

Organizacijska odpornost

Tematska zahteva

Topical Requirement



The Institute of
Internal Auditors

Prevedel:



The Institute of Internal Auditors
Združenje notranjih revizorjev
IIA – Slovenski inštitut
Slovenia

Tematska zahteva: Organizacijska odpornost

Mednarodni okvir strokovnega ravnanja (International Professional Practices Framework[®]) sestavljajo Globalni standardi notranjega revidiranja™ (Global Internal Audit Standards™), Tematske zahteve in Globalne smernice. Tematske zahteve so obvezne in se morajo uporabljati skupaj s Standardi, ki so uradna podlaga za zahtevane prakse.

Tematske zahteve določajo jasna pričakovanja za notranje revizorje, saj določajo osnovne ravni za revidiranje določenih področij tveganj. Profil tveganja organizacije lahko od notranjih revizorjev zahteva, da upoštevajo dodatne vidike te teme, vključno z lokalnimi predpisi.

Skladnost s Tematskimi zahtevami bo povečala doslednost izvajanja storitev notranjega revidiranja in izboljšala kakovost ter zanesljivost storitev in izidov notranjega revidiranja. Navsezadnje tematske zahteve dvigujejo stroko notranjega revidiranja.

Notranji revizorji morajo upoštevati Tematske zahteve v skladu z Globalnimi standardi notranjega revidiranja. Skladnost s Tematskimi zahtevami je obvezna za storitve dajanja zagotovil in priporočljiva za svetovalne storitve.

Tematska zahteva se uporablja, kadar je tema ena od naslednjih:

- Predmet posla v notranjerevizijskem načrtu.
- Prepoznana med izvajanjem posla.
- Predmet naročenega posla, ki ni bil v prvotnem notranjerevizijskem načrtu.

Vseh posameznih zahtev ni mogoče uporabiti pri vsakem poslu, nekatere pa je mogoče izpolniti z drugimi pristopi. Če je zahteva izključena ali nadomeščena z drugimi regulativnimi ali pogodbenimi zahtevami ali obravnavana z izvajanjem postopkov v skladu z Globalnimi standardi notranjega revidiranja, je treba utemeljitev dokumentirati in shraniti. Skladnost bo ocenjena v okviru presoje kakovosti.

Za več informacij glejte Uporabniški priročnik za Tematsko zahtevo Organizacijska odpornost.

Organizacijska odpornost

Mednarodna organizacija za standardizacijo opredeljuje organizacijsko odpornost kot "sposobnost organizacije, da sprejema in se prilagaja spreminjajočemu se okolju" (ISO 22316:2017). Čeprav ta opredelitev predstavlja jasno težnjo, se organizacije v praksi močno razlikujejo glede tega, kako predvidevajo spremembe in motnje, se nanje odzivajo, se jim prilagajajo in po njih okrevajo. Ker organizacijska odpornost zajema strateške, delovne, tehnološke, človeške, družbene in finančne razsežnosti, lahko nekatere organizacije uspešno sprejemajo spremembe, medtem ko se druge s tem težje spoprijemajo ali pa se ob negotovosti odločijo za drugačne pristope.

Organizacijska odpornost je krovni izraz, ki obravnava tveganja, ki lahko bistveno ovirajo ali zmanjšajo zmožnost organizacije za zagotavljanje osrednjih izdelkov in storitev, ohranjanja zaupanja deležnikov ali izpolnjevanja strateških ciljev. Ta tveganja so lahko posledica nenadnih dogodkov (kot so naravne nesreče, kibernetiki napadi in geopolitični spori), dolgotrajnih okoljskih pritiskov (kot so pomanjkanje virov in krize na področju javnega zdravja) ali sprememb v zunanjem okolju (kot so tehnološke motnje, regulativne spremembe in okrnitev ugleda).

Ta tveganja so lahko tudi postopne spremembe ali počasi nastajajoči pritiski, ki sčasoma ogrozijo stabilnost organizacije in njeno sposobnost prilagajanja. Takšna postopna naraščajoča tveganja so pogosto spregledana. Odporne organizacije predvidevajo in se prilagajajo tako nenadnim kot manj očitnim tveganjem, da bi bile uspešne.

Vgrajeni dejavniki tveganja, ki povečujejo grožnje odpornosti, vključujejo zelo zapletene dejavnosti, globalizirane dobavne verige, centralizirano infrastrukturo ali podatkovne sisteme, omejeno razpoložljivost delovne sile, nestabilne tržne razmere in močno odvisnost od ključnih tretjih oseb ali geografskih lokacij. Organizacije v panogah, kjer je zanesljivost ključnega pomena ali tiste, ki delujejo pod strogim regulativnim nadzorom, se lahko soočajo tudi s tveganji, ki so zaradi javnega vpliva in obveznosti zagotavljanja skladnosti že po naravi večja.

Organizacijska odpornost se osredotoča na obvladovanje tveganj pred motnjami, med njimi in po njih. Notranji revizorji pogosto ocenjujejo procese in kontrole informacijske tehnologije (IT) v zvezi z neprekinjenim poslovanjem in obnovitvijo po nesreči. V načrtu neprekinjenega poslovanja so podrobno opisani ukrepi, ki jih organizacija sprejme za zagotavljanje ključnih funkcij in ponovno vzpostavitev normalnega delovanja v primeru nesreče. Načrt za obnovo po nesreči opisuje, kako bodo organizacije po dogodku, ki povzroča motnje v poslovanju, obnovile svoje informacijske sisteme, ključne podatke in delovanje, da bi ponovno vzpostavile običajno poslovanje.

Organizacijska odpornost, ki vključuje oba načrta, zahteva strateško načrtovanje, celovito obvladovanje tveganj, uspešno vodenje in kulturo ter kontrolne procese v celotni organizaciji. Strožji kontrolni procesi za organizacijsko odpornost organizacijam ne omogočajo le nenehnega predvidevanja, pripravljanja, odzivanja in prilagajanja na spremembe, temveč jim omogočajo tudi preživetje in razvoj.



Vrednotenje in ocenjevanje upravljanja, obvladovanja tveganj in kontrolnih procesov organizacijske odpornosti

Ta Tematska zahteva zagotavlja dosleden in celovit pristop k ocenjevanju zasnove in izvajanju upravljanja, obvladovanju tveganj in kontrolnih procesov organizacijske odpornosti. Zahteve predstavljajo minimalno osnovno raven za ocenjevanje organizacijske odpornosti.

Upravljanje

Zahteve

Notranji revizorji morajo oceniti naslednje vidike upravljanja organizacijske odpornosti:

- A.** Vodstvo vzpostavi uradno strategijo, ki naslavlja organizacijsko odpornost, organ nadzora jo sprejme in nadzira in vključuje delovne, tehnološke in finančne gradnike, potrebne za obvladovanje sprememb in nadaljevanje poslovanja. Cilji odpornosti so usklajeni s celovitim pristopom organizacije k obvladovanju tveganj.
- B.** O napredku pri doseganju ciljev odpornosti se obdobno poroča organu nadzora v pregled. To zagotavlja, da je odpornost vgrajena v strateški nadzor, procese dolgoročnega načrtovanja, načrtovanje nasledstev in organizacijsko kulturo, vključno z viri in proračunskimi zahtevami za podporo ključnih poslovnih dejavnosti.
- C.** Z namenom okrepitve kontrolnega okolja so vzpostavljene politike in postopki za ključne delovne, tehnološke in finančne procese. Politike in postopki se redno pregledujejo, preizkušajo in po potrebi posodablajo.
- D.** Za izredne razmere je vzpostavljena struktura vodenja. Uporablja se za nadzor in podporo ciljem organizacijske odpornosti. Le-ta opredeljuje hierarhije odločanja, protokole sporočanja in prenosa na višjo raven odločanja in vodstvene in delovne vloge ter odgovornosti.
- E.** Vzpostavljen je proces za redno potrjevanje kompetenc, potrebnih za uspešno odpornost, in večkratno ocenjevanje kompetenc posameznikov, ki opravljajo ključne vloge v procesih odpornosti.
- F.** Vzpostavljen je proces, ki zagotavlja, da so vsi primerni notranji in zunanji deležniki prepoznani, prednostno razvrščeni in vključeni v vzpostavitev informacijskih in poročevalskih struktur za doseganje ciljev organizacijske odpornosti. Deležniki lahko vključujejo poslovodstvo, operativne funkcije, obvladovanje tveganj, informacijsko tehnologijo, nabavno službo, obvladovanju objektov, kadrovske službe, finance, pravno službo, izvajalce storitev dajanja zagotovil (vključno z notranjo revizijo), skladnost poslovanja, odnose z javnostmi, ključne dobavitelje, kupce, regulatorje in druge.



Obvladovanje tveganj

Zahteve

Notranji revizorji morajo oceniti naslednje vidike obvladovanja tveganj organizacijske odpornosti:

- A.** Tveganja, povezana z organizacijsko odpornostjo, se redno prepoznavajo, ocenjujejo in obvladujejo v celotni organizaciji. Tveganja odpornosti so usklajena s strateškimi cilji organizacije. Proces obvladovanja tveganj odpornosti vključuje ocenjevanje ključnih procesov.
- B.** Pristojnosti in odgovornosti za obvladovanje tveganj organizacijske odpornosti so jasno opredeljene. Za redno spremljanje in poročanje o obvladovanju tveganj organizacijske odpornosti, vključno z viri, potrebnimi za blažitev tveganj, ter prepoznavanjem novih groženj za organizacijsko odpornost, se imenuje oseba ali skupina.
- C.** Vzpostavljen je proces za spremljanje ravni tveganj organizacijske odpornosti (nastajajočih ali že prepoznanih) ter hitro sporočanje na višjo stopnjo odločanja tistih tveganj, ki dosežejo nesprejemljivo raven glede na vzpostavljene smernice organizacije za obvladovanje tveganj in mejo dopustnega tveganja ali glede na veljavne zakonske in regulativne zahteve. Upoštevani so vplivi tveganja organizacijske odpornosti.
- D.** Vodstvo je vzpostavilo in redno preizkuša proces za odzivanje na krize, motnje in izredne razmere ter okrevanje po njih. Proces odzivanja na incidente in obnovitve vključuje zaznavanje, določanje prednostnih nalog, zamejitev, obnovitev in analizo po incidentu. Pristop k odzivanju na incidente vključuje analize scenarijev in obdobja obremenitvena testiranja za različne dogodke, ki bi lahko povzročili motnje v poslovanju.

Kontrolni procesi

Zahteve

Notranji revizorji morajo oceniti naslednje vidike kontrolnih procesov, povezanih z organizacijsko odpornostjo:

- A.** Vzpostavljen je proces za prepoznavanje ključnih tretjih oseb (dobaviteljev in ponudnikov) in določitev minimalnih ravni zalog, ki so potrebne za zagotavljanje delovanja ključnih dejavnosti. Proces vključuje tudi vodenje posodobljenega seznama rezervnih dobaviteljev.
- B.** Podatki, ki so ključni za delovanje, so prepoznani in razvrščeni. Razvrstitev podatkov vključuje opredelitev, kje se podatki nahajajo, kdo potrebuje dostop do njih, kako se do njih dostopa ter ali so varnostno kopirani in jih je mogoče obnoviti v izrednih razmerah.
- C.** Vzpostavljene so ključne kontrole informacijske tehnologije in neprekinjeno spremljanje za zmanjšanje tveganj informacijske varnosti (vključno s kibernetскими tveganji) ter zagotavljanje zaščite občutljivih podatkov med krizami, motnjami in izrednimi razmerami. Kontrole in neprekinjeno spremljanje vključujejo obveščanje o grožnjah v dejanskem času in omejevanje dostopa samo na pooblaščen uporabnike.
- D.** Izvede se popis ključnih sredstev informacijske tehnologije. Sredstva vključujejo strojno in programsko opremo ter storitve, potrebne za podporo delovanja v krizah, motnjah in izrednih razmerah.



- E. Vzpostavljeni so načrti za neprekinjeno poslovanje in obnovitev po nesreči, ki vključujejo opredeljene vloge osebja in skupin dodeljenih za obnovo. Načrti se obdobno preizkušajo (na primer z "namizno vajo"), o izidih preizkušanja, vključno z možnostmi izboljšav, pa se poroča organu nadzora in poslovodstvu.
- F. Vzpostavljen je proces za prilagoditev delovnega okolja v času kriz, motenj in izrednih razmer.
- G. Vzpostavljen je proces za neprekinjeno spremljanje in poročanje o nastajajočih grožnjah in ranljivostih, ki bi lahko vplivale na organizacijsko odpornost. Proces se uporablja za prepoznavanje, prednostno razvrstitev in uvajanje izboljšav na področju organizacijske odpornosti, vključno s sistemi za prijavljanje nepravilnosti ali zbiranje informacij o tveganjih.
- H. Vzpostavljen je proces za izobraževanje in usposabljanje osebja v zvezi z organizacijsko odpornostjo, ki zagotavlja, da so seznanjeni s politikami in postopki, ki jih je treba upoštevati, ter z ukrepi, ki jih je treba sprejeti ob pojavu kriz, motenj in izrednih razmer. Proces vključuje vaje za usposabljanje, v katerih se ponazarjajo scenariji, ki povzročajo motnje v poslovanju.
- I. Vzpostavljen je proces, ki zagotavlja, da so potrebna delovna, kadrovska, tehnološka in finančna sredstva zagotovljena v proračunu in na voljo v času kriz, motenj in izrednih razmer. Finančna sredstva, potrebna za podporo organizacijski odpornosti, se redno analizirajo in sporočajo organu nadzora.
- J. Vzpostavljen je proces za pregled kriz, motenj in izrednih razmer po njihovem nastanku ter za analizo pregledov po incidentu v okviru procesa učenja iz izkušenj, vključno z vključevanjem pridobljenih spoznanj v prihodnje načrtovanje organizacijske odpornosti.

O Inštitutu notranjih revizorjev (IIA)

Inštitut notranjih revizorjev (IIA) je mednarodno strokovno združenje, ki združuje več kot 265.000 članov po vsem svetu in je podelilo več kot 200.000 strokovnih nazivov Certified Internal Auditor® (CIA®) po vsem svetu. Inštitut IIA je bilo ustanovljeno leta 1941 in je globalno priznано kot vodilno združenje na področju standardov, strokovnih nazivov, izobraževanja, raziskav in tehničnega vodenja notranje revizije. Za več informacij obiščite theiia.org.

Avtorske pravice

© 2026 The Institute of Internal Auditors, Inc. Vse pravice pridržane. Za dovoljenje za reprodukcijo se obrnite na copyright@theiia.org.

April 2026



The Institute of
Internal Auditors

Globalni sedež

1035 Greenwood Blvd., soba 401
Lake Mary, FL 32746 ZDA
Telefon: +1-407-937-1111
Faks: +1-407-1101

