

Organizacijska otpornost

Tematski zahtjev

Topical Requirement



The Institute of
Internal Auditors

Tematski zahtjev za organizacijsku otpornost

Međunarodni okvir profesionalnog djelovanja (International Professional Practices Framework® - IPPF®) uključuje Globalne standarde interne revizije (Global Internal Audit Standards™), Tematske zahtjeve i Globalne smjernice. Tematski zahtjevi su obvezni i moraju se koristiti zajedno sa Standardima, koji predstavljaju mjerodavnu osnovu za zahtijevane prakse.

Tematski zahtjevi pružaju jasna očekivanja za interne revizore postavljanjem minimalne osnove za reviziju određenih tema vezanih uz rizike. Profil rizika organizacije može zahtijevati od internih revizora da razmotre i dodatne aspekte pojedine teme, uključujući lokalne propise.

Sukladnost s tematskim zahtjevima povećat će dosljednost s kojom se obavljaju usluge interne revizije te poboljšati kvalitetu i pouzdanost usluga i rezultata interne revizije. Naposljetku, tematski zahtjevi uzdižu profesiju interne revizije.

Interni revizori moraju primjenjivati tematske zahtjeve u skladu s Globalnim standardima interne revizije. Sukladnost s tematskim zahtjevima obvezna je za usluge izražavanja uvjerenja i preporučuje se za savjetodavne usluge.

Tematski zahtjev primjenjiv je kada je tema:

- predmet angažmana uključen u plan interne revizije
- identificirana tijekom provođenja angažmana
- predmet naknadnog zahtjeva za angažman koji nije bio uključen u prvobitni plan interne revizije.

Ne moraju se svi pojedinačni zahtjevi primjenjivati na svaki revizijski angažman, a neki se mogu ispuniti i drugim pristupima. Ako je određeni zahtjev isključen ili zamijenjen drugim regulatornim ili ugovornim zahtjevima ili je obuhvaćen provedbom postupaka u skladu s Globalnim standardima interne revizije, potrebno je dokumentirati i čuvati obrazloženje za takvo postupanje.

Sukladnost s Tematskim zahtjevom obvezna je i ocjenjivat će se tijekom procjena kvalitete.

Za više informacija pogledajte Korisnički vodič za primjenu Tematskog zahtjeva za organizacijsku otpornost.



Organizacijska otpornost

Međunarodna organizacija za standardizaciju - ISO (International Organisation for Standardization) definira organizacijsku otpornost kao „sposobnost organizacije da apsorbira promjene i prilagodi se promjenjivom okruženju” (ISO 22316:2017).

Iako ova definicija postavlja jasan cilj, u praksi se organizacije znatno razlikuju u načinu na koji predviđaju, reagiraju, prilagođavaju se i oporavljaju od promjena i poremećaja. Budući da organizacijska otpornost obuhvaća strateške, operativne, tehnološke, ljudske, društvene i financijske dimenzije, neke organizacije mogu učinkovito apsorbirati promjene, dok se druge s njima teže nose ili odabiru drugačije pristupe u uvjetima neizvjesnosti.

Organizacijska otpornost je krovni pojam koji obuhvaća rizike koji mogu značajno poremetiti ili ugroziti sposobnost organizacije da isporučuje svoje ključne proizvode i usluge, održava povjerenje dionika ili ostvaruje svoje strateške ciljeve. Ti rizici mogu proizaći iz iznenadnih događaja (poput prirodnih katastrofa, kibernetičkih napada i geopolitičkih sukoba), dugotrajnih pritisaka iz okruženja (poput nestašice resursa i kriza u javnom zdravstvu) ili promjena u vanjskom okruženju (poput tehnoloških poremećaja, regulatornih promjena i narušavanja ugleda).

Ti rizici mogu biti i postupne promjene ili polako rastući pritisci koji s vremenom narušavaju stabilnost organizacije i njezinu sposobnost prilagodbe. Takvi rizici koji se razvijaju postupno često mogu ostati nezapaženi tijekom rutinskih provjera ili procjena. Otporne organizacije predviđaju i prilagođavaju se kako iznenadnim tako i suptilnim rizicima kako bi bile uspješne.

Čimbenici inherentnih rizika koji povećavaju prijetnju organizacijskoj otpornosti uključuju vrlo složene operacije, globalne lance opskrbe, centraliziranu infrastrukturu ili podatkovne sustave, ograničenu dostupnost radne snage, nestabilne tržišne uvjete te veliku ovisnost o ključnim trećim stranama ili geografskim lokacijama. Organizacije koje djeluju u sektorima visoke pouzdanosti ili pod intenzivnim regulatornim nadzorom također se mogu suočavati s inherentno višim rizicima zbog utjecaja na javnost i obveza usklađenosti s propisima.

Organizacijska otpornost usmjerena je na upravljanje rizicima prije, tijekom i nakon poremećaja. Interni revizori uobičajeno procjenjuju procese i kontrole informacijske tehnologije (IT) povezane s kontinuitetom poslovanja i oporavkom od katastrofa.

Plan kontinuiteta poslovanja opisuje korake koje organizacija poduzima kako bi održala ključne funkcije i vratila se u uobičajeno operativno stanje nakon nastanka katastrofe. Plan oporavka od katastrofa opisuje način na koji će organizacija obnoviti svoje IT sustave, ključne podatke i poslovne operacije nakon ometajućeg događaja kako bi ponovno uspostavila redovno poslovanje.

Organizacijska otpornost, koja uključuje oba navedena plana, zahtijeva strateško planiranje, upravljanje rizicima na razini cijelog poduzeća, učinkovito vodstvo i organizacijsku kulturu te kontrolne procese na razini cijele organizacije. Snažni kontrolni procesi za organizacijsku otpornost ne samo da omogućuju organizacijama da kontinuirano predviđaju, pripremaju se za, reagiraju na i prilagođavaju se promjenama, nego im također omogućuju da opstanu i napreduju.

Vrednovanje i procjena procesa korporativnog upravljanja, upravljanja rizicima i kontrolnih procesa povezanih s organizacijskom otpornošću

Ovaj Tematski zahtjev pruža dosljedan i sveobuhvatan pristup procjeni dizajna i provedbe procesa korporativnog upravljanja, upravljanja rizicima i kontrolnih procesa povezanih s organizacijskom otpornošću.

Zahtjevi predstavljaju minimalnu osnovu za procjenu organizacijske otpornosti.

Korporativno upravljanje

Zahtjevi

Interni revizori moraju procijeniti sljedeće aspekte upravljanja organizacijskom otpornošću:

- A. Menadžment je uspostavio službenu strategiju za organizacijsku otpornost, koju je usvojio i nadzire odbor, a koja uključuje operativne, tehnološke i financijske elemente potrebne za upravljanje promjenama i osiguravanje kontinuiteta poslovanja. Ciljevi organizacijske otpornosti usklađeni su s cjelokupnim pristupom organizacije upravljanju rizicima.
- B. Informacije o ostvarenju ciljeva organizacijske otpornosti periodično se dostavljaju odboru na razmatranje. Time se osigurava da je organizacijska otpornost ugrađena u strateški nadzor, procese dugoročnog planiranja, planiranje nasljeđivanja ključnih funkcija te organizacijsku kulturu, uključujući planiranje i raspodjelu resursa i proračunski sredstava potrebnih za podršku kritičnim poslovnim aktivnostima.
- C. Uspostavljene su politike i procedure za kritične operativne, tehnološke i financijske procese te se periodično preispituju, testiraju i prema potrebi ažuriraju radi jačanja kontrolnog okruženja.
- D. Uspostavljena je struktura upravljanja incidentima koja se koristi za nadzor i podršku ostvarivanju ciljeva organizacijske otpornosti. Ona uključuje hijerarhiju donošenja odluka, protokole komunikacije i eskalacije te jasno definirane upravljačke i operativne uloge i odgovornosti.
- E. Uspostavljen je proces za periodičnu provjeru kompetencija potrebnih za uspješno ostvarivanje i upravljanje organizacijskom otpornošću te za ponovno procjenjivanje kompetencija osoba koje obnašaju ključne uloge u procesima upravljanja organizacijskom otpornošću.
- F. Uspostavljen je proces kojim se osigurava da su svi relevantni interni i vanjski dionici identificirani, prioritetno rangirani i uključeni u uspostavu informacijskih i izvještajnih struktura potrebnih za ostvarenje ciljeva organizacijske otpornosti. Dionici mogu uključivati viši menadžment, operacije, upravljanje rizicima, IT, lanac opskrbe i nabavu, upravljanje nekretninama i infrastrukturu, ljudske resurse, financije, pravne poslove, pružatelje usluga s izražavanjem uvjerenja (uključujući internu reviziju), funkciju usklađenosti, odnose s javnošću, ključne dobavljače, klijente, regulatore i druge relevantne strane.



Upravljanje rizicima

Zahtjevi

Interni revizori moraju procijeniti sljedeće aspekte upravljanja rizicima organizacijske otpornosti:

- A. Rizici povezani s organizacijskom otpornošću periodično se identificiraju, procjenjuju i njima se upravlja na razini cijele organizacije. Rizici organizacijske otpornosti povezani su sa strateškim ciljevima organizacije. Proces upravljanja rizicima organizacijske otpornosti uključuje procjenu ključnih poslovnih procesa.
- B. Krajnja odgovornost i operativna zaduženja za upravljanje rizicima organizacijske otpornosti jasno su definirani. Određena osoba ili tim zaduženi su za redovito praćenje i izvještavanje o upravljanju rizicima organizacijske otpornosti, uključujući resurse potrebne za ublažavanje rizika te prepoznavanje novih prijetnji organizacijskoj otpornosti.
- C. Uspostavljen je proces za praćenje razine rizika organizacijske otpornosti (novonastalih ili prethodno identificiranih rizika) te za njihovu brzu eskalaciju kada dosegnu razinu koju organizacija smatra neprihvatljivom, u skladu s utvrđenim smjernicama za upravljanje rizicima, prihvatljivom razinom rizika za organizaciju ili primjenjivim zakonskim i regulatornim zahtjevima. U obzir se uzimaju i posljedice rizika organizacijske otpornosti.
- D. Menadžment je uspostavio i periodično testira proces odgovora na krize, poremećaje i izvanredne situacije te oporavka nakon njihova nastanka. Proces odgovora na incidente i oporavka uključuje otkrivanje, određivanje prioriteta, ograničavanje posljedica, oporavak i analizu nakon incidenta. Pristup upravljanja i odgovora na incidente uključuje analize scenarija i periodično stresno testiranje otpornosti na različite vrste ometajućih događaja.

Kontrolni procesi

Zahtjevi

Interni revizori moraju procijeniti sljedeće aspekte kontrolnih procesa povezanih s organizacijskom otpornošću:

- A. Uspostavljen je proces za identificiranje ključnih trećih strana - pružatelja usluga (dobavljača i isporučitelja) te za određivanje minimalnih razina zaliha potrebnih za održavanje ključnih poslovnih aktivnosti. Proces također uključuje vođenje ažurnog popisa alternativnih dobavljača.
- B. Podaci ključni za poslovanje identificirani su i klasificirani. Klasifikacija podataka uključuje utvrđivanje mjesta pohrane podataka, osoba kojima je potreban pristup podacima, načina pristupa podacima te jesu li podaci sigurnosno kopirani i mogu li se obnoviti u slučaju izvanredne situacije.
- C. Uspostavljene su ključne IT kontrole i kontinuirani nadzor radi ublažavanja rizika informacijske sigurnosti (uključujući kibernetičke rizike) te zaštite osjetljivih podataka tijekom kriza, poremećaja i izvanrednih situacija. Kontrole i kontinuirani nadzor uključuju praćenje prijetnji u stvarnom vremenu te ograničavanje pristupa isključivo ovlaštenim korisnicima.
- D. Vodi se inventar ključne IT imovine. Imovina uključuje hardver, softver i usluge potrebne za podršku poslovnim operacijama tijekom kriza, poremećaja i izvanrednih situacija.



- E. Uspostavljeni su planovi kontinuiteta poslovanja i planovi oporavka od katastrofa koji uključuju jasno definirane uloge zaduženog osoblja i timova za oporavak. Planovi se periodično testiraju (primjerice, provođenjem vježbi temeljenih na simulaciji kriznih scenarija), a o rezultatima testiranja, uključujući mogućnosti za poboljšanje, izvještavaju se odbor i viši menadžment.
- F. Uspostavljen je proces za prilagodbu radnog okruženja tijekom kriza, poremećaja i izvanrednih situacija.
- G. Uspostavljen je proces za kontinuirano praćenje i izvještavanje o novim prijetnjama i ranjivostima koje mogu utjecati na organizacijsku otpornost. Proces se koristi za prepoznavanje, određivanje prioriteta i provedbu mjera za unapređenje organizacijske otpornosti, uključujući sustave za prijavu nepravilnosti ili prikupljanje i analizu informacija o rizicima (*risk intelligence*).
- H. Uspostavljen je proces edukacije i osposobljavanja zaposlenika o organizacijskoj otpornosti kojim se osigurava da su upoznati s politikama i procedurama koje trebaju slijediti te radnjama koje trebaju poduzeti u slučaju kriza, poremećaja i izvanrednih situacija. Proces uključuje vježbe obuke u kojima se simuliraju scenariji i situacije poremećaja u poslovanju.
- I. Uspostavljen je proces kojim se osigurava da su potrebni operativni, ljudski, tehnološki i financijski resursi planirani u proračunu i dostupni tijekom kriza, poremećaja i izvanrednih situacija. Financijski resursi potrebni za podršku organizacijskoj otpornosti periodično se analiziraju i o njima se izvještava odbor.
- J. Uspostavljen je proces za procjenu kriza, poremećaja i izvanrednih situacija nakon njihova nastanka te analizu rezultata naknadnih ocjena incidenata kroz postupak utvrđivanja “naučenih lekcija” pri čemu se stečene spoznaje ugrađuju u buduće planiranje organizacijske otpornosti.

O Institutu internih revizora

Institut internih revizora (The Institute of Internal Auditors -) IIA je međunarodna strukovna udruga koja broji više od 265.000 članova diljem svijeta i dodijelila je više od 200.000 certifikata ovlaštenog internih revizora® (CIA®) diljem svijeta. Osnovano 1941. godine, IIA je diljem svijeta priznata kao vodeća organizacija u struci internih revizora u području standarda, certifikacija, obrazovanja, istraživanja i tehničkih smjernica. Za više informacija posjetite <https://www.theiia.org>.

Autorska prava

© 2026 The Institute of Internal Auditors, Inc. Sva prava pridržana. Za dopuštenje za reproduciranje obratite se na copyright@theiia.org.

April 2026



The Institute of
Internal Auditors

Global Headquarters

1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-1101

