

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

220 – Načrtovanje posla

Notranji revizorji morajo razvijati in olistiniti načrt vsakega posla, vključno z njegovimi cilji, obsegom, časom ter razporeditvijo dejavnikov.

1. Proučite ta svetovalni napotek v povezavi s svetovalnimi napotki 2010-2: Uporaba ravnanja s tveganjem pri načrtovanju notranje revizije, 2210-1: Cilji posla, in 2210.A1-1: Presoja tveganja pri načrtovanju posla in svetovalna navodila za tveganje pri poslovanju in informacijski tehnologiji (GAIT-R).
2. Ta svetovalni napotek predpostavlja, da so cilji posla notranje revizije določeni in da so pri načrtovanju notranje revizije prepoznana nastala tveganja. Usmerja uporabo deduktivnega na tveganju zasnovanega načina prepoznavanja in vključuje v obseg posla (standard 2220) ključne kontrole za obvladovanje tveganj.
3. "Deduktivnost" usmerja temeljni obseg opredelitve na pomembnejša tveganja organizacije. To je v nasprotju z razvijanjem obsega, zasnovanega na tveganjih posameznih vrst, ki ne utegnejo biti pomembna za organizacijo kot celoto. Deduktivni način zagotavlja, da je notranje revidiranje osredotočeno, kot je zapisano v svetovalnem napotku 2010-2, na "dajanje zagotovil za ravnanje s pomembnimi tveganji".
4. Ureditev notranjega kontroliranja praviloma vključuje ročne in samodejne kontrole. (Upoštevajte, da se to nanaša na kontrole na katerikoli ravni – organizacije, poslovnega procesa in splošne kontrole informacijske tehnologije – ter na katerikoli sloj kontrolnega ogrodja; na primer, dejavnosti v kontrolnem okolju, spremljanju ali sloju presojanja tveganja so lahko tudi samodejne). Opravljena mora biti presoja obeh vrst kontrol, da bi ugotovili, ali obstaja uspešno ravnanje s poslovnimi tveganji. Zlasti pa mora notranji revizor presoditi, ali obstaja ustrezna kombinacija kontrol, vključno s tistimi, ki se nanašajo na informacijsko tehnologijo, da ublažijo poslovna tveganja v dopustni razpon za organizacijo. Notranji revizor mora proučiti postopke presojanja in potrditi, da je dopustni razpon tveganja običajen in ustrezen.
5. Obseg notranje revizije mora zajemati vse kontrole, ki so potrebne za dajanje upravičenih zagotovil o uspešnem ravnanju s tveganji (predmet pojasnil je v 9. členu v nadaljevanju). Take kontrole so obravnavane kot ključne kontrole – tiste, ki neizogibno obravnavajo tveganja, povezana s ključnim poslovnim ciljem. Samo ključne kontrole je treba presoditi, čeprav se lahko notranji revizor odloči vključiti v presojo tudi neključne kontrole (npr. odvečne, ponavljajoče se kontrole), če oceni, da imajo takšna zagotovila vrednost za poslovanje. Notranji revizor se lahko tudi pogovori s poslovodstvom, če so neključne kontrole potrebne.
6. Upoštevajte, da se tam, kjer ima organizacija dobro razvit in učinkovit program ravnanja s tveganjem, ključne kontrole zanašajo na ravnanje z vsakim prepoznanim tveganjem. V takih primerih mora notranji revizor presoditi, ali sta prepoznavanje poslovodstva in presojanje ključnih kontrol ustrezna.

7. Ključne kontrole imajo lahko naslednje oblike:

Kontrole na ravni organizacije (npr., zaposleni so usposobljeni in opravijo preizkus svojega razumevanja kodeksa ravnanja). Kontrole na ravni organizacije so lahko ročne, povsem samodejne ali delno samodejne.

Ročne kontrole v okviru poslovnega procesa (npr. izpolnitev ali popis zalog).

Povsem samodejne kontrole v okviru poslovnega procesa (npr. uskladitev ali posodobitev kontov v glavni knjigi).

Delno samodejne kontrole v okviru poslovnega procesa (označene tudi kot "hibridne" ali od informacijske tehnologije odvisne kontrole), kjer se siceršnja ročna kontrola opira na delovanje uporabniške rešitve računalniškega programa, kot je poročilo o odmiku. Če napaka pri delovanju ni odkrita, utegne biti celotna kontrola neuspešna. Na primer, ključna kontrola odkrivanja dvakratnega plačila lahko vključuje pregled poročila, ki ga zagotavlja ureditev. Ročni del kontrol ne zagotavlja, da je poročilo popolno. Zato mora biti omogočena presoja delovanja računalniškega programa, ki vzpostavlja poročilo.

Notranji revizor lahko uporablja tudi druge metode ali ogrodja, dokler niso ključne kontrole ravnanja s tveganji, na katere se zanaša, prepoznane in presojene, vključno z ročnimi, samodejnimi kontrolami in kontrolami v okviru splošnih postopkov informacijske tehnologije.

8. Povsem in delno samodejne kontrole – ali na ravni organizacije ali poslovnega procesa – so na splošno odvisne od pravilne zasnove in uspešnega delovanja splošnih kontrol informacijske tehnologije. GAIT-R obravnava priporočene postopke prepoznavanja ključnih splošnih kontrol informacijske tehnologije.
9. Presoja ključnih kontrol je lahko opravljena s posebnim, sestavljenim notranjerevizijskim poslom revizije ali v povezavi več notranjerevizijskih poslov. Na primer, posamezni notranjerevizijski posel se lahko ukvarja s ključnimi kontrolami, ki jih opravljajo uporabniki poslovnega procesa, medtem ko drugi pokriva ključne splošne kontrole informacijske tehnologije, tretji pa se nanaša na presojo ustreznosti kontrol, ki delujejo na ravni organizacije. To je običajno, kadar se sklicujemo na iste kontrole (zlasti tiste na ravni organizacije ali v okviru splošnih kontrol informacijske tehnologije) na več področjih tveganja, ne samo na enem.
10. V 5. členu je navedeno, da je treba pred dajanjem mnenja o uspešnosti ravnanja s tveganjem na področju, ki ga pokriva notranja revizija, presoditi povezanost ključnih kontrol. Celo pri izvedbi večkratnih notranjerevizijskih poslov, pri katerih se vsak ukvarja z nekaterimi ključnimi kontrolami, mora notranji revizor vključiti v obseg najmanj enega notranjerevizijskega posla presojo zasnove ključnih kontrol kot celote (tj. prek povezanih notranjerevizijskih poslov), in če je primerno, izpeljati ravnanje s tveganji v obsegu dopustnega razpona v organizaciji.
11. Če področje notranje revizije (z upoštevanjem drugih notranjerevizijskih poslov, kot je obravnavano v 9. členu) vključuje nekatere, vendar ne vseh ključnih kontrol, ki so potrebne pri ravnanju s ciljnim tveganji, je treba upoštevati omejitev obsega in o tem jasno poročati v notranjerevizijskih objavah in končnem poročilu.