

Informacijska sigurnost i upravljanje rizicima u svjetlu mjeriteljstva

2. međunarodna mjeriteljska konferencija pod nazivom
"Odmjereno u Europu"
Šibenik, Solaris 19. - 21. svibnja 2011.



Autor
Zdenko Adelsberger

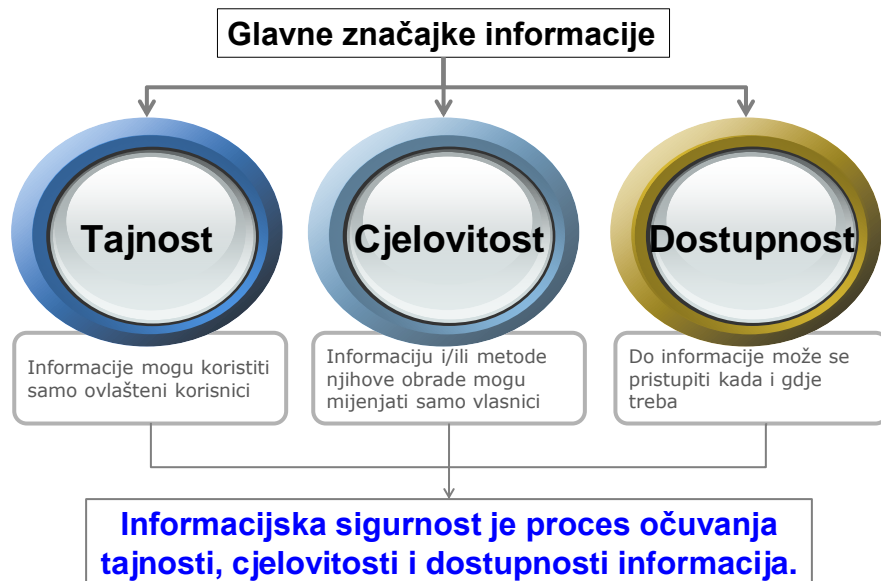
Što je informacijska sigurnost ?

Što je upravljanje rizicima ?

**Postoji li neki značaj
informacijske sigurnosti i
upravljanje rizicima za
mjeriteljstvo?**



Što je informacijska sigurnost?

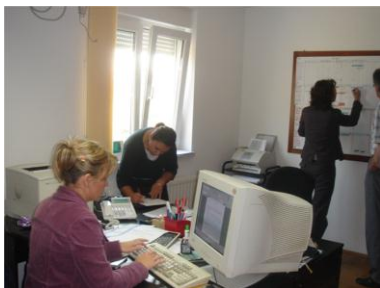


Što je informacijski sustav?

Informacijski sustav (IS) skup resursa i pravila unutar kojega se generiraju, pohranjuju, prerađuju i transferiraju informacije.

IT sustav skup IT resursa i pravila unutar kojega se generiraju, pohranjuju, prerađuju i transferiraju informacije.

Činjenica: IT ≠ IS



Postoji IS i IT



Postoji IS

Značaj informacija za poslovne sustave i sustave upravljanja

- Svi poslovni sustavi, kao i sustavi upravljanja, **informacije** koriste kao elementarni, odnosno **glavni resurs**.
- Informacijski sustavi su osnova funkcioniranja svakog poslovnog sustava i sustava upravljanja.
- Bez informacijskog sustava nemoguće je funkcioniranje poslovnih sustava i sustava upravljanja.
- Nesigurnost informacija, znači nesigurnost informacijskog sustava, što dovodi do nesigurnosti poslovnih sustava i sustava upravljanja, odnosno u konačnici do njihovog uništenja.

Što o informaciji kaže norma ISO/IEC 27001:2005 ?

“Informacija je **imovina** koja kao i ostala važna imovina u poslovanju ima **vrijednost** za organizaciju i mora biti stalno **odgovarajuće štice**na.”



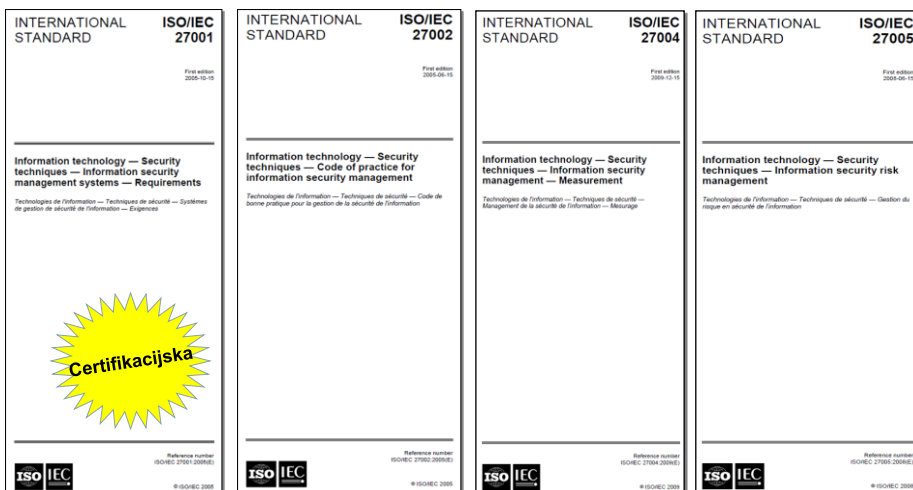
RELEVANTNI OBLICI NOSIOCA INFORMACIJA U POSLOVNOM SUSTAVU



KOMPONENTE SIGURNOSNOG RJEŠENJA



Ključne norme za uspostavu ISMS



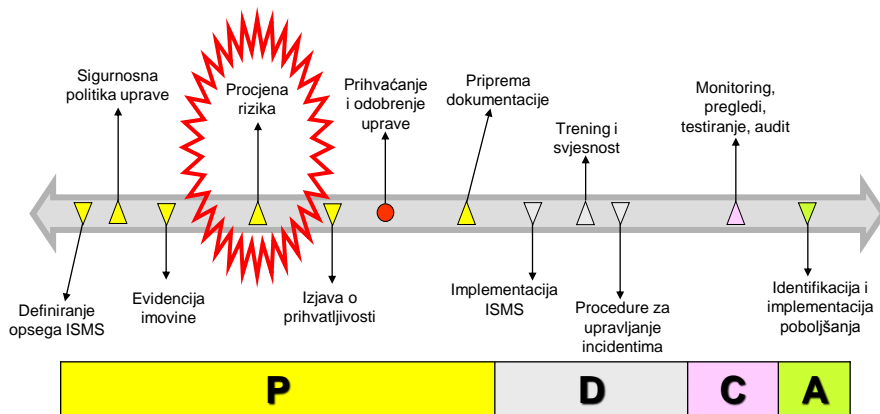
ISMS = Information Security Management System

Glavni cilj uspostave ISMS prema ISO/IEC 27001:2005

Osigurati očuvanje tri aspekta informacijske sigurnosti:

- Tajnost,
- Cjelovitost, i
- Dostupnost

Implementacija ISMS prema ISO/IEC 27001:2005



Upravljanje rizicima je temelj implementacije i poboljšanja ISMS



Što je rizik?

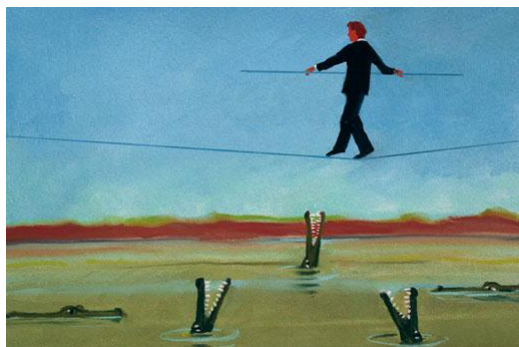
Kada se pojavljuje?

Zašto je važno poznavanje rizika?

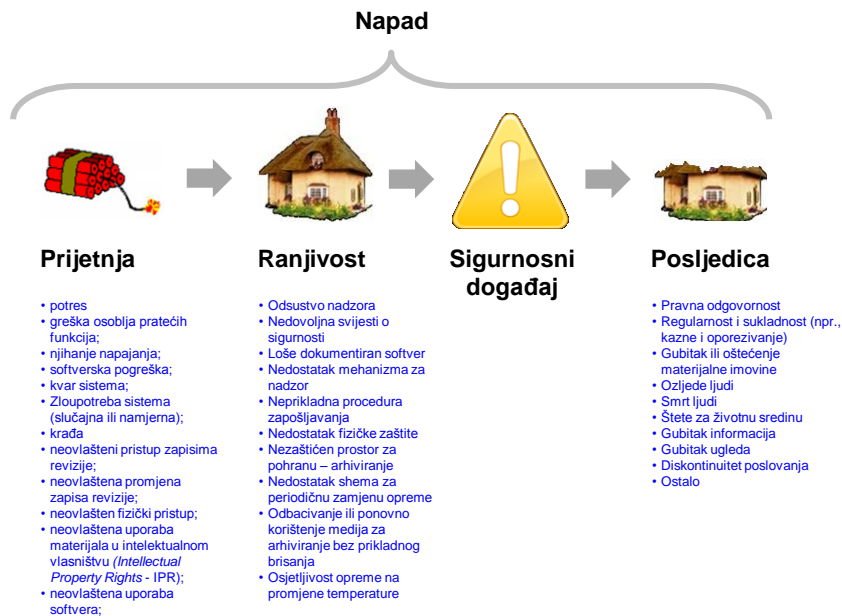
Što je rizik ?

Pojednostavljena definicija:

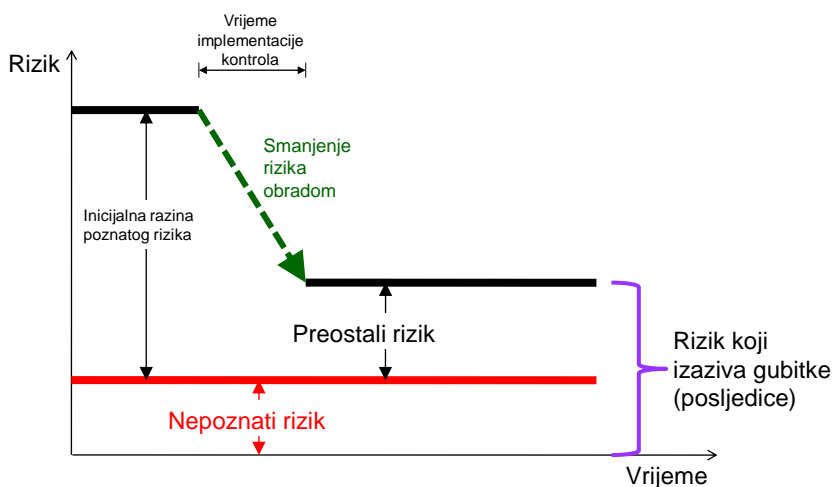
Rizik je vjerojatnost da se dogodi neželjena posljedica, odnosno neki gubitak.



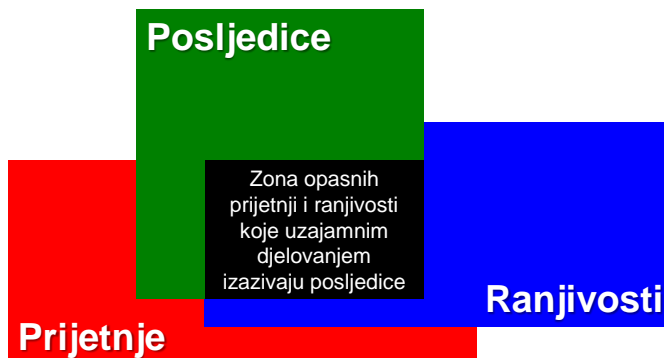
Mehanizam pojave rizika



Upravljanje rizicima smanjuje posljedice



Odnos prijetnji, ranjivosti i posljedica za sigurnost



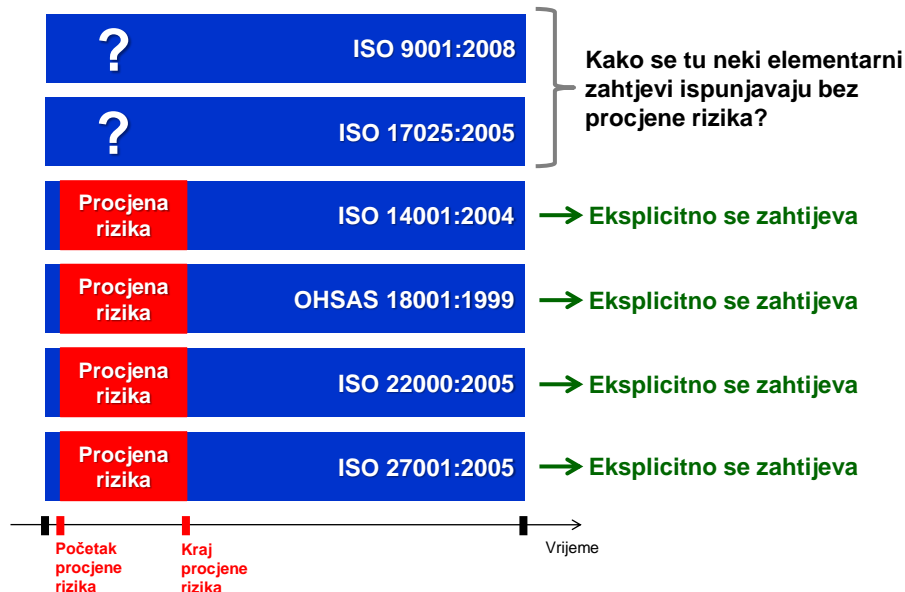
Da li je upravljanje rizicima moda ili kontinuitet prošlosti?

Činjenice:

Kada ne bi bilo upravljanja rizicima, ratovi ne bi bili takvi kakvi su bili, piramida ne bi bilo, ne bi poletio ni jedan avion i raketa, ne bi bilo podmornica, automobila, ne bi bilo hrane, ne bi bilo ni ljudi.

Kada bi se bolje i više formalno upravljalo rizicima manje bi banaka i firmi propadalo, općenito bi se sigurnije živjelo.

Upravljanje rizicima i sustavi upravljanja?



Informacijska sigurnost i sustavi upravljanja?



U tim sustavima upravljanja se spominje samo: zapise se ne smije mijenjati (nikada i nitko). Ostale dokumente smije mijenjati samo vlasnik uz odobrenje.

Kako se ispunjavaju ovi zahtjevi?

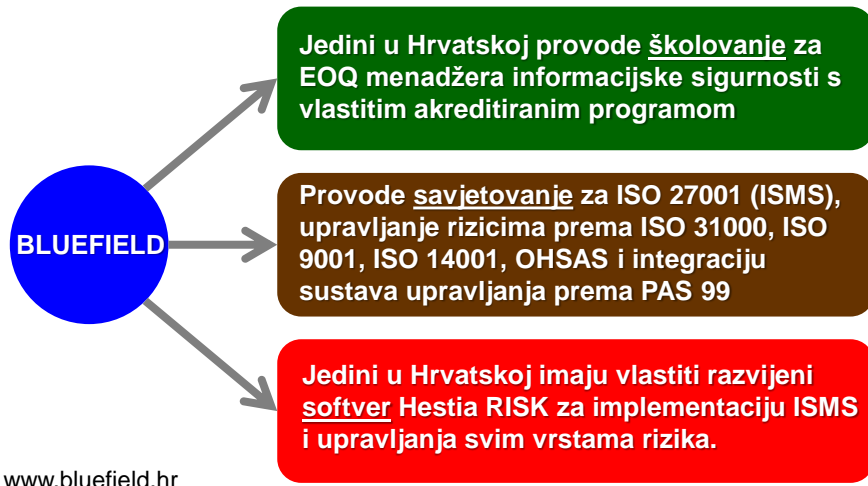
Što se dešava s integracijom sustava upravljanja?



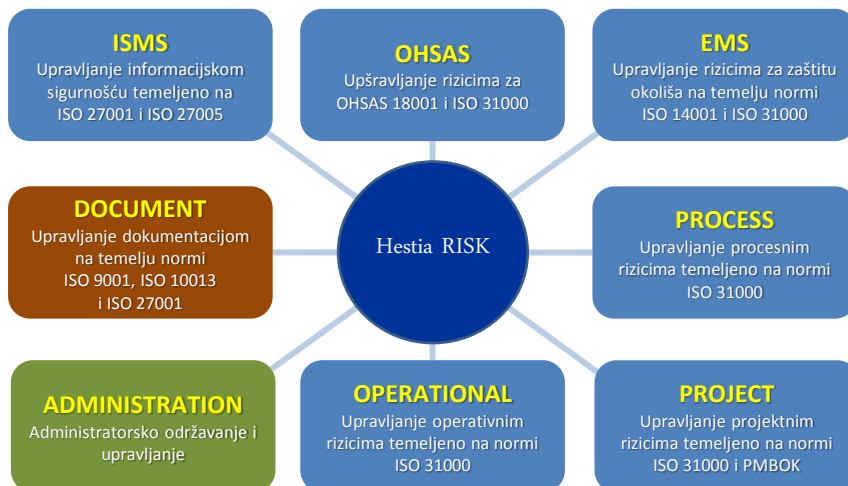
Kako implementirati ISMS i upravljanje rizicima u organizaciju

1. **SVIJEST VRHOVNE UPRAVE:** Ako vrhovnu upravu ne prisile zakoni i partneri, ona mora postati svjesna značaja upravljanja rizicima i problema informacijske sigurnosti
2. **EDUKACIJA:** obrazovati kritičnu masu specijalista (menadžera, operativaca, internih auditora)
3. **POKRENUTI PROJEKT:** vrhovna uprava mora osigurati resurse za pokretanje i provođenje projekta implementacije. Poseban je naglasak na nabavci odgovarajućih softverskih alata.
4. **STRUČNA POMOĆ:** nužno je osigurati stručnu pomoć savjetnika tijekom implementacije
5. **CERTIFICIRATI SUSTAV**
6. **UŽIVATI** u blagodatima novo-implementiranog sustava (vrhovna uprava i svi ostali)

Primjer podrške korisnika za implementaciju upravljanja rizicima i informacijskom sigurnošću



Hestia RISK



www.bluefield.hr

