

Kako pristopiti k varovanju informacij po standardu SIST ISO/IEC 27001:2006

Mladen Terčelj

CISM, CIS-A

Pooblaščenec za varovanje informacij
in varstvo osebnih podatkov v NLB d.d., Ljubljana

Cilji varovanja informacij

- ▶ **Preprečevati**
 - ▶ nezakonite in neupravičene posege v informacije
 - ▶ poslovno škodo
 - ▶ prekinjenost poslovanja
- ▶ **Ohranjati osnovne značilnosti informacij**
 - ▶ **zaupnost** – dostopnost do informacij le pooblaščenim osebam
 - ▶ **celovitost** – pravilnost in popolnost informacij in obdelav
 - ▶ **razpoložljivost** – informacije in obdelave so dostopne uporabnikom, ko jih potrebujejo

Pristop k implementaciji SUVI (1)

- ▶ Pridobiti odobritev vodstva za začetek projekta SUVI



- ▶ Opredeliti obseg SUVI
- ▶ Izdelati metodologijo informacijskih tveganj
- ▶ Izvesti analizo informacijskih tveganj
- ▶ Izvesti postopke za zmanjšanje tveganj
- ▶ Implementirati dokumentirani SUVI

Pristop k implementaciji SUVI (2)

- ▶ Opredeliti nosilce aktivnosti SUVI
- ▶ Ozaveščati zaposlene in pogodbene
- ▶ Izšolati notranje presojevalce
- ▶ Izvesti notranje presoje
- ▶ Pripraviti in izvesti vodstveni pregled

Odobritev vodstva za projekt SUVI

- ▶ Ravnati po Metodologiji za upravljanje projektov
 - ▶ predlog projekta s študijo izvedljivosti
 - ▶ zagonska koncepcija
 - ▶ vsebina (PODLAGE)
 - ▶ namenski (KAJ) cilji
 - ▶ objektni (KAKO) cilji
 - ▶ opredelitev virov (LJUDJE, SREDSTVA, ČAS)
 - ▶ opredelitev posameznih faz projekta (KAJ, KDO, KDAJ)
 - ▶ tveganja neizvedbe projekta



Opredelitev obsega SUVI v družbi

- ▶ Poslovni vidik
- ▶ Organiziranost
- ▶ Lokacijo(e)
- ▶ Sredstva
- ▶ Tehnologijo
- ▶ Nevarnost – slabo izbran obseg SUVI

Izdelati metodologijo informacijskih tveganj

- ▶ Obravnavati informacijska tveganja z vidika zaupnosti, celovitosti in razpoložljivosti (Z/C/R)
- ▶ Opredeliti obravnavo informacijskih tveganj poslovno / podpornih procesov
- ▶ Opredeliti informacijska sredstva
- ▶ Opredeliti grožnje in ranljivost sredstev
- ▶ Opredeliti obravnavo informacijskih tveganj
- ▶ Lahko kupite že izdelano programsko rešitev
 - ▶ posamezne rešitve so usmerjene v analizo tveganj sredstev informacijske tehnologije

Izvesti analizo informacijskih tveganj

- ▶ Opredeliti tveganja poslovno / podpornega procesa (Z/C/R)
- ▶ Določiti pomembnejša informacijska sredstva, ki so uporabljena v istem procesu
- ▶ Izbrati ustrezne grožnje in ranljivosti informacijskih sredstev
- ▶ Določiti informacijska tveganja za vsako informacijsko sredstvo (Z/C/R)



Izvesti postopke za zmanjšanje tveganj

- ▶ Izbrati ustrezne ukrepe za zmanjšanje tveganj
- ▶ Sprejeti tveganja
- ▶ Izogniti se posameznim tveganj
- ▶ Prenesti tveganja na druge stranke



Implementirati dokumentirani SUVI

- ▶ Izvesti GAP analizo za obstoječe postopke varovanja informacij (predvsem v IT)
 - ▶ dobre prakse institucij
 - ▶ poiskati ustrezna določila v SIST ISO/IEC 27002:2008
- ▶ Izdelati manjkajoče postopke varovanja informacij
 - ▶ upoštevati zakonska določila
 - ▶ upoštevati ukrepe v SIST ISO/IEC 27001:2006
- ▶ Pripraviti SOA – “Listo o primernosti”



Opredeliti nosilce aktivnosti SUVI

- ▶ Vodja SUVI
- ▶ Koordinatorja SUVI
- ▶ Vodje OE
- ▶ Koordinatorji SUVI v OE

Ozaveščati zaposlene in pogodbene

- ▶ E-izobraževanje za zaposlene
- ▶ Posebno izobraževanje za vodje drugega in tretjega organizacijskega nivoja
- ▶ Posredovanje “Dobrih praks”
- ▶ Objava sprememb na spletni strani in posredovanje obvestil o spremembah za vse zaposlene

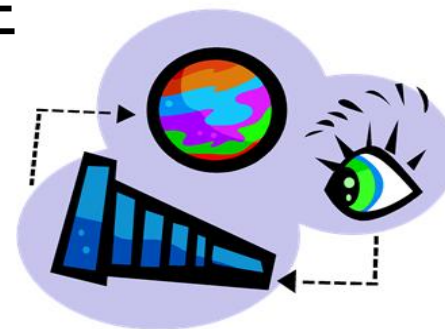
Izšolati notranje presojevalce

- ▶ Koga izbrati za notranje presojevalce
 - ▶ tisti, ki se že ukvarjajo z operativnimi tveganji
- ▶ Kakšno število notranjih presojevalcev
- ▶ Kako jih izšolati
 - ▶ preko institucije
 - ▶ opravljeni izpiti
 - ▶ potrdila



Izvesti notranje presoje

- ▶ Za vse procese v družbi najkasneje v treh letih
- ▶ Pripraviti plan notranje presoje
 - ▶ vodstvo SUVI in koordinatorji SUVI v OE
 - ▶ uskladiti z vodstvi OE
- ▶ Izvesti notranje presoje
 - ▶ predlog korektivnih ukrepov
 - ▶ predlog preventivnih ukrepov
- ▶ Uskladiti predloge ukrepov z vodstvi OE



Pripraviti in izvesti vodstveni pregled

- ▶ Rezultati pregledov SUVI
- ▶ Stanje predhodnih korektivnih / preventivnih ukrepov
- ▶ Grožnje in ranljivosti, ki še niso bile obravnavane
- ▶ Incidenti
- ▶ Rezultati meritev učinkovitosti SUVI
- ▶ Spremembe, ki vplivajo na SUVI
- ▶ Priporočila za izboljšavo
- ▶ Rezultati pregleda – glej desno



Kritični dejavniki uspeha

- ▶ Vidna podpora in zavezanost vodstva
- ▶ Pristop, ki je v skladu z organizacijsko kulturo v družbi
- ▶ Dokumentirani varnostna politika, cilji in postopki
- ▶ Zagotavljanje ustreznega usposabljanja in izobraževanja – učinkovito posredovanje pomena varovanja informacij vsem zaposlenim

