

# **Hierarhija pravil notranjega revidiranja**

Tina Toman Pfajfar, IIA Slovenski inštitut  
(maj 2011)

- Slovenski inštitut za revizijo, Sekcija za notranjo revizijo, 1997, Hierarhija pravil notranjega revidiranja
- Ameriški inštitut notranjih revizorjev (Institute of Internal Auditors), 1941, Okvir mednarodnih strokovnih ravnanj in
- IIA Slovenski inštitut, 2007
- [http://www.si-revizija.si/notranji\\_revizorji/pravila\\_stroke.php](http://www.si-revizija.si/notranji_revizorji/pravila_stroke.php)

# Hierarhija pravil notranjega revidiranja

- Prva raven:
  - zakoni ter verodostojna razlaga posameznih določb zakona;
  - obvezni del Okvira mednarodnih strokovnih ravnanj;
  - slovenski standardi ter
  - kodeksa notranjerevizijskih načel in poklicne etike.
- Druga raven:
  - pojasnila in stališča Strokovnega sveta Inštituta;
  - usmeritve slovenskih nadzornih inštitucij;
  - metodološka gradiva in priročniki Inštituta ter
  - priporočljivi del Okvira mednarodnih strokovnih ravnanj.
- Tretja raven:
  - literatura o notranjem revidiranju in
  - strokovna pravila v tuji praksi.

## Hierarhija pravil notranjega revidiranja

### Prva raven - obvezno

- zakoni ter verodostojna razlaga posameznih določb zakona
- obvezni del Okvira mednarodnih strokovnih ravnanj
  - definicija notranjega revidiranja: namen, narava, področje notranjega revidiranja
  - kodeks etike: neoporečnost, nepristranskost, zaupnost, usposobljenost
  - standardi
- slovenski standardi ter
- kodeksa notranjerevizijskih načel in poklicne etike (1998, 2004, 2011)

## Hierarhija pravil notranjega revidiranja Prva raven - obvezno

### Obvezni del Okvira mednarodnih strokovnih ravnanj - **standardi**

- okvir za delovanje
- veljavnost od 1. 1. 2009
- veljavnost sprememb od 1. 1. 2011
- standardi značilnosti
  - organizacija in posamezniki
  - neodvisnost in nepristranskost
- standardi delovanja
  - notranje revidiranje
  - načrtovanje, izvajanje, poročanje, spremljanje napredovanja
- standardi izvedbe
  - dajanje zagotovil
  - svetovanje
- pojmovnik

## Hierarhija pravil notranjega revidiranja Prva raven - obvezno

### Obvezni del Okvira mednarodnih strokovnih ravnanj - **standardi**

- standardi značilnosti
  - 1200 – Strokovnost in potrebna strokovna vestnost: Posli morajo biti opravljeni strokovno in strokovno vestno.
  - 1210.A1 – Notranjerevizijski predstojnik mora pridobiti ustrezen nasvet in pomoč, če notranji revizorji nimajo znanja, veščin in drugih sposobnosti, potrebnih za izvedbo celotnega ali dela posla.
  - 1210.A3 – Notranji revizorji morajo imeti zadostno poznavanje ključnih informacij o tehnoloških tveganjih in kontrolah ter o razpoložljivih tehnološko zasnovanih postopkih za izvedbo dodeljene naloge. Vendar se od vseh notranjih revizorjev ne pričakuje, da bi imeli strokovno znanje notranjega revizorja, katerega glavna naloga je revidiranje informacijske tehnologije.

## Hierarhija pravil notranjega revidiranja Prva raven - obvezno

### Obvezni del Okvira mednarodnih strokovnih ravnanj – **standardi**

Notranjerevizijski izvajalec lahko funkcionira na različne načine (lastna OE, občasna pomoč, samo zunanji izvajalec...). V primeru zunanje pomoči pri izvajanju notranjerevizijske dejavnosti je potrebno upoštevati:

- odgovornost za vzpostavitev notranjerevizijske dejavnosti je na strani vodstva,
- odgovornost za izvedbo notranje revizijskih poslov ostaja v organizaciji: notranjerevizijski predstojnik (NRP),
- NRP je odgovoren za pripravo in izvedbo pogodbenih določil z zunanjim izvajalcem, za nadzor nad kvaliteto opravljenega dela, poročanje naročniku in spremljanje napredovanja,
- NRP mora pretehtati usposobljenost, neodvisnost in nepristranskost zunanjega izvajalca, pa tudi preveriti potrebna znanja, veščine in druge sposobnosti za izvajanje posla,
- NRP sodeluje z zunanjim izvajalcem pri določanju ciljev in obsega dela, dostopa do delovnih gradiv in pomembnih informacij, lastništva in hrambe delovnega gradiva, zaupnosti informacij,
- pri izvajanju notranjih revizij – tudi z zunanjim izvajalcem – je vedno potrebno zagotavljati skladnost dela s standardi in ustreznimi kodeksi.

## Hierarhija pravil notranjega revidiranja Druga raven - priporočljivo

- pojasnila in stališča Strokovnega sveta Inštituta
- usmeritve slovenskih nadzornih inštitucij
- metodološka gradiva in priročniki Inštituta ter
- **priporočljivi del Okvira mednarodnih strokovnih ravnanj**
  - stališča (Position Papers)
  - svetovalni napotki (Practice Advisories)
  - strokovna navodila (Practice Guides)

## Hierarhija pravil notranjega revidiranja Druga raven - priporočljivo

### Priporočljivi del Okvira mednarodnih strokovnih ravnanj

- stališča (Position Papers): navodila, ki zajemajo primere, povezane s posebnostmi področja, panoge:
  - Vloga notranjega revidiranja pri obvladovanju tveganja na ravni podjetja
  - Vloga notranjega revidiranja pri podpori notranjerevizijskemu izvajalcu
- svetovalni napotki (Practice Advisories): povezani s posameznim standardom; ponujajo konkretne primere, rešitve (prevedeni v slovenščino):
  - svetovalni napotki veljajo od 1. 1. 2009
  - 3 spremembe/dopolnitve v 2009
  - 12 sprememb/dopolnitev v 2010
- strokovna navodila (Practice Guides): procesi, postopki, orodja, tehnike, programi za posamezne primere notranjih revizij:
  - PG
  - GTAG
  - GAIT

## Hierarhija pravil notranjega revidiranja Druga raven - priporočljivo

### Priporočljivi del Okvira mednarodnih strokovnih ravnanj – **strokovna navodila**

- PG – Practice Guides – strokovna navodila - 9
- GTAG – Global Technology Audit Guide – Navodila za revizijo globalne informacijske tehnologije - 15
- GAIT - Guide to the Assessment of IT Risk – Navodila za oceno tveganja informacijske tehnologije – 3

Vsi naslovi so prevedeni v slovenski jezik in dostopni na SIR internetni strani!

## Hierarhija pravil notranjega revidiranja Druga raven - priporočljivo

### Priporočljivi del Okvira mednarodnih strokovnih ravnanj – PG – strokovna navodila

- Merjenje uspešnosti in učinkovitosti notranje revizije
- Presojanje ustreznosti ravnanja s tveganjem
- Notranje revidiranje in prevare
- Revidiranje zunanjih poslovnih povezav
- Oblikovanje in izražanje mnenj notranje revizije
- Ovrednotenje družbene odgovornosti/trajnostnega razvoja gospodarske družbe
- Revidiranje plače in posebnih ugodnosti poslovođnikov
- NRP - Uveljavljanje, ovrednotenje izvedbe in prenehanje
- Podpiranje delovanja malega notranjerevizijskega izvajalca v skladu z izvajanjem mednarodnih standardov strokovnega ravnanja pri notranjem revidiranju

## Hierarhija pravil notranjega revidiranja Druga raven - priporočljivo

Priporočljivi del Okvira mednarodnih strokovnih ravnanj – GTAG – Global Technology Audit Guide – Navodila za revizijo globalne informacijske tehnologije

- PG GTAG-1 Kontrole informacijske tehnologije (Information Technology Controls)
- PG GTAG-2 Sprememba in popravek poslovodskih kontrol: odločilno za uspeh organizacije (Change and Patch Management Controls: Critical for Organizational Success)
- PG GTAG-3 Nprekinjeno revidiranje: posledice za zagotovitev, spremljanje in oceno tveganja (Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment)
- PG GTAG-4 Poslovođenje revidiranja informacijske tehnologije (Management of IT Auditing)
- PG GTAG-5 Ravnanje s tveganji in revidiranje v zvezi z zasebnostjo (Managing and Auditing Privacy Risks)
- PG GTAG-6 Ravnanje z občutljivostjo informacijske tehnologije in njeno revidiranje (Managing and Auditing IT Vulnerabilities)
- PG GTAG-7 Zunanje izvajanje informacijske tehnologije (Information Technology Outsourcing)

## Hierarhija pravil notranjega revidiranja Druga raven - priporočljivo

Priporočljivi del Okvira mednarodnih strokovnih ravnanj – GTAG – Global Technology Audit Guide – Navodila za revizijo globalne informacijske tehnologije

- PG GTAG-8 Revidiranje kontrol uporabnostnih rešitev (Auditing Application Controls)
- PG GTAG-9 Obvladovanje prepoznavanja in dostopa (Identity and Access Management)
- PG GTAG-10 Obvladovanje trajnosti poslovanja (Business Continuity Management)
- PG GTAG-11 Razvijanje načrta revizije informacijske tehnologije (Developing the IT Audit Plan)
- PG GTAG-12 Revidiranje projektov informacijske tehnologije (Auditing IT Projects)
- PG GTAG-13: Preprečevanje prevar in njihovo odkrivanje v avtomatiziranem svetu (Fraud Prevention and Detection in an Automated World)
- PG GTAG-14: Revidiranje uporabniških računalniških rešitev (Auditing User-developed Applications)
- PG GTAG-15 Upravljanje celovitosti informacije (Information Security Governance)

## Hierarhija pravil notranjega revidiranja Druga raven - priporočljivo

Priporočljivi del Okvira mednarodnih strokovnih ravnanj – GAIT - Guide to the Assessment of IT Risk – Navodila za oceno tveganja informacijske tehnologije

- PG GAIT Metodika navodil za oceno tveganja informacijske tehnologije (The GAIT Methodology)
- PG GAIT Navodilo za oceno splošne pomanjkljivosti obvladovanja tveganj informacijske tehnologije (GAIT for IT General Control Deficiency)
- PG GAIT Navodilo za poslovanje in tveganje informacijske tehnologije (GAIT for Business and IT Risk)

## Hierarhija pravil notranjega revidiranja Druga raven - priporočljivo

### Pojasnila in stališča Strokovnega sveta Inštituta

- Končno poročanje o izsledkih posla:
  - namenjeno tistim, ki lahko na podlagi ugotovitev in priporočil izboljšajo obvladovalno okolje in pripomorejo k obvladovanju tveganj in
- Olistinjenje informacij – Razvidi o poslu:
  - v primeru, da notranje revidiranje izvaja zunanji izvajalec, se gradivo lahko hrani pri naročniku ali pri izvajalcu.
- v obravnavi – zunanje opravljanje notranjerevizijske dejavnosti

## Hierarhija pravil notranjega revidiranja Druga raven - priporočljivo

### Pojasnila in stališča Strokovnega sveta Inštituta

- v obravnavi – zunanje opravljanje notranjerevizijske dejavnosti:
  - komu je namenjeno
  - kaj želimo doseči
  - kaj se pričakuje od zunanjega izvajalca
  - odgovornosti in pristojnosti NPR
  - odgovornosti in pristojnosti zunanjega izvajalca
  - delovno gradivo
  - pogodbeno določila

#### Pojasnila in stališča Strokovnega sveta Inštituta

- predlogi na odboru Sekcije za notranjo revizijo ali s strani notranjih revizorjev
- osnutek gradiva in usklajevanje na odboru
- javna obravnava
- pripombe slovenskih inštitucij
- potrditev – strokovni svet inštituta in objava v Ur.l.

**Hvala!**

[tina.tomanpfajfar@kd-group.si](mailto:tina.tomanpfajfar@kd-group.si)