Svetovalni napotek 2200-2: Uporaba deduktivnega (angl. top-down) na tveganju zasnovanega prepoznavanja kontrol, ki jih je treba oceniti pri poslu notranje revizije

Temeljni standard v tej zvezi
2200 – Načrtovanje posla
Notranji revizorji morajo pripraviti in dokumentirati načrt za vsak posel, vključno z njegovimi cilji, obsegom, časom in razporeditvijo virov.

---

1. Preberite ta svetovalni napotek v povezavi s svetovalnimi napotki 2010-2: *Uporaba upravljanja tveganj pri načrtovanju notranje revizije*, 2210-1: *Cilji posla* in 2210.A1-1: *Ocena tveganj pri načrtovanju posla* in strokovnim navodilom *Smernica za poslovna tveganja in tveganja IT* (GAIT-R)

2. Ta svetovalni napotek predpostavlja, da so cilji posla notranje revizije določeni in da so bila pri načrtovanju notranje revizije tveganja prepoznana. Daje navodilo za uporabo deduktivnega, na tveganju zasnovanega načina prepoznavanja ključnih kontrol za upravljanje tveganj in jih vključuje v obseg posla (Standard 2220).

3. "Deduktivnost" se nanaša na dejstvo, da je obseg posla opredeljen glede na pomembnejša tveganja organizacije. To je v nasprotju s pripravo obsega posla na podlagi tveganj na določenem mestu, ki morda niti niso pomembna za organizacijo kot celoto. Deduktivni način (od zgoraj navzdol) zagotavlja, da je notranje revidiranje osredotočeno, kot je zapisano v svetovalnem napotku 2010-2, na »dajanje zagotovila glede upravljanja pomembnih tveganj«.

4. Sistem notranjega kontroliranja običajno vključuje ročne in samodejne kontrole. (Upoštevajte, da to velja za kontrole na katerikoli ravni – organizacije, poslovnega procesa in splošne kontrole informacijske tehnologije – ter za katero koli plast kontrolnega ogrodja; aktivnosti v kontrolnem okolju, pri spremljanju ali pri presojanju tveganj so na primer lahko tudi samodejne.) Da bi ugotovili, ali se poslovna tveganja uspešno upravljajo, je treba oceniti obe vrsti kontrol. Zlasti pa mora notranji revizor presoditi, ali obstaja ustrezna kombinacija kontrol, vključno s tistimi, ki se nanašajo na informacijsko tehnologijo, da se poslovna tveganja zmanjšajo v meje dopustnega tveganja za organizacijo. Notranji revizor mora proučiti postopke presojanja in potrditi, da je dopustni razpon tveganja običajen in primeren.

5. Obseg notranje revizije mora zajemati vse kontrole, ki so potrebne za dajanje sprejemljivega zagotovila o uspešnem upravljanju tveganj (ob upoštevanju pripomb iz 9. odstavka v nadaljevanju). Take kontrole veljajo za ključne kontrole – tiste, ki so potrebne za upravljanje tveganj, povezanih s ključnim poslovnim ciljem. Oceniti je treba samo ključne kontrole, čeprav se notranji revizor lahko odloči, da vključiti v presojo tudi neključne kontrole (npr. odvečne, podvojene kontrole), če oceni, da je takšno zagotovilo koristno za poslovanje. Notranji revizor se lahko pogovori z vodstvom, ali je potrebna tudi ocena neključnih kontrol.

6. Upoštevajte, da so tam, kjer ima organizacija dobro razvit in učinkovit program upravljanja tveganj, opredeljene ključne kontrole, na katere se je treba opreti pri upravljanju vsakega prepoznanega tveganja. V takih primerih mora notranji revizor presoditi, ali poslovodstvo ustrezno prepozna in oceni ključne kontrole.

7 Ključne kontrole imajo lahko naslednje oblike:

- kontrole na ravni organizacije (npr., zaposlenci so usposobljeni in opravijo preizkus, da potrdijo poznavanje kodeksa ravnanja). Kontrole na ravni organizacije so lahko ročne, povsem samodejne ali delno samodejne;
- ročne kontrole v poslovnem procesu (npr. izvedba fizičnega popisa zalog);
- povsem samodejne kontrole v poslovnem procesu (npr. uskladitev ali posodobitev kontov v glavni knjigi);
- delno samodejne kontrole v poslovnem procesu (imenovane tudi "hibridne" ali od informacijske tehnologije odvisne kontrole), kjer se sicer ročna kontrola opira na delovanje uporabniške rešitve računalniškega programa, kot je poročilo o odmiku. Če napaka pri delovanju ne bi bila odkrita, bi bila celotna kontrola neuspešna. Ključna kontrola za odkrivanje dvakratnega plačila lahko na primer vključuje pregled sistemsko generiranega poročila. Ročni del kontrole ne bi zagotovil, da je poročilo popolno. Zato mora biti omogočena tudi ocena delovanja računalniškega programa, ki je ustvaril poročilo.

Notranji revizor lahko uporablja tudi druge metode ali ogrodja, pomembno je le, da so ugotovljene in ocenjene vse ključne kontrole, na katere se organizacija zanaša pri upravljanju tveganj, vključno z ročnimi, samodejnimi kontrolami in kontrolami v okviru splošnih postopkov kontroliranja informacijske tehnologije.

8. Povsem in delno samodejne kontrole na ravni organizacije ali poslovnega procesa so na splošno oprte na pravilne zasnove in na uspešno delovanje splošnih kontrol informacijske tehnologije. Smernica GAIT-R obravnava priporočene postopke za prepoznavanja ključnih splošnih kontrol informacijske tehnologije.

9. Presoja ključnih kontrol je lahko opravljena z enim samim celovitim notranjerevizijskim poslom ali v povezavi z več notranjerevizijskimi posli. En notranjerevizijski posel se na primer lahko ukvarja s ključnimi kontrolami, ki jih opravljajo uporabniki poslovnega procesa, medtem ko drug posel pokriva ključne splošne kontrole informacijske tehnologije, tretji pa presoja ustreznost kontrol, ki delujejo na ravni organizacije. To je običajno, kadar se na iste kontrole (zlasti tiste na ravni organizacije ali v okviru splošnih kontrol informacijske tehnologije) opiramo na več področjih tveganja, in ne samo na enem.

10. V petem odstavku je navedeno, da je treba pred dajanjem mnenja o uspešnosti upravljanja tveganj na področju, ki ga pokriva obseg notranje revizije, oceniti kombinacijo ključnih kontrol. Tudi če je presoja razdeljena na več notranjerevizijskih poslov, od katerih vsak obravnava le nekatere ključne kontrole, mora notranji revizor vključiti v obseg najmanj enega notranjerevizijskega posla presojo zasnove ključnih kontrol kot celote (to je povezavo za vse opravljene posle pregleda kontrol), skupaj s presojo, ali so zadostne za upravljanje tveganj v mejah dopustnih tveganj v organizaciji.

11. Če obseg notranje revizije (z upoštevanjem drugih notranjerevizijskih poslov, obravnavanih v 9. odstavku) vključuje nekatere ključne kontrole, vendar ne vseh, ki so potrebne za upravljanje ciljnih tveganj, je treba upoštevati omejitev obsega in o tem jasno poročati v notranjerevizijskem obvestilu in končnem poročilu.

Objavljeno aprila 2010.

***