Notranje kontrole kot pomemben dejavnik za delovanje informacijskega sistema

mag.Andrej Tomšič

Informatika, d.d.

Namen prispevka

- kaj so NK in kakšen pomen imajo za poslovanje
- zaobjamejo NK tudi del informacijske podpore
- obravnavamo v okviru obvladovanja IT tudi NK
- kako naj bodo NK integrirane v IS
- Kako jih pri prenovi IS upoštevati, da bo le-ta daja želene rezultate

Opredelitev NK

Notranje kontrole

- so upravljalske (kibernetske) zanke
- vgrajene v poslovanje (vse ravni in področja)
- bistvene za kakovost poslovanja (red!)
- zmanjšujejo tveganje…
- ki jih letno presojajo tudi revizorji
- v računalniško zasnovanem IS so večinoma vgrajene v IT

ključni element Foreign Corrupt Practices Act (FCPA) 1977 in Sarbanes-Oxley Act iz leta 2002

Opredelitev NK

Ustroj NK z vidika računovodske funkcije:

1. Splošne NK (tem. org. pog. za delovanje: akti, NR, navodila, sistem poročil, inf.varnost, ISO...)
2. Računovodske NK (zagotavljati spl.org.pogoje za računov.)
   - 2.1. Temeljne kontrole
     - 2.1.1 Kontrole pravilnosti podatkov (odobritev, primerjanje(Sa), primerjava 2 NK (psw))
     - 2.1.2 Kontrole popolnosti obdelave podatkov (oštev.dok, kontr.vsota, odprte post.)
     - 2.1.3 Kontrole ponovnega opravljanja nekaterih postopkov (2X isti P)
   - 2.2. Nadzorne kontrole
     - 2.2.1 Razmejitev dolžnosti (porazdelitev dela na več oseb: kasiranje, štetja...)
     - 2.2.2 Materialna odgovornost in omejevanje pristopa (žig, ključi, gesla,..)
     - 2.2.3 Nadziranje (vgrajeno v sistem NK: parafi pog, likvidacija fa; neposredno: šefi, presoje,...)

NK so v <u>vseh</u> procesih, ne le v računovodski funkciji

Informacijski vidik NK

NK = kibernetska zanka,
vpeljana na pozicijo,
kjer želimo obvladovati tveganje

= odločitveni proces,
s katerim vplivamo na obvladovani poces

NK z informacijskega vidika

= informacijska podpora kontroliranju

NK v okolju IT

Obstajata dve glavni skupini kontrol:

- kontrole informacijskih rešitev (IT per se) in
- splošne kontrole v okviru IT okolja (poslovni procesi, podprti z IT).

NK v okolju IT

Vpeljava / menjava IT **razširi področje NK** na področje obvladovanja IT:

- zadovoljiti potrebe po kakovosti, zanesljivosti in varnosti informacij in (informacijskih) sredstev
- ➔ obvladovati uporabo razpoložljivih IT virov: SW, HW, podatkov in informacij, infrastrukture ter ljudi
- ➔ sistem IT kontrolnih ciljev, ki jih je mogoče sistematično načrtovati, meriti in spremljati

➔ Dobimo cel sklop procesov in virov, ki poganjajo sami sebe, da na koncu poganjajo poslovanje ???

NK v okolju IT

Vpeljava / menjava IT **spremeni naravo NK**. Primeri:

- Omejena **sledljivost** dokumenta (veriga dokazov)
- Pojav **sistematične napake**
- Prenos **kontrole** ločevanja iz posameznikov v verigi na službo **operative** in **potrjevanje poslov**
- **Podatki v BP** terjajo drugo vrsto kontrol, kot na klasičnih nosilcih (pristopi, obvladovanje,…)
- Množica analitičnih podatkov in njihovo sintetiziranje
- Tveganje zaradi vdora v sistem (virusi,…), napačnih investicij v IT, manipulacij s podatki,…
- …

NK v okolju IT

1. Kontrole **organiziranosti in delovanja**
2. Kontrole delovanja IS (**operativa**)
3. Kontrole **izgradnje** IS in njegovega **vzdrževanja**
4. Kontrole **varnosti**
5. Kontrole **podatkov in postopkov**
6. Kontrole v **uporabniških rešitvah**
7. ...

NK v okolju IT

Ad 1) Kontrole organiziranosti in delovanja

Odnos vodstva do obvladovanja tveganj pri uvajanju IT

- Tveganje pri **investiranju** : izplen (TCO : skrite koristi)
- Tveganje glede na **organizacijski ustroj**
- Tveganje glede pos.**poslovnih funkcij** (kadrovska,...)
- ...

NK v okolju IT

Ad 1) Kontrole organiziranosti in delovanja

Primer: Načelo ločevanja nalog
(npr: priprava in izplačilo plačilnih nalogov je avtomatizirano)

➔ Tveganje: programer/operater neposredno pristopa do f.sredstev

➔ Primerne NK:

- **katalog verzij programov** z odgovorno osebo in zgodovino sprememb,
- **avtorizacija pristopov** do programov,
- predhodna **odobritev** vsake **spremembe kode**,
- **prepoved programerjem**, da izvajajo obdelave,
- dosledna **dokumentiranost** procesov z diagrami programov in vrisanimi vgrajenimi **NK** ter odgovornostjo in nadzor nad tem,
- **obvladovanje napak** – kontrolni pregledi, testiranje, help desk, evidenca pritožb,...
- **evidence obdelav** – tudi interaktivnih s spremnimi podatki, z odobritvijo posla,...
- **kroženje operaterjev** – za morebitno poneverbo je tako potreben dogovor več oseb,...
- ...

Opis želenega stanja

Sistem NK, ki bo s podporo IT:

- omogočal učinkovito in **uspešno odvijanje** notranjega kontroliranja,
- **konsistenten in integriran** z ostalimi deli upravljanja, vključno z obvladovanjem kakovosti in varnosti IS,
- **integriran** v preostali del (prenovljenega) IS,
- v informacijskih rešitvahe ustrezno **dokumentiran** - z eksplicitno opredeljenimi NK (procesi, podatkovno zasnovo, zapisi, naborom ukrepov ter odgovornostmi, zadolžitvami in kompetentnostjo),
- omogočal **enostavno rokovanje** s podatki oz.spremno dokumentacijo ki pri tem nastane,
- nudil čim lažje **pridobivanje informacij** iz dokumentov,
- omogočal čim lažje **prilagajanje** spremembam v organizaciji in poslovanju...

Težave in pasti

pri integraciji IS za podporo NK v prenovljen IS:

- **Teoretična izhodišča** prenove IS upoštevajo NK?
- Pomen **NEračunovodskih NK** in revizija.
- **So NK svet zase**? Izolirane rešitve in integracija.
- NK so **dinamične**. Prilagajanje zaradi njihove zapletenosti?
- NK so **specifične** glede na okolje. **Nakup SW? Integracija?**
- Povezovanje z **IS izven organizacije** (vsebina, programsko okolje in splošne varnostne omejitve, kar vpliva na NK?).
- **EUC**, ki s strani NK formalno ni obvladovan, lahko nekonsistentnost notranjega kontroliranja bistveno poveča.
- **Stična znanja** udeležencev in prenova IS...

Predlogi izvedbe

Načela izvedbe:

- NK obravnavati kot integralni del procesov:
  - NK = delni sistem US
  - Inf.podpora NK = delni sistem IS
- Dvonivojski pristop k izgradnji in integraciji NK:
  - Koncipiranje NK: top-down
  - Izgradnja in integracija: bottom-up
- Upoštevati dinamiko NK ob prenovi IT/IS
- PDCA - Deming

Predlogi izvedbe

Faze izvedbe:

- **strateška** zasnova sistema NK,
- celovito **opredelitev vseh procesov**, kjer uvajamo oz.prenavljamo NK,
- določiti event. **tveganja**,
- izbira ustreznih **standardov ali metod** kot usmeritev za NK,
- **specifikacija zahtev** NK,
- opredelitev **procesov z integriranimi NK** ter pripadajoče **podatkovne zasnove**,
- **prevernaje**, **potrditev** NK in izvedba **izgradnje** oz.prenove informacijske rešitve,
- **vzdrževanje** sistema NK skladno z mnenjem revizorja oz.veščakov.

Predlogi izvedbe

Načela izvedbe:

- povabiti k sodelovanju vse vpletene udeležence (stakeholders):
  - vrhovni, srednji in operativni **menedžment**,
  - **uporabnika** na operativnem nivoju IS,
  - **revizorja** in/ali **veščake** na vsebinskem področju,
  - **strokovnjake** za obvladovanje kakovosti in varnosti IS, informatike,
  - **računalniške** strokovnjake, **informatike**, ...

Za (permanentno) obvladovanje NK – zlasti pri prenovi IS je odgovorno VODSTVO

Predlogi izvedbe

Načela izvedbe:

- vse vgrajene NK **kupljenih IS** niso primerne za naše okolje in jih je potrebno ustrezno dopolniti oz. prilagoditi,
- enako velja, kadar se vključujemo v **medorganizacijske IS**, kjer je treba skupne NK posebej dogovoriti z ostalimi.

Predlogi izvedbe

Načela izvedbe:

- Glede na vedno večji razmah (**EUC**) velja opozoriti, da informacijske rešitve takih sistemov niso izgrajene po ustaljeni dobri praksi in metodah razvoja IS, kar velja tudi za sistem NK.

- Zato je v okviru teh rešitev potrebna dodatna pozornost pri integracijah le-teh v celoten IS

  ➔ **splošno** : **individualno** obravnavanje vsakega procesa NK.

Predlogi izvedbe

Načela izvedbe:

- **zaposleni** so najpomembnejši kontrolni faktor,
- omogočijo, da dogodki sploh nastanejo – nič se ne zgodi brez njih;
- ➔ lahko dosežejo, da deluje slab ali dober IS.

- Zato je potrebno nenehno **negovanje** njihove izobrazbe, usposobljenosti, kompetentnosti in poslovne kulture,
- da bodo sami motivirani za prilagajanje in dosledno vzdrževanje NK na njihovem poslovnem področju.