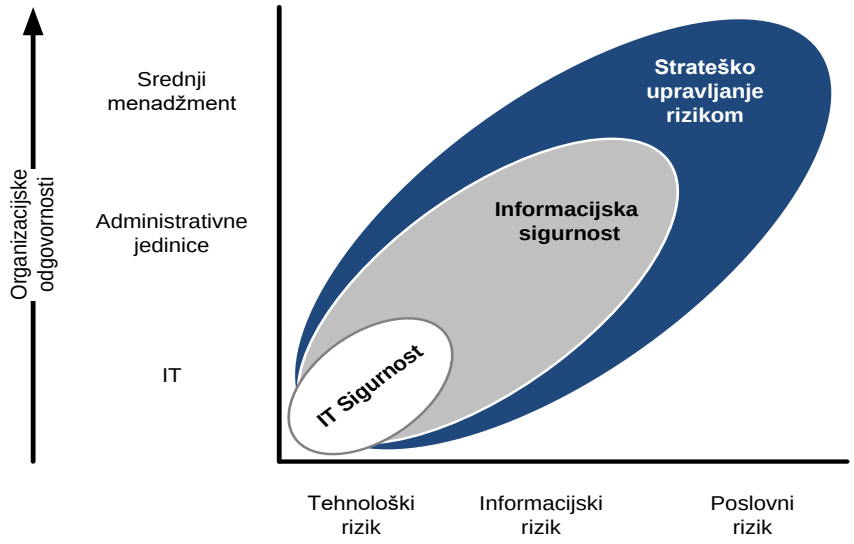
Upravljanje rizicima informacijska sigurnost (ISO 27005 i dr.)

Značaj

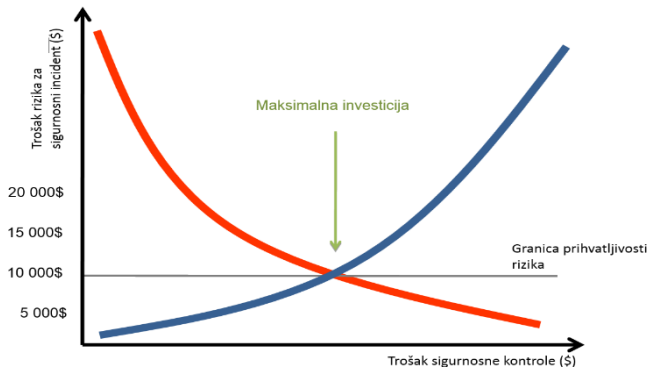
Informacije su temeljni pogon svakog poslovnog sustava, zbog kojeg je nužno uspostaviti primjerenu razinu sigurnosti ovog resursa. No, informacijska sigurnost je „pokretna meta“, područje koje se stalno i brzo mijenja. Upravljanje rizicima osnova je donošenja odluka o postupanju s ovim rizicima i uspostave sustava informacijske sigurnosti. Rizici vezani uz IT ulaze u svaki dio poslovnog sustava, kao što se vidi na slici u nastavku:

Odnos između IT rizika, informacijskih rizika i poslovnih rizika prikazan je na slici u nastavku:

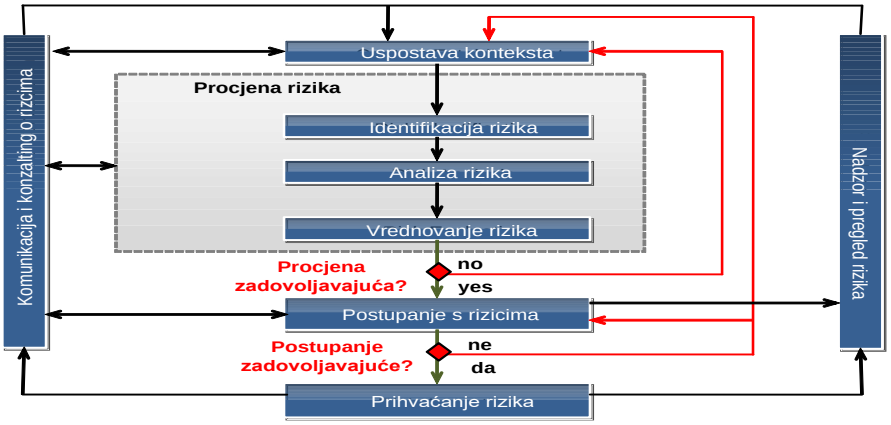


Istraživanja relevantnih svjetskih institucija i organizacija (World Bank, Gartner, Forrester, PwC, SANS Institute, SEI, Disaster Recovery Institute, IBM-a, Cisco-a itd.)

pokazuju da je područje IT-a i informacija visoki poslovni rizik. Osnovna zadaća upravljanja informacijskim rizicima je ispuniti sigurnosne zahtjeve propisane određenom normom, uz određivanje prihvatljive točke odnosa između ulaganja u sigurnosne kontrole i troška u slučaju pojave sigurnosnog incidenta. To je pojednostavljeno prikazano na slijedećoj slici:



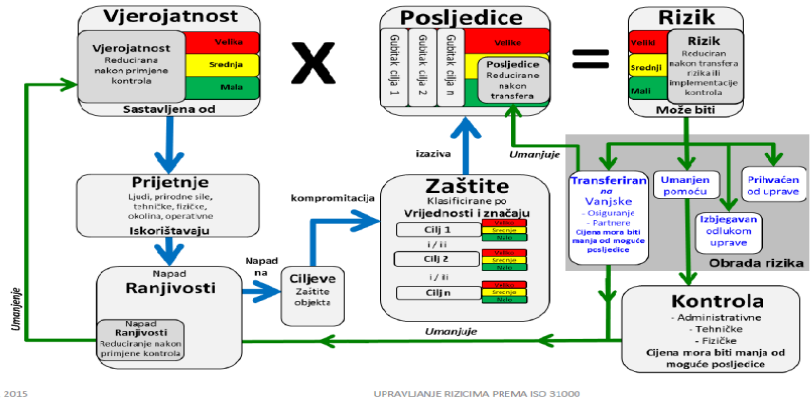
Postoji više načina upravljana rizicima. ISO je razvio normu ISI/IEC 27005 *Information Security Risk Management* putem koje se identificiraju potrebe nekog poslovnog sustava za informacijskom sigurnošću, omogućava donošenje ispravnih odluka u vezi sa ovim aspektom sigurnosti i usmjerava oblikovanje sustava informacijske sigurnosti. Ova norma slijedi uobičajeni proces upravljanja rizicima (ISO 31000) primjenjiv i za informacijsku sigurnost, prema slici u nastavku:



Norma ISO 27005 pruža dobre smjernice za upravljanje rizicima informacijske sigurnosti. Omogućava detaljnije pristupe procjenjivanju ovih rizika, od procjene rizika visoke razine, do raznih metoda i tehnika kao što su npr.:

- matrica predefiniranih vrijednosti,
- rangiranje prijetnji prema procjeni rizika i
- procjene vjerojatnosti ostvarenja i mogućih posljedica rizika

Slika u nastavku prikazuje postupak Identifikacije – Analize – Vrednovanja – Postupanja s rizicima informacijske sigurnosti.



Kroz svoje konzultantske aktivnosti ZIH je pouzdan partner da u suradnji s korisnikom riješi sve ove faze, a putem seminara osposobi Vaše djelatnike da ih dalje samostalno obavljaju.

Problematika upravljanja rizicima informacijske sigurnosti naročito je interesantna:

- Članovima uprava zaduženim za sigurnost
- Voditeljima korporativne sigurnosti
- Voditeljima funkcije upravljanja rizicima
- Voditeljima informacijske sigurnosti
- Stručnjacima koji se bave informacijskom sigurnošću
- Auditorima / procjeniteljima informacijske sigurnosti
- Svima koje zanima područje sigurnosti i informacijske sigurnosti

Usluge ZIH-a

Obzirom na svoje izuzetno dobre reference u području informacijske sigurnosti i drugih sustava temeljenih na svjetskim normama, te raspoloživa ekspertna znanja, ZIH Vam može pružiti slijedeće konzultantske usluge i seminare:

Konzultantske usluge

- Priprema pristupa upravljanju rizicima informacijske sigurnosti
- Edukacija stručnjaka za upravljanje rizicima i informacijsku sigurnost
- Uspostavljanje procesa upravljanja rizicima informacijske sigurnosti
- Odabir metode za upravljanje rizicima informacijske sigurnosti
- Izrada procedure za upravljanje rizicima informacijske sigurnosti
- Sudjelovanje u identifikaciji rizika informacijske sigurnosti
- Sudjelovanje u procjenama rizika informacijske sigurnosti
- Sudjelovanje u odabiru načina umanjivanja rizika informacijske sigurnosti
- Izrada prijedloga odgovornosti za rizike informacijske sigurnosti
- Sudjelovanje u implementaciji rješenja u praksu
- Sudjelovanje u provjeri (auditu) upravljanja rizicima informacijske sigurnosti

Seminari

ZIH održava slijedeće seminare iz ovog područja:

- Zašto i kako upravljati rizicima informacijske sigurnosti?
- Certified ISO 27005 Foundation (PECB)
- Certified ISO 27005 Risk Manager (PECB)
- Certified ISO 27005 Lead Risk Manager (PECB)

Način rada

Poduhvat razvoja, implementacije i izobrazbe iz područja upravljanja rizicima informacijske sigurnosti ZIH realizira zajedničkim radom svojih stručnjaka i tima korisnika.