Univerza v Mariboru
*Fakulteta za logistiko*

# UPRAVLJANJE INFORMACIJSKIH TVEGANJ PO NIST SP 800-30

Mateja Škornik

# OZADJE

- Standard ISO/IEC 27005:2008 (skupina standardov ISO27k – področje informacijske varnosti) opisuje proces upravljanja s tveganji in njegove aktivnosti, s katerimi zagotavljamo informacijsko varnost v okviru splošnih konceptov, ki jih podaja ISO/IEC 27001:2005.

- Standard 27005 ne predpisuje, ne predlaga in ne imenuje posamezne metode ali orodja za analizo tveganj.

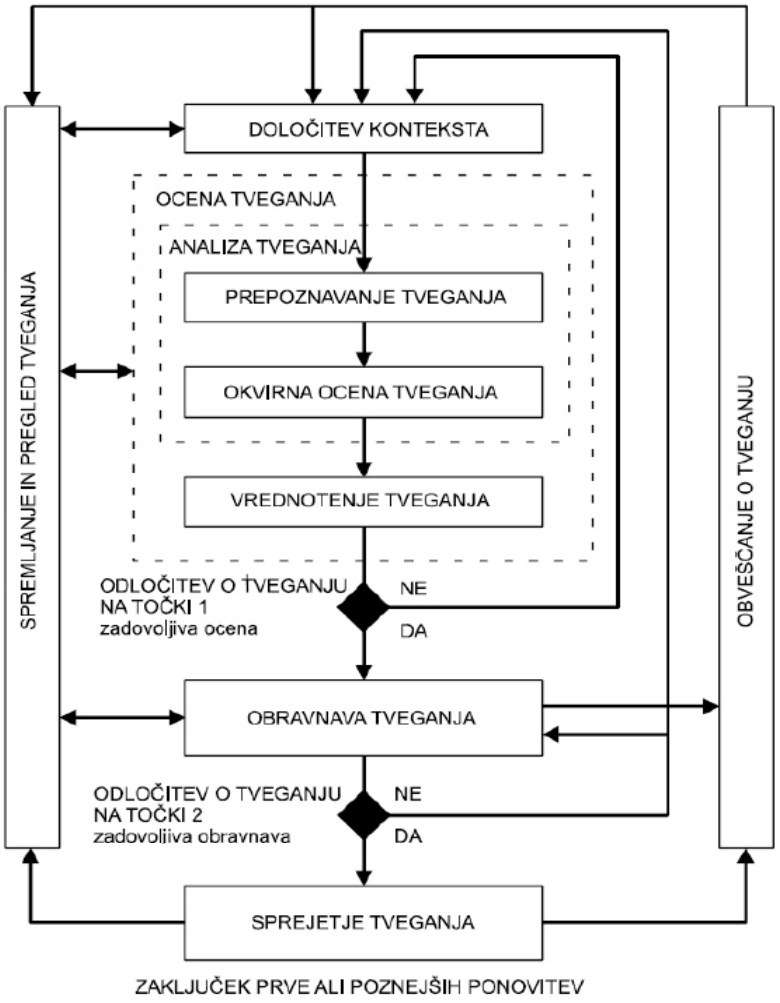
- Organizacija mora sama prepoznati metodologijo, ki najbolj ustreza njenemu SUIV.

# ISO 27005

- Opisuje en proces. Proces sestavljajo aktivnosti. Aktivnosti vsebujejo dejavnosti (opravila).

- Pri vsaki aktivnosti so opravila razdeljena v naslednja področja:
  - Prispevek (*Input*),
  - Ukrep (*Action*),
  - Navodila za vpeljavo (*Implementation guidance*),
  - Rezultat (*Output*).

# AKTIVNOSTI PROCESA PO ISO 27005



# METODE IN ORODJA ZA UPRAVLJANJE IT TVEGANJ

- NIST
- OCTAVE
- FRAP
- COBRA
- Risk Watch
- CRAMM
- FMEA

# NIST SP 800-30

- Metoda, ki je namenjena predvsem kakovostnem usposabljanju varnostnih analitikov. Razvita s strani *National Institute of Standards and Technology*, ZDA.
- Obvladovanje tveganj vključuje v SDLC (*System Developement Life Cycle*).
- Opisuje postopek ublažitve tveganj in strateški pristop za nadzor nad izvajanjem kontrolnih kategorij.
- Obravnava že uveljavljene prakse in potrebe po stalnem ocenjevanju tveganj in dejavnikov.

# NIST SP 800-30

Metodologija NIST sestoji iz 9 korakov:

- korak 1: karakterizacija sistema (*System Characterization*),
- korak 2: identifikacija groženj (*Threat Identification*),
- korak 3: identifikacija ranljivosti (*Vulnerability Identification*),
- korak 4: analiza kontrole (*Control Analysis*),
- korak 5: ocena verjetnosti (*Likelihood Determination*),
- korak 6: analiza vpliva (*Impact Analysis*),
- korak 7: določitev tveganja (*Risk Determination*),
- korak 8: priporočila kontrole (*Control Recomendations*),
- Korak 9: dokumentiranje rezultatov (*Results Documentation*).

# 1 KARAKTERIZACIJA SISTEMA

- Določitev mej informacijskega sistema, vključno z viri in informacijami, ki predstavljajo sam sistem.
- Opredelitev obsega ocene tveganja.
- Zasnova učinkovite avtorizacijske meje podajanja informacij (tako programskih in strojnih, kot tudi informacije o sistemskih povezljivostih, ter o odgovornem podpornem osebju), ki so bistvenega pomena za opredelitev tveganja.

# 2 IDENTIFIKACIJA GROŽENJ

- Ocena virov groženj, potencialnih šibkih točk ter obstoječe kontrole.

- Identifikacija morebitnih virov groženj ter opredelitev potencialno nevarnih virov za vrednoten  informacijski sistem.

# 3 IDENTIFIKACIJA RANLJIVOSTI

- Analiza groženj informacijskega sistema mora vključevati analizo ranljivosti povezano s sistemom okolja.

- Cilj tega koraka je sestaviti seznam pomanjkljivosti sistema (šibkosti in pomanjkljivosti), ki bi jih viri groženj lahko izkoristili.

# 4 ANALIZA KONTROLE

- Analiza kontrol, ki so bile izvedene oz. so načrtovane za izvajanje s strani organizacije, za zmanjšanje oz. odpravo verjetnosti uresničenja grožnje iz sistema ranljivosti.

- Za izpeljavo splošne ocene verjetnosti (korak 5), ki kaže potencialne ranljivosti je pri izvajanju že implementiranih oz. načrtovanih kontrol potrebno upoštevati še grožnje okolja.

# 5 OCENA VERJETNOSTI

Ocenitev verjetnosti potencialne ranljivosti z upoštevanjem sledečih dejavnikov:

- motivacijo in zmožnost vira grožnje,
- naravno ranljivost,
- obstoj in učinkovitost sedanjih kontrol.

# 6 ANALIZA VPLIVA

- Opredelitev škodljivih vplivov, ki izhajajo iz uspešno izvedenega koraka 2 (Identifikacija groženj) in 3 (Identifikacija ranljivosti).

- Pred začetkom izvajana tega koraka je potrebno pridobiti naslednje informacije:

  - naloge sistema,
  - kritičnost podatkov in sistema,
  - občutljivost sistema in podatkov.

# 7 DOLOČITEV TVEGANJA

- Ocena stopnje tveganja informacijskega sistema.
- Za merjenje groženj je potrebno determinirati lestvico obsega groženj in matriko ravni tveganja.

# 8 PRIPOROČILA KONTROLE

- Zagotovijo se kontrole za zmanjšanje in odpravo ugotovljenih tveganj.

- Cilj je zmanjšati stopnjo tveganja informacijskega sistema in njegovih podatkov na sprejemljivo raven. Pri podajanju priporočil ali alternativnih rešitev za zmanjšanje ali celo odpravo tveganj je pametno upoštevati naslednje dejavnike:

  - učinkovitost priporočljivih možnosti (npr. sistemska združljivost),
  - zakonodajo in uredbo,
  - politiko organizacij,
  - operativni vpliv,
  - varnost in zanesljivost.

# 9 DOKUMENTIRANJE REZULTATOV

Rezultate je potrebno dokumentirati v uradno poročilo.

[osnutek poročila]

Univerza v Mariboru
*Fakulteta za logistiko*

# POROČILO OCENE TVEGANJA

## POVZETEK IZVAJANJA

### I. Uvod

*-Namen*
*- Področja ocen tveganja*

*Opišemo sistemske komponente, elemente, uporabnike in druge podrobnosti o sistemu, ki je zajet v oceni.*

### II. Pristop k oceni tveganja

*Na kratko povzamemo pristop k oceni tveganja, zajamemo*

- *udeležence (ekipo),*
- *tehniko uporabljeno za zbiranje informacij (npr. uporaba orodij, vprašalnikov),*
- *opis in razvoj lestvice tveganja (matrika tveganja).*

### III. Opredelitev sistema

*Opredelimo sistem, vključno s strojno in programsko opremo, sistemskimi vmesniki ter podatki in uporabniki. Podamo diagram povezav oz. organigram sistemskih vhodov in izhodov s katerim očrtamo področja ocene tveganja.*

### IV. Nevarnosti/grožnje

*Sestavimo seznam potencialnih groženj in sistematiziramo grožnje, ki se navezujejo na ocenjeni sistem.*

### V. Rezultati

*Sestavimo seznam opomb. Vsako opazka mora vključevati*

- *številko opazke in kratek opis,*
- *razpravo o nevarnosti virov in ranljivosti,*
- *opredelitev obstoječih kontrol (varnostnih ukrepov) za ublažitev,*
- *verjetnostno razpravo in vrednotenje,*
- *analizo vpliva,*
- *oceno tveganja, ki temelji na ravni matrike tveganja,*
- *priporočitev kontrol in alternativne možnosti za zmanjšanje tveganja.*

### VI. Povzetek

*Povzamemo skupno število opazovanj. Za lažje izvajanje priporočenega nadzora in ublažitev tveganj v obliki tabele povzamemo še stališča, stopnje tveganja in priporočila.*

# ZAKLJUČEK 1/3

- Za izvedbo učinkovitega ISMS (*Information Security Management System*) morajo organizacije poskrbeti za sistematično upravljanje IT tveganj.

- Upravljanje IT tveganj mora biti skladno s potrebami, usmeritvami in okoljem v katerem organizacija deluje. Prav tako mora biti skladno z upravljanjem vseh tveganj, s katerimi se organizacija srečuje.

- Proces je potrebno vzpostaviti in ga po vzpostavitvi stalno izvajati in dopolnjevati.

- Metoda NIST SP 800-30 predstavlja samo eno izmed metod.

# ZAKLJUČEK 2/3

- NIST SP 800-30 zajema več kot 50 strani. Vsebuje še dodatke s primeri in dodatnimi informacijami.
- Pojem ‘tveganje’ definira na 28. strani: ‘Tveganje je funkcija verjetnosti vira grožnje, ki kaže na možne ranljivosti in škodljive vplive na organizacijo.’
- ISO 27005 pojem ‘tveganje’ definira na 23. strani kot: ‘Tveganje je kombinacija:
  - posledic, ki lahko sledijo pojavu neželenega dogodka in
  - verjetnosti pojava dogodka.’

# ZAKLJUČEK 3/3

- Seven J. Ross [*Gang Aft Agley, ISACA Journal; Vol 3, 2009*] meni, da ‘tveganje’ sploh ni definirano (ne glede na standard ISO 27005), temveč je definirana le izpostavljenost, ki je predstavljena kot izguba, ki se da predvideti v neki posamezni situaciji.

- Dr. Borut Jereb [*Kaj so tveganja?, 17. mednarodna konferenca o revidiranju in kontroli informacijskih sistemov, zbornik referatov, 2009*] predlaga definicijo pojma ‘tveganje’. Tveganje opiše kot izpostavljenost negotovosti in poudari, da moramo pri izračunavanju tveganj nujno vključiti javnost kot definiran parameter.

Univerza v Mariboru
Fakulteta za logistiko

Je možno natančno obravnavati problematiko, katere osnovni pojmi niso jasno definirani?

**mateja.skornik@fl.uni-mb.si**