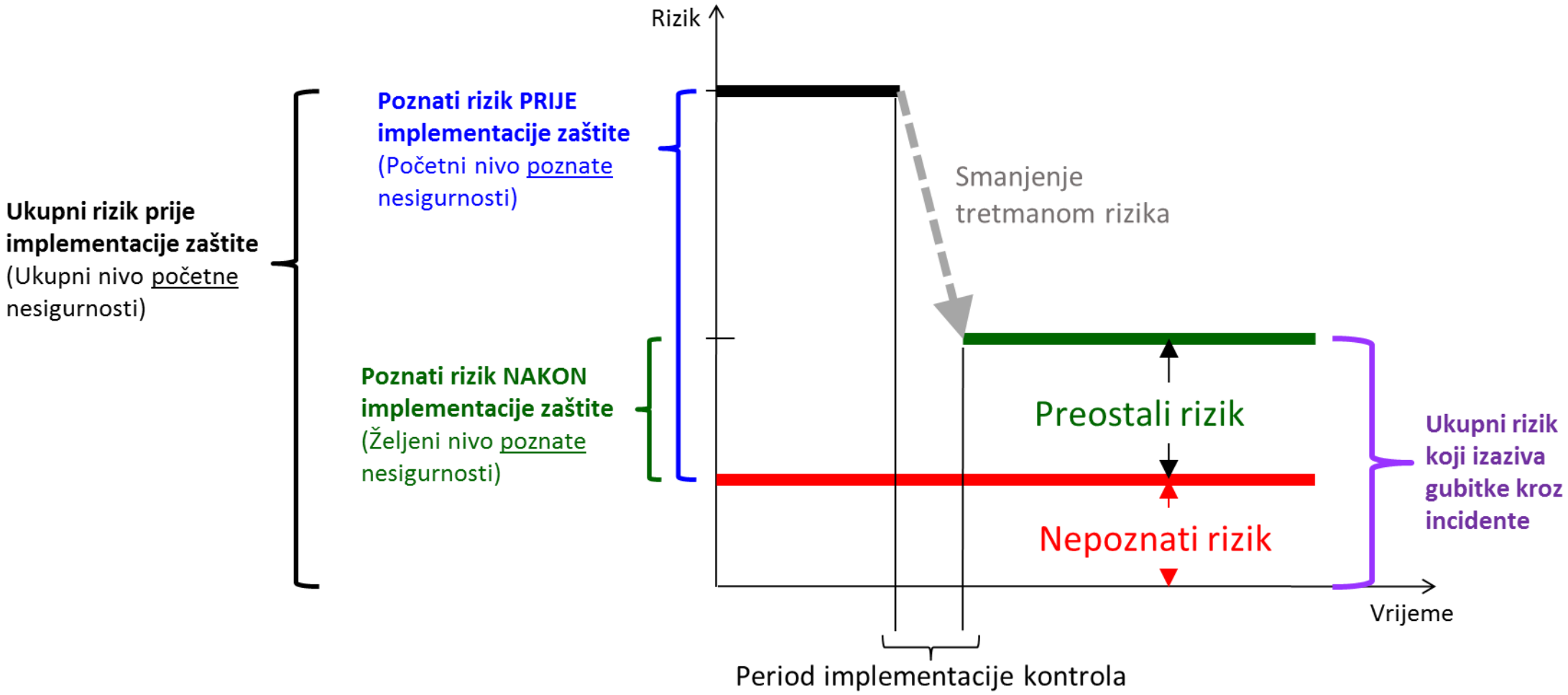
Komponente sigurnosnog rješenja



Razina sigurnosti organizacije

Razina sigurnosti je kompromis između prihvatljivog rizika i investicije u sigurnost.

Koncepcija upravljanja rizicima

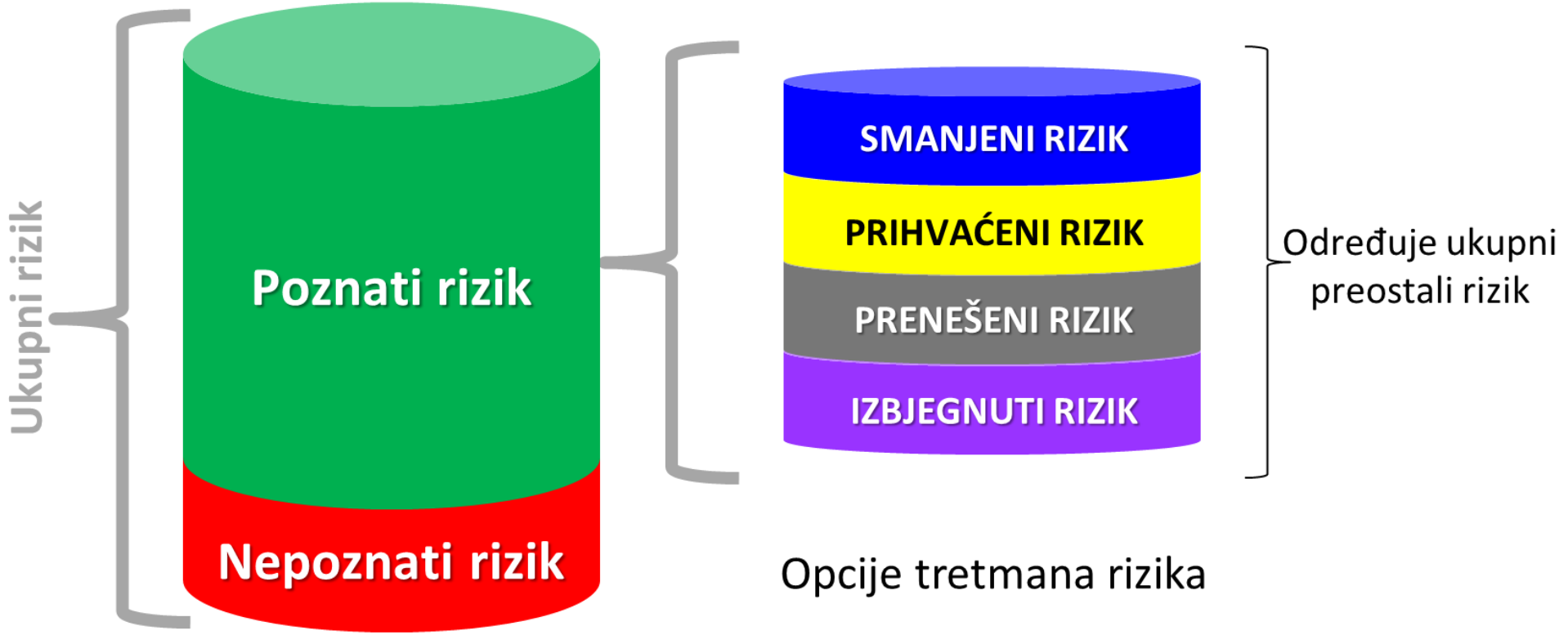


Struktura rizika

(prema ISO Guide 73, ISO 31000)

Premise:

- Svi rizici (prijetnje i/ili ranjivosti) **ne mogu** biti identificirani
- Ne može se neutralizirati svaki rizik

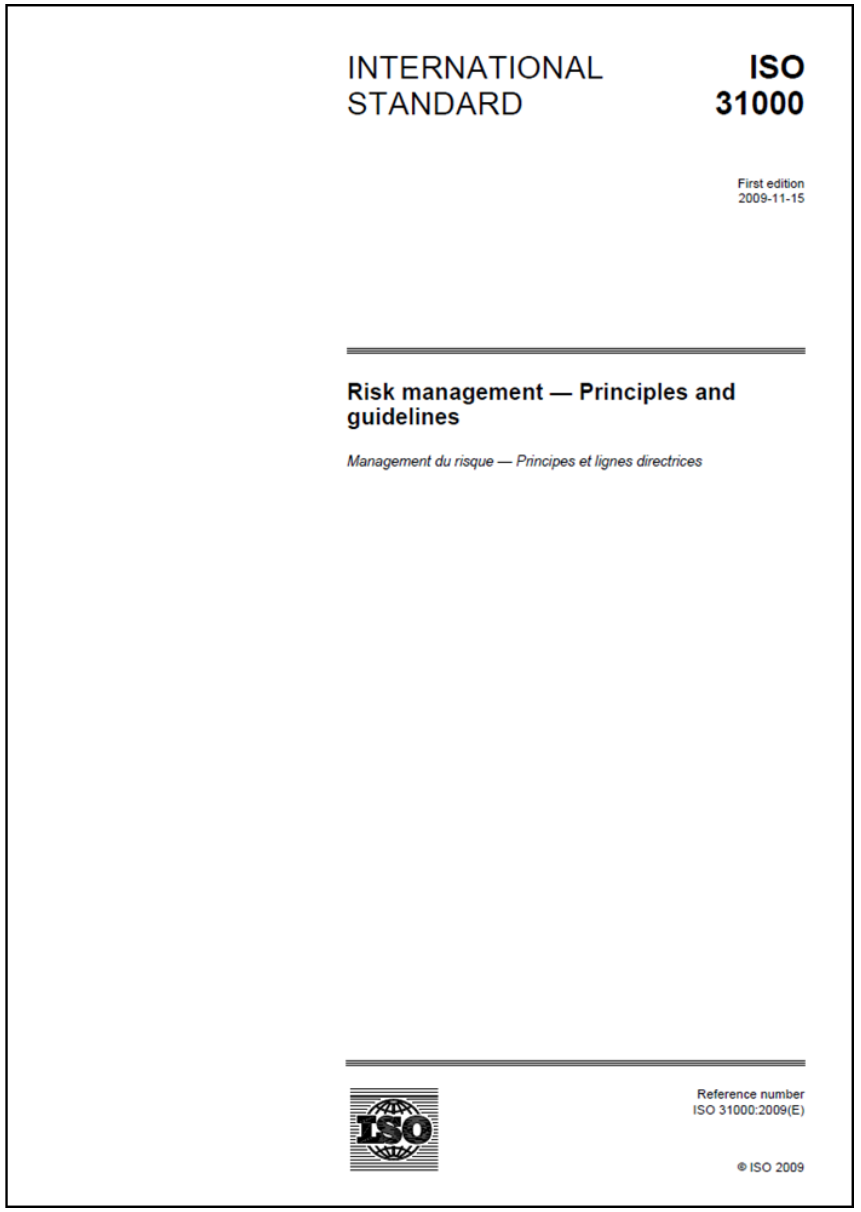


ISO 31000:2009

ISO je objavio međunarodnu normu ISO 31000 kojim se opisuje 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.

Često se sreću neke specifične preporuke u pojedinim područjima za procjenu rizika, ali nakon detaljnijeg pregleda može se pokazati da su u pravilu pojednostavljenje ili nekompletnost sadržaja ove norme.


INTERNATIONAL STANDARD

ISO 31000

First edition
2009-11-15

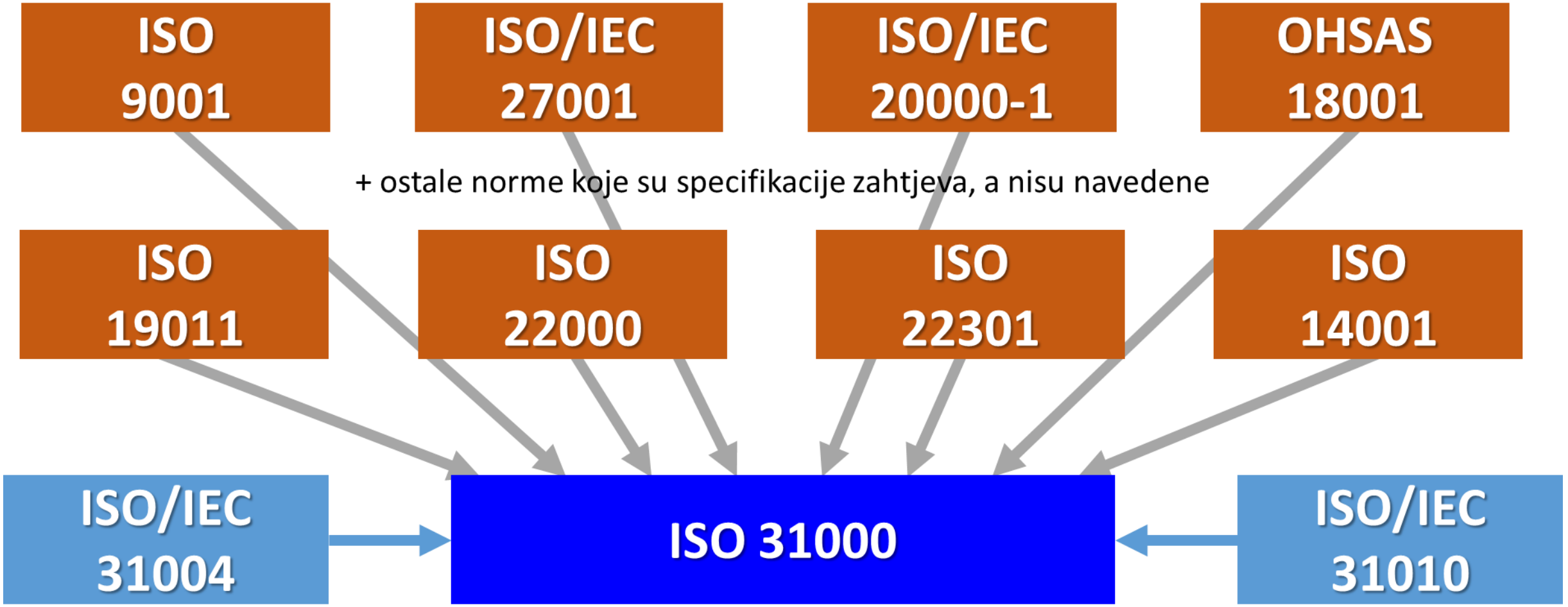
Risk management — Principles and guidelines

Management du risque — Principes et lignes directrices

Reference number
ISO 31000:2009(E)

© ISO 2009

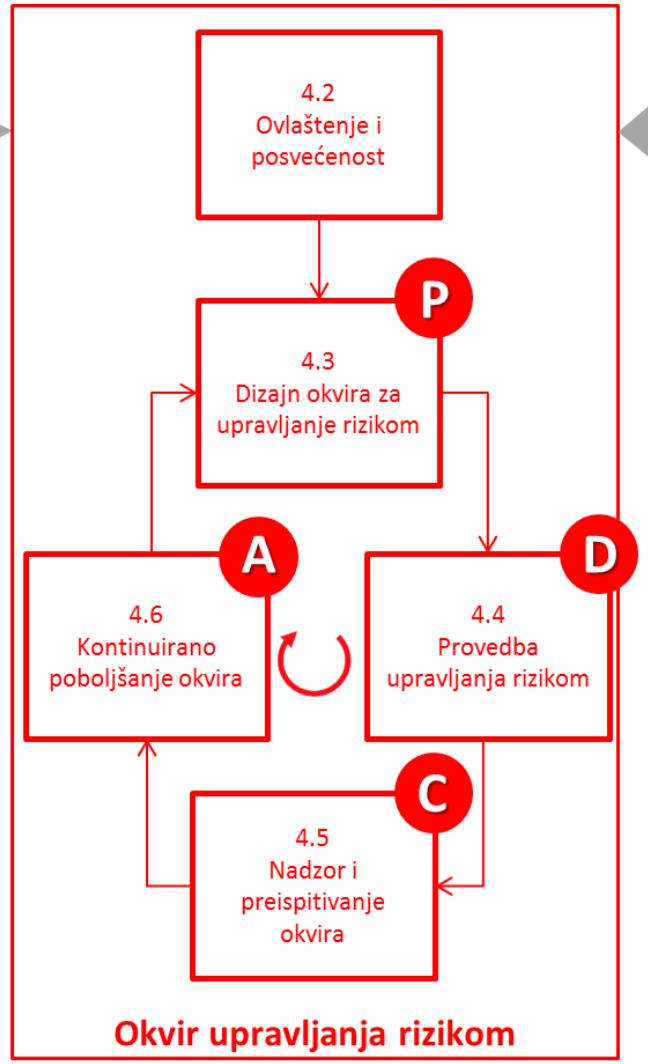
Područje primjene ISO 31000



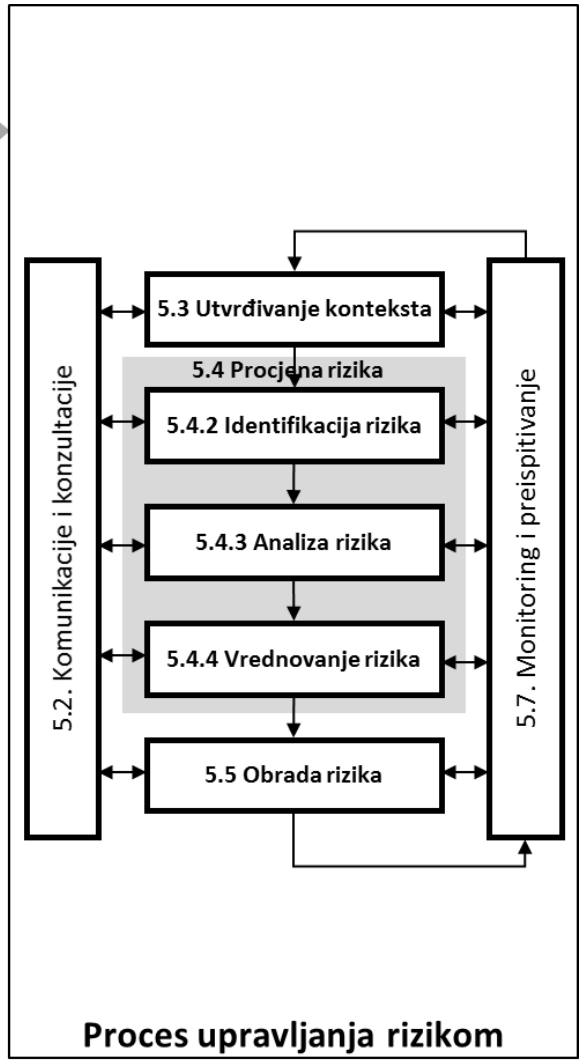
ISO 31000:2009 - KOMPONENTE

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

Principi upravljanja rizikom



Okvir upravljanja rizikom



Proces upravljanja rizikom

Pojmovi procesa za upravljanje rizicima

Komunikacija i konzultacija

Komunikacija i konzultacija s internim i eksternim ulagačima – zainteresiranim stranama, kako je primjereno, na svakom stupnju procesa upravljanja rizikom i razmatranje procesa kao cjeline.

Utvrđivanje konteksta

Utvrđivanje eksternog, internog i konteksta upravljanja rizikom u kojem će se odvijati ostatak procesa. Treba utvrditi kriterije prema kojima će se procjenjivati rizik i definirati struktura analize.

Identifikacija rizika

Identifikacija gdje, kada, zašto i kako bi događaji mogli spriječiti, umanjiti, odložiti ili povećati postizanje ciljeva.

Analiza rizika

Identifikacija i procjena postojećih kontrola. Određivanje posljedica i vjerojatnosti i zatim razine rizika. Ova analiza treba razmotriti područje potencijalnih posljedica i kako bi se one mogle pojaviti.

Ocjena rizika

Usporedba procijenjenih razina rizika s prethodno utvrđenim kriterijima i razmatranje ravnoteže između potencijalnih koristi i nepovoljnih rezultata. To omogućuje donošenje odluka o opsegu i prirodi potrebnih obrada i o prioritetima.

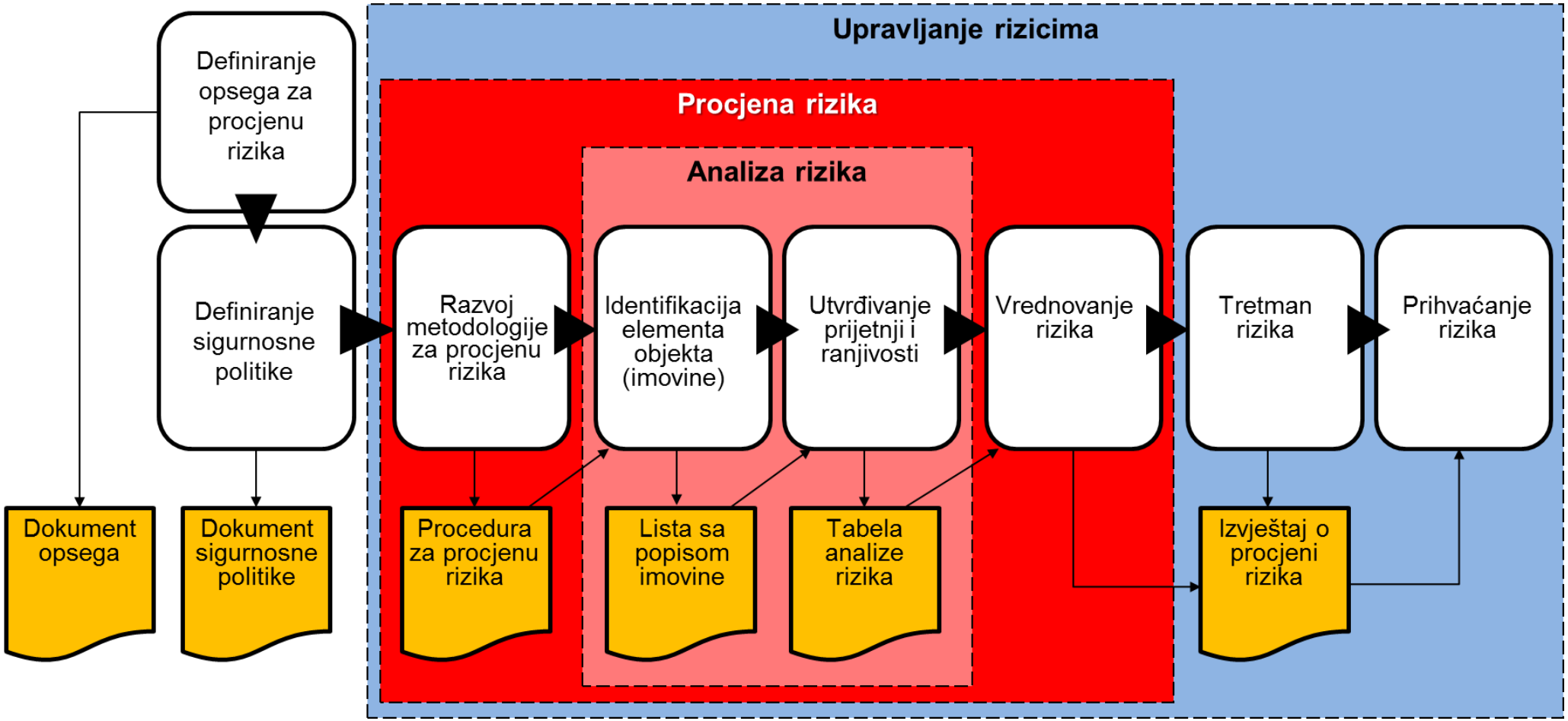
Obrada rizika

Izrada i primjena specifičnih troškovno učinkovitih strategija i akcijskih planova za povećanje potencijalnih koristi i smanjenje potencijalnih troškova.

Praćenje i preispitivanje

Neophodno je pratiti učinkovitost svih koraka procesa upravljanja rizikom. To je važno za neprekidno poboljšavanje. Potrebno je pratiti rizike i učinkovitost mjera obrade kako bi se osiguralo da promjena uvjeta ne mijenja prioritete.

Blok shema faze planiranja (P) upravljanja rizicima prema ISO 31000:2009



Alati za procjenu rizika

(ISO/IEC 31010:2009)

Alati i tehnike	Proces procjene rizika				
	Identifikacija rizika	Analiza rizika			Vrednovanje rizika
		Posljedice	Vjerojatnost	Razina rizika	
Brainstorming					
Structured or semi-structured interviews					
Delphi					
Check-lists					
Primary hazard analysis					
Hazard and operability studies (HAZOP)					
Hazard Analysis and Critical Control Points (HACCP)					
Environmental risk assessment					
Structure "What if?" (SWIFT)					
Scenario analysis					
Business impact analysis					
Root cause analysis					
Failure mode effect analysis					
Fault tree analysis					
Event tree analysis					
Cause and consequence analysis					
Cause-and-effect analysis					
Layer protection analysis (LOPA)					
Decision tree					
Human reliability analysis (HRA)					
Bow tie analysis					
Reliability centred maintenance					
Sneak circuit analysis					
Markov analysis					
Monte Carlo simulation					
Bayesian statistics and Bayes Nets					
FN curves					
Risk indices					
Consequence/probability matrix					
Cost/benefit analysis					
Multi-criteria decision analysis (MCDA)					

Strogo preporučeno

može se koristiti

nije primjenljivo

Metodologije za procjenu rizika

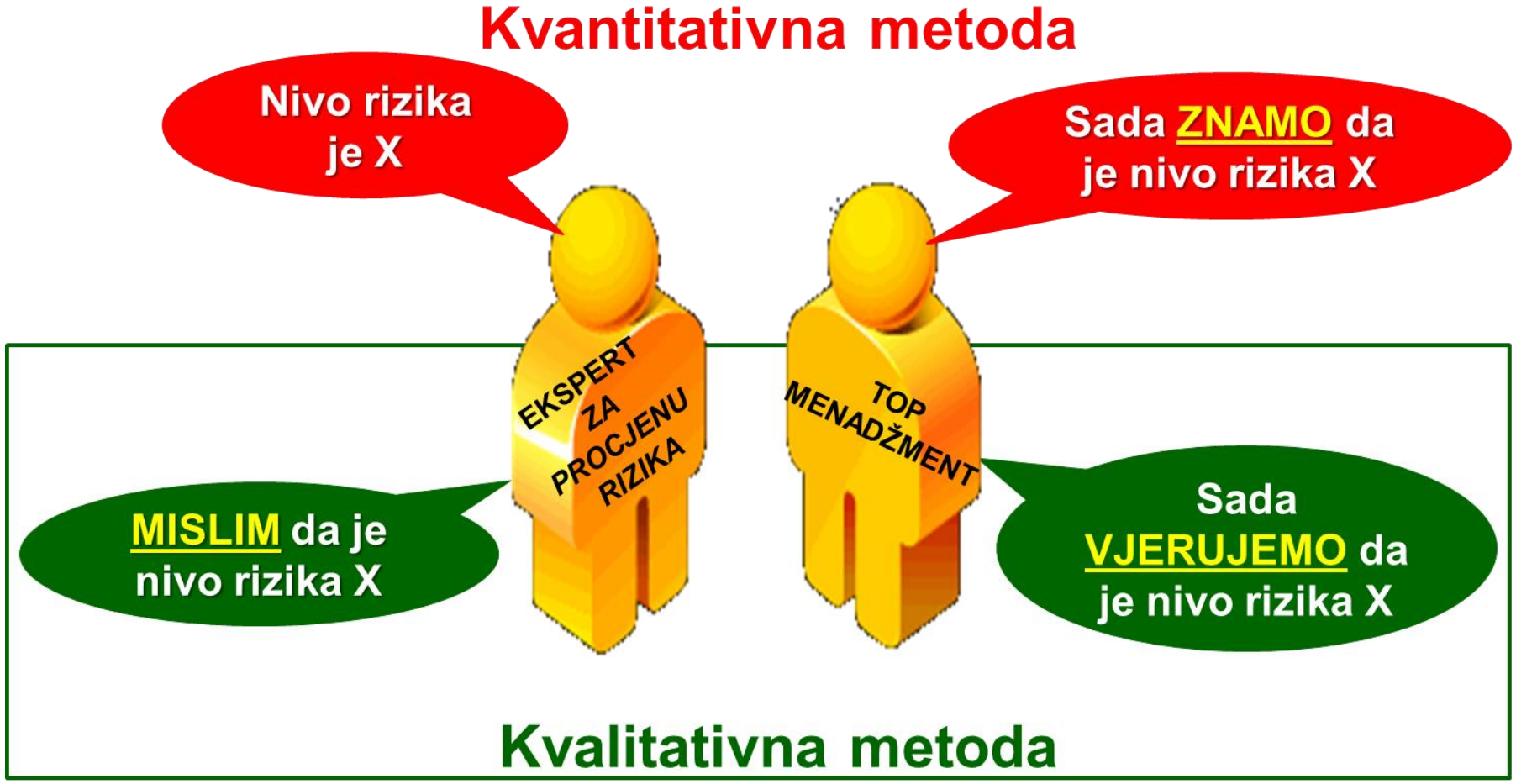
Kvantitativna metoda

Kvantitativna procjena koristi brojčane vrijednosti za posljedice i vjerojatnost (a ne opisne skale kao u kvalitativnoj procjeni), korištenjem podataka iz raznih izvora.
Kvaliteta procjene ovisi od točnosti i potpunosti korištenih brojčanih vrijednosti i valjanosti primijenjenih modela.
Posljedice se mogu procijeniti modeliranjem: rezultata nekog događaja ili niza događaja, ili ekstrapolacijom iz eksperimentalnih studija ili podataka iz prošlosti.
Posljedice se mogu izraziti s obzirom na novčane, tehničke ili humane kriterije učinka, ili neki od drugih kriterija.

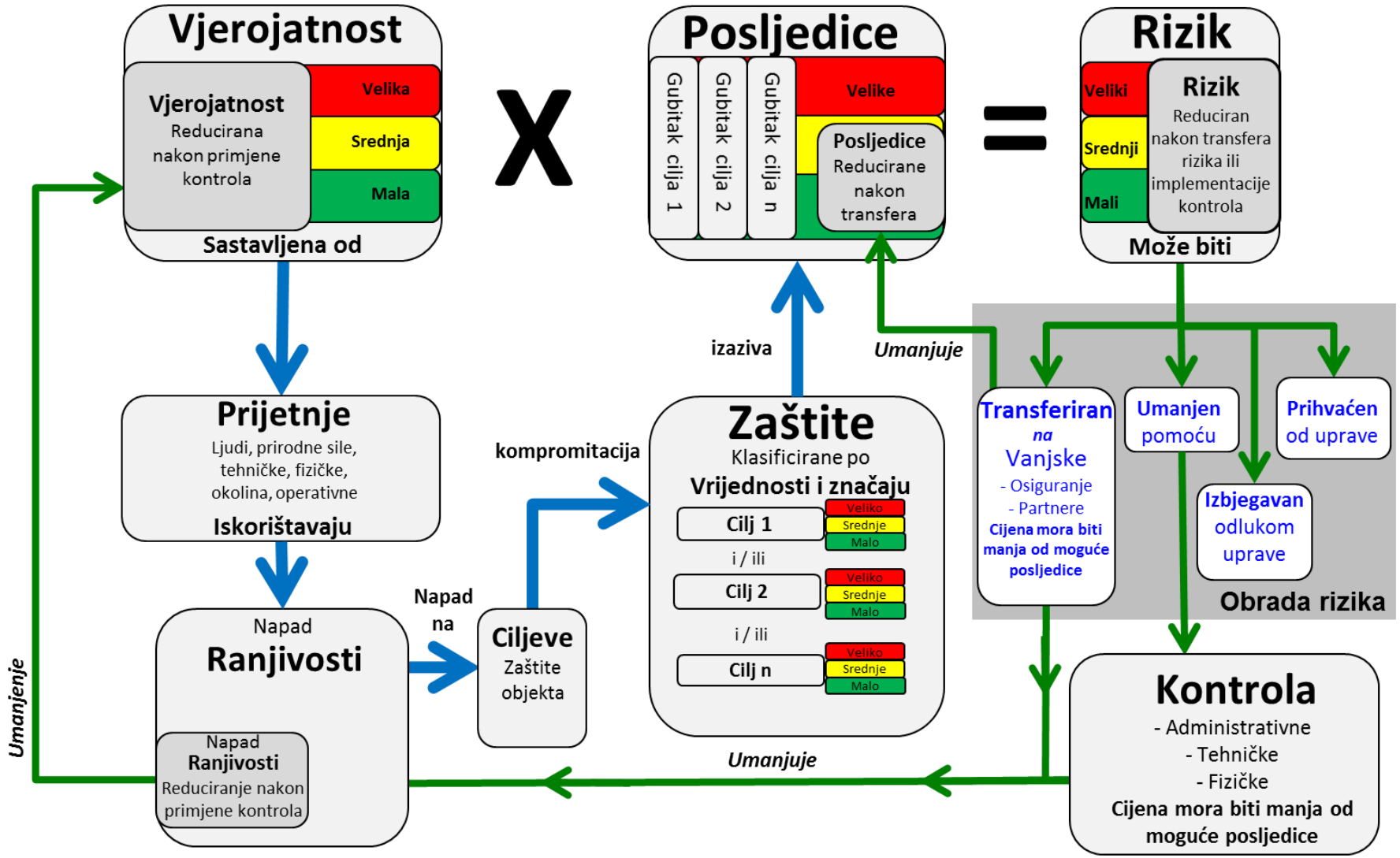
Kvalitativna metoda

Kvalitativna procjena koristi tekst za opisivanje veličine potencijalnih posljedica i vjerojatnosti da će te posljedice nastati. Ove se skale mogu prilagoditi ili podesiti okolnostima i za različite rizike se mogu koristiti različiti opisi. Kvalitativna procjena se može koristiti u slučajevima: kao početna aktivnost za identifikaciju rizika koji zahtijevaju detaljniju analizu; gdje je ova vrsta analize primjerena za donošenje odluka; ili gdje brojčani podaci ili resursi nisu odgovarajući za kvantitativnu procjenu.
Kvalitativnu procjenu treba dopuniti stvarnim informacijama i podacima gdje god su raspoloživi.

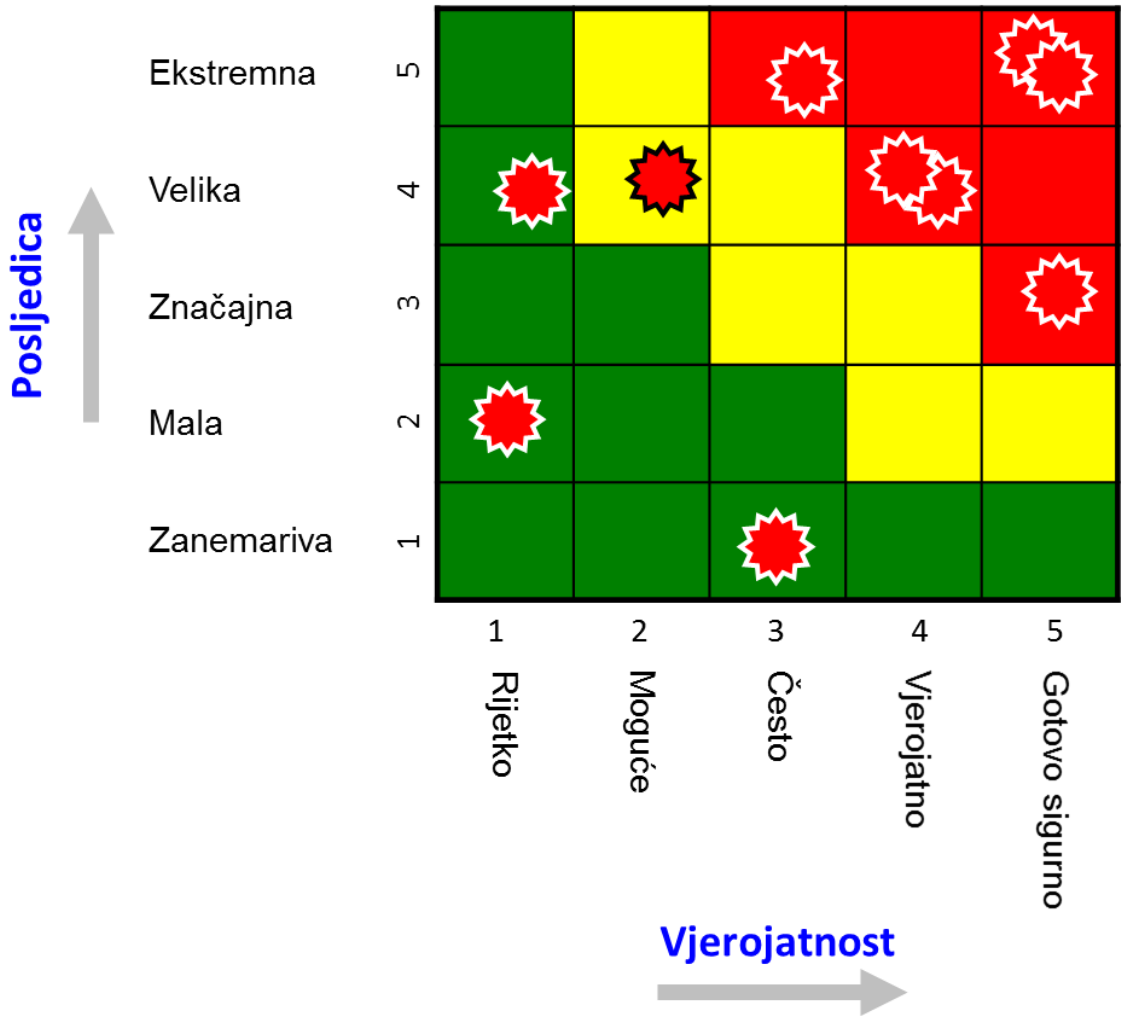
Razlika između kvantitativne i kvalitativne metode procjene rizika



Blok shema kvalitativne procjene rizika



Distribucija rizika u matrici rizika

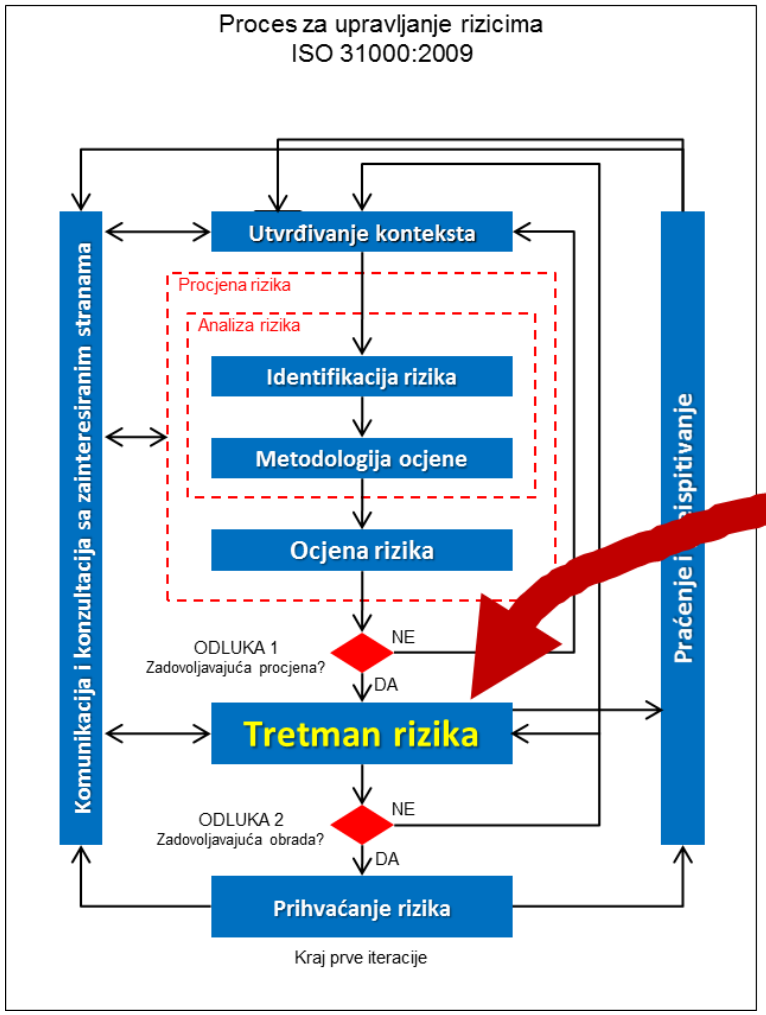


Smisao **upravljanja rizicima** je neprihvatljive rizike sveti na razinu prihvatljivosti i održavati ih na toj razini.

Smisao **poboljšanja upravljanja rizicima** je periodički smanjivati rizik apetitet*, odnosno donositi strožu matricu prihvatljivosti rizika izraženu kroz sigurnosnu politiku.

* Rizik apetit su količina i vrste rizika koje je organizacija spremana preuzeti. U doslovnom smislu, definirati apetit znači definirati kolika je "glad" za rizicima.

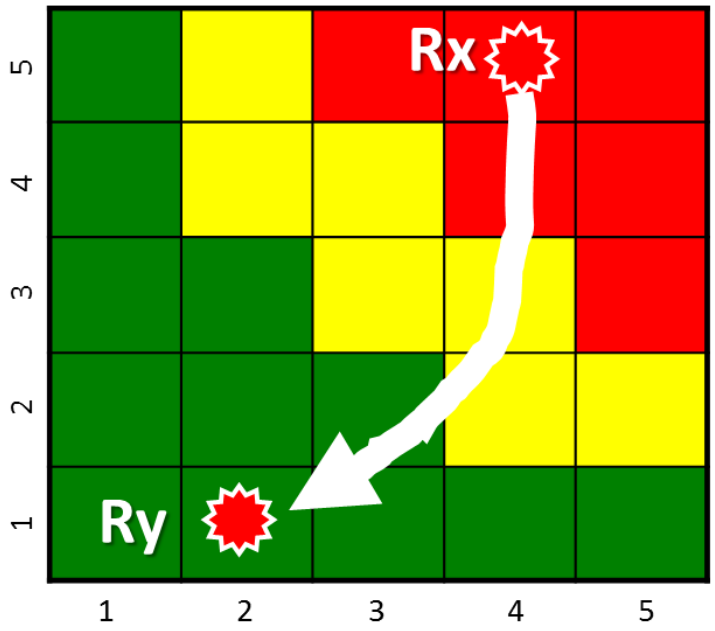
Opcije tretmana rizika prema ISO 31000:2009



- Izbjegavanje rizika
- Transfer rizika
- Smanjenje rizika
- Prihvaćanje rizika

Tretman rizika: Smanjenje razine rizika

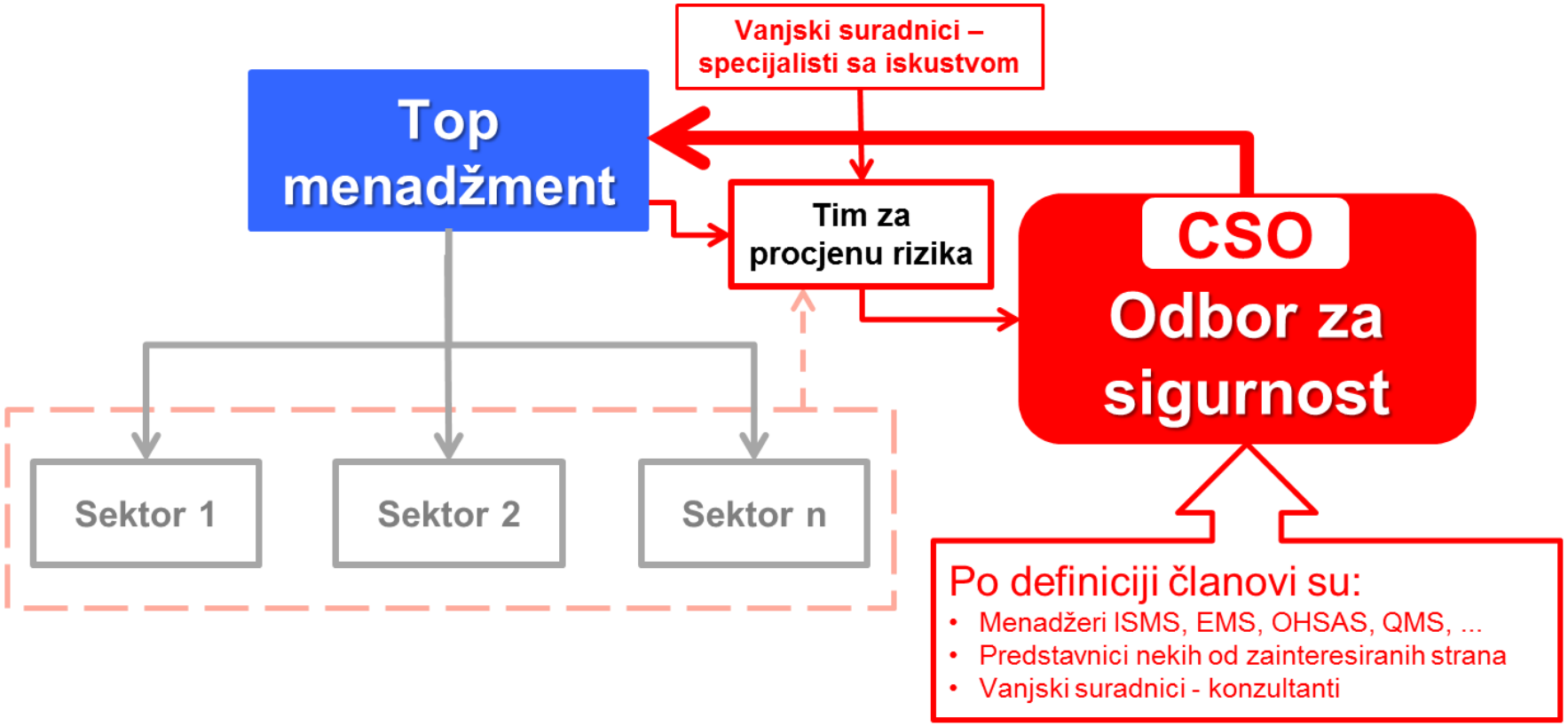
Treba smanjiti razinu rizika Rx na razinu Ry



a) Odrediti cilj akcije smanjivanja razine rizika
b) Definirati i opisati akciju
c) Planirati način provedbe akcije, rokove, odgovornosti, napraviti Cost-benefit analizu
d) Procijeniti preostali rizik nakon provedbe akcije smanjenja
e) Ishoditi odobrenje za provedbu akcije smanjenja rizika

Akcija smanjenja rizika naziva se KONTROLA ili SIGURNOSNA MJERA.

Integracija procesa 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.

Zaključak

- Upravljanje rizicima je stalna potreba i oduvijek se provodilo u nekom obliku.
- Formaliziranje upravljanja rizicima na temelju preporuka ISO 31000 je u praksi potvrđeno kao optimalno rješenje za gotovo sve klase problema vezanih za neizvjesnosti ostvarenja bilo kakvih ciljeva.
- Upravljanje rizicima pruža veće šanse uz manje gubitke za ostvarenje planiranih ciljeva

Efekti lošeg upravljanja rizicima

- Utrošak mnogo resursa – sigurnost nije povećana
- Nedovoljni utrošak sredstava – sigurnost smanjena
- Velike šanse za pojavu neidentificiranih rizika – neočekivane štete
- Nezadovoljstvo dionika za sigurnost

Risk comes from not knowing what you're doing

Hvala na pažnji…

Pitanja ?

Komentari ?