Organizacijska otpornost

Tematski zahtjev

Korisnički vodič

Topical Requirement

The Institute of
Internal Auditors

Sadržaj

Pregled Tematskih zahtjeva

Tematski zahtjevi su ključna komponenta Međunarodnog okvira profesionalnog djelovanja® uz Globalne standarde interne revizije™ i Globalne smjernice. Institut internih revizora zahtijeva da se Tematski zahtjevi koriste zajedno s Globalnim standardima (Standard 4.1 Usklađenost s Globalnim standardima interne revizije), koji pružaju mjerodavnu osnovu zahtijevanih praksi. Reference na Standarde pojavljuju se u ovom vodiču kao izvor detaljnijih informacija.

Tematski zahtjevi formaliziraju način na koji interni revizori rješavaju prevladavajuća rizična područja kako bi promovirali kvalitetu i dosljednost unutar profesije. Mandat interne revizije jasno definira opseg i vrste usluga koje obavlja funkcija interne revizije, što uključuje razmatranje Tematskih zahtjeva (Standard 6.1 Mandat interne revizije). Tematski zahtjevi uspostavljaju osnovu i pružaju relevantne kriterije za obavljanje usluga s izražavanjem uvjerenja povezanih s predmetom Tematskog zahtjeva (Standard 13.4 Kriteriji ocjenjivanja). Usklađenost s Tematskim zahtjevima obvezna je za angažmane s izražavanjem uvjerenja i preporučuje se za evaluaciju tijekom pružanja savjetodavnih usluga. Tematski zahtjevi nisu namijenjeni pokrivanju svih potencijalnih aspekata koje treba uzeti u obzir prilikom obavljanja angažmana s izražavanjem uvjerenja, već su namijenjeni pružanju minimalnog skupa zahtjeva kako bi se omogućila dosljedna i pouzdana procjena teme.

Tematski zahtjevi jasno se povezuju s IIA Modelom tri linije i Globalnim standardima interne revizije. Procesi korporativnog upravljanja, upravljanja rizicima i kontrole glavne su komponente Tematskih zahtjeva, usklađeni sa Standardom 9.1 Razumijevanje korporativnog upravljanja, upravljanja rizikom i kontrolnih procesa. U odnosu na Model tri linije, korporativno upravljanje se povezuje s odborom/upravljačkim tijelom, upravljanje rizicima se povezuje s drugim linijom, a kontrole ili kontrolni procesi s prvom linijom. Dok je menadžment predstavljen i u prvoj i u drugoj liniji, funkcija interne revizije prikazana je u trećoj liniji kao neovisni i objektivni pružatelj usluga s izražavanjem uvjerenja koji izvještava odbor/upravljačko tijelo (Načelo 8 pod nadzorom Odbora).

Primjenjivost, rizik i profesionalna prosudba

Tematski zahtjevi moraju se poštovati kada funkcije interne revizije provode angažmane s izražavanjem uvjerenja o temama za koje postoji Tematski zahtjev ili kada se aspekti Tematskog zahtjeva identificiraju unutar drugih angažmana s izražavanjem uvjerenja.

Kao što je opisano u Standardima, procjena rizika važan je dio planiranja rukovoditelja interne revizije. Određivanje angažmana s izražavanjem uvjerenja koji će se uključiti u plan interne revizije zahtijeva procjenu strategija, ciljeva i rizika organizacije najmanje jednom godišnje (Standard 9.4 Plan interne revizije). Prilikom planiranja pojedinačnih angažmana s izražavanjem uvjerenja, interni revizori moraju procijeniti rizike relevantne za angažman (Standard 13.2 Procjena rizika angažmana).

Kada se predmet Tematskog zahtjeva identificira tijekom procesa planiranja interne revizije temeljene na riziku i uključi u plan revizije, tada se zahtjevi navedeni u Tematskom zahtjevu moraju koristiti za procjenu teme unutar primjenjivih angažmana. Osim toga, kada interni revizori provode angažman (bilo da je uključen u plan ili nije) i pojave se elementi Tematskog zahtjeva, Tematski zahtjev mora se procijeniti radi primjenjivosti kao dio angažmana. Konačno, ako se zatraži provođenje angažmana koji izvorno nije bio u planu i angažman uključuje temu, Tematski zahtjev se mora se procijeniti radi primjenjivosti. (pogledajte Standard 9.4 dio koji se odnosi promjene u planu interne revizije).

Profesionalna prosudba igra ključnu ulogu u primjeni Tematskog zahtjeva. Procjene rizika utječu na odluke rukovoditelja interne revizije o tome koje angažmane uključiti u plan interne revizije (Standard 9.4). Osim toga, interni revizori koriste profesionalnu prosudbu kako bi odredili koji će aspekti biti obuhvaćeni svakim angažmanom (Standardi 13.3 Ciljevi i opseg angažmana, 13.4 Kriteriji ocjenjivanja i 13.6 Program rada angažmana) kao i kako bi identificirali potrebne resurse za realizaciju ciljeva angažmana (Standard 13.5 Resursi za angažman). Prilog A „Scenariji za primjenu Tematskog zahtjeva" opisuju način na koji interni revizori primjenjuju Tematski zahtjev.

Ne moraju se svi pojedinačni zahtjevi primjenjivati na svaki revizijski angažman, a neki se mogu ispuniti i na druge načine. Ako je zahtjev isključen ili nadomješten drugim regulatornim ili ugovornim zahtjevima ili je obuhvaćen provedbom postupaka u skladu sa Standardima, obrazloženje za takvo postupanje mora biti dokumentirano i čuvano. Usklađenost s Tematskim zahtjevima bit će ocijenjena u procjenama kvalitete.

Usklađenost s Tematskim zahtjevom mora se dokumentirati korištenjem profesionalne prosudbe revizora kako je opisano u Standardu 14.6 Dokumentacija angažmana.

Iako Tematski zahtjev pruža osnovu kontrolnih procesa koje treba uzeti u obzir, organizacije koje procjenjuju rizičnost teme kao vrlo visoku, možda će trebati procijeniti dodatne aspekte.

Ako rukovoditelj interne revizije utvrdi da funkcija interne revizije nema potrebne kompetencije za obavljanje revizijskih angažmana na temi koja je predmet tematskog zahtjeva, provođenje angažmana se može ugovoriti s vanjskim pružateljem usluga (Standardi 3.1 Kompetentnost, 7.2 Kvalifikacije rukovoditelja interne revizije, 10.2 Upravljanje ljudskim resursima). Rukovoditelj interne revizije može koristiti Okvir kompetencija za internu reviziju donesen od strane IIA kao koristan resurs. Standardi se primjenjuju na svaku osobu ili funkciju koja pruža usluge interne revizije, neovisno o tome da li organizacija zapošljava interne revizore izravno, ugovara ih s vanjskim pružateljem usluga ili oboje. Rukovoditelj interne revizije zadržava konačnu odgovornost za osiguravanje usklađenosti. Osim toga, ako rukovoditelj interne revizije utvrdi da su resursi interne revizije nedovoljni, rukovoditelj interne revizije mora obavijestiti odbor o utjecaju ograničenja resursa i o načinu rješavanja eventualnih nedostataka resursa (Standard 8.2 Resursi).

Izvedba, dokumentacija i izvještavanje

Prilikom primjene Tematskih zahtjeva, interni revizori su također dužni postupati u skladu sa Standardima i provoditi svoj rad u skladu s Domenom V: Obavljanje usluga interne revizije. Standardi u Domeni V opisuju planiranje angažmana (Načelo 13 Učinkovito planirajte angažmane), provođenje angažmana (Načelo 14 Provodite angažman) i komuniciranje rezultata angažmana (Načelo 15 Priopćite rezultate angažmana i pratite akcijske planove).

Tematski zahtjevi su osmišljeni kako bi podržali dosljedne, visokokvalitetne prakse interne revizije. Primjenjuju se zajedno s primjenjivim lokalnim zakonima, propisima, očekivanjima nadzornih tijela i drugim profesionalno priznatim okvirima, koji mogu nametnuti dodatne ili specifičnije zahtjeve. Moguće je da su interni revizori već razvili radne programe i postupke testiranja temeljene na tim propisima i okvirima. Interni revizori trebaju uskladiti njihove planirane aktivnosti testiranja kontrola organizacijske otpornosti i sva pouzdana testiranja provedena od strane drugih internih i eksternih pružatelja usluga s izražavanjem uvjerenja (Standard 9.5 Koordinacija i oslanjanje) s Tematskim zahtjevom radi osiguranja o odgovarajuće pokrivenosti.

Pokrivenost Tematskog zahtjeva može se dokumentirati ili u planu interne revizije ili u radnim dokumentima angažmana na temelju profesionalne prosudbe revizora. Jedan ili više angažmana interne revizije mogu pokrivati zahtjeve. Osim toga, možda neće biti primjenjivi svi zahtjevi. Dokazi da je Tematski zahtjev procijenjen na primjenjivost moraju se sačuvati, uključujući obrazloženje koje objašnjava sva isključenja.

Opcionalni alat iz Priloga D može se koristiti kao referenca kao i za dokumentiranje rada internih revizora

Osiguranje kvalitete

Standardi zahtijevaju od rukovoditelja interne revizije da razvije, implementira i održava program osiguranja i unaprjeđenja kvalitete koji obuhvaća sve aspekte funkcije interne revizije (Standard 8.3 Kvaliteta, Standard 8.4 Eksterna procjena kvalitete, Standard 12.1 Interna procjena kvalitete). Rezultati se moraju priopćiti odboru i višem menadžmentu.

Priopćenja moraju izvještavati o usklađenosti funkcije interne revizije sa Standardima i ostvarenju ciljeva izvođenja.

Usklađenost s Tematskim zahtjevima bit će uzeta u obzir u nadzornim aktivnostima na razini angažmana (Standard 12.3 Nadgledanje i unapređivanje provedbe angažmana) te ocijenjena u procjenama kvalitete. Radi pripreme za procjenu kvalitete, interni revizori mogu koristiti alat iz Priloga D.

Organizacijska otpornost

Organizacijska otpornost odnosi se na sposobnost organizacije da se uspješno nosi s promjenama i prilagodi im se, osobito kada nastupe poremećaji. Prema međunarodnom standardu ISO 22316 koji predstavlja sveobuhvatni okvir Međunarodne organizacije za standardizaciju (ISO), organizacijska otpornost je definirana kao „sposobnost organizacije da apsorbira promjene i prilagodi se promjenjivom okruženju".

Iako ova definicija postavlja jasan cilj, u praksi se organizacije znatno razlikuju u načinu na koji predviđaju, reagiraju na, 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.

U praksi, otporne organizacije su bolje pripremljene za suočavanje s neočekivanim izazovima te imaju veću sposobnost preživljavanja, razvoja i napretka kada se s njima suoče.

Brojni poremećaji mogu spriječiti organizaciju u ostvarivanju njezinih strateških ciljeva i zadataka, uključujući, ali ne ograničavajući se na:

- prirodne katastrofe, poput potresa, požara, poplava, uragana, tsunamija, tropskih oluja i drugih ekstremnih vremenskih događaja
- kibernetičke napade, kao što su ucjenjivački softver (ransomware), zlonamjerni softver (malware), napadi uskraćivanjem usluge (denial of service), povrede sigurnosti podataka, prijetnje iznutra (insider threats) i druge zlonamjerne aktivnosti usmjerene na nanošenje štete organizaciji ili ometanje njezina poslovanja
- geopolitičke sukobe, poput gospodarskih sankcija, carina, terorizma, ratova i drugih sukoba među državama
- pritiske iz okruženja, poput nestašica resursa, kriza javnog zdravstva, čimbenika održivosti ili klimatskih promjena
- promjene vanjskih čimbenika, poput razvoja tehnologije (uključujući umjetnu inteligenciju), promjena u zahtjevima usklađenosti (pravnim, regulatornim i zahtjevima financijskog izvještavanja), razine zaposlenosti, potražnje potrošača i ugleda organizacije
- financijske izazove, poput inflacije ili deflacije, kamatnih stopa, tečajeva valuta te prevladavajućih tržišnih uvjeta, poput recesije ili gospodarskog rasta
- operativne izazove, poput složenih procesa, velike ovisnosti o trećim stranama, geografske lokacije, kulturoloških izazova, ograničene dostupnosti radne snage te neučinkovitog rukovodstva ili upravljanja rizicima
- poremećaje u lancu opskrbe, poput nemogućnosti nabave sirovina, nedostatka alternativnih dobavljača i nestabilnih cijene roba i sirovina
- interne događaje, poput odlaska ključnih zaposlenika i pogrešaka u poslovanju.

Iako se priroda poremećaja može razlikovati, organizacija bi trebala imati jasno definiranu strategiju otpornosti i formalizirane procese za kontinuirano predviđanje, pripremu, reagiranje i prilagodbu promjenama. Organizacijska otpornost krovni je pojam, a strategija može uključivati različite sastavnice, ovisno o organizaciji, poput kontinuiteta poslovanja, oporavka od katastrofa, matrica kritičnih funkcija, planova nasljeđivanja ključnih funkcija i testiranja oporavka.

Zahtjevi Tematskog zahtjeva za organizacijsku otpornost uključuju:

- korporativno upravljanje što se odnosi na jasno definirane temeljne ciljeve i strategije organizacijske otpornosti koji podupiru ostvarenje misije i vizije organizacije
- upravljanje rizicima odnosi se na procese za identificiranje, analizu, upravljanje i praćenje prijetnji organizacijskoj otpornosti, uključujući proces za pravodobnu eskalaciju incidenata povezanih s organizacijskom otpornošću
- kontrolne procese koje je uspostavio menadžment i koji se periodično procjenjuju radi obuhvaćanja i upravljanja rizicima organizacijske otpornosti.

Razmatranja

Interni revizori mogu koristiti sljedeća razmatranja kao pomoć pri procjeni zahtjeva iz Tematskog zahtjeva za organizacijsku otpornost. Slovne oznake pojedinih razmatranja povezane su s odgovarajućim zahtjevima iz Tematskog zahtjeva. Ova razmatranja imaju ilustrativan karakter i ne predstavljaju obvezne zahtjeve. Interni revizori trebali bi se oslanjati na profesionalnu prosudbu pri određivanju što uključiti u svoje procjene.

Ograničenja u angažmanima interne revizije u javnom sektoru koja proizlaze iz zakonodavstva, ustroja državne uprave ili političkog okruženja, prepoznate su kao potencijalne prepreke za obuhvaćanje određenih aspekata ovog područja. Interni revizori u javnom sektoru trebaju dokumentirati takva ograničenja opsega u okviru procesa procjene rizika i primijeniti profesionalnu prosudbu kako bi jasno definirali i komunicirali prilagođeni opseg revizije.

Razmatranja o korporativnom upravljanju

Kako bi procijenili način na koji se procesi korporativnog upravljanja mogu primijeniti na ciljeve organizacijske otpornosti, interni revizori mogu pregledati dokaze o sljedećem:

A. Dokumentirana je strategija organizacijske otpornosti koju je uspostavio menadžment te ju je odobrio i nadzire odbor. Strategija je formalno priopćena svim zaposlenicima te je usko povezana s misijom, vizijom, kulturom i pristupom upravljanju rizicima organizacije te ih podupire. Ciljeve strateškog plana organizacijske otpornosti odobrava odbor, oni su usklađeni s cjelokupnim pristupom organizacije upravljanju rizicima te se periodično testiraju i pregledavaju. Plan može uključivati operativne, tehnološke i financijske elemente, kao što su:

   - operativni elementi – koordinacija aktivnosti organizacijske otpornosti na razini cijele organizacije; procesi procjene rizika organizacijske otpornosti; planiranje kontinuiteta poslovanja koje uključuje periodično testiranje i izvještavanje; upravljanje krizama; prilagodljivost radne snage (primjerice, kapacitet za naglo povećanje rada na daljinu, minimalan broj zaposlenika potrebnih na lokaciji i osiguranje zamjenjivosti za ključne funkcije provođenjem osposobljavanja zaposlenika za više različitih funkcija); planiranje nasljeđivanja ključnih funkcija; otpornost lanca opskrbe; uspostava ključnih pokazatelja uspješnosti (Key Performance Indicators – KPI) te edukacija članova odbora radi podizanja svijesti o organizacijskoj otpornosti
   - tehnološki elementi – zahtjevi za IT infrastrukturu; identifikacija ključnih podataka (klasifikacija podataka); sigurnosne kopije podataka; jačanje kibernetičke sigurnosti i praćenje prijetnji; održavanje ključne tehnološke imovine; te definirani ciljani trenutak oporavka i ciljano vrijeme oporavka za ključne podatke (potvrđeni su testiranjem postupka obnove podataka iz sigurnosnih kopija)

- financijski elementi – određena planirana financijska sredstva namijenjena organizacijskoj otpornosti; novčane pričuve za održavanje poslovanja tijekom poremećaja; procesi financijskog izvještavanja kojima se osigurava točno evidentiranje transakcija povezanih s poremećajima; police osiguranja za ublažavanje rizika povezanih s poremećajima; te dostupnost kreditnih linija za hitno financiranje.

B. Osoba ili tim odgovoran za organizacijsku otpornost periodično (primjerice mjesečno ili tromjesečno) izvještava odbor o stanju organizacijske otpornosti. Izvješća mogu uključivati definirane pragove tolerancije na rizik, ključne pokazatelje uspješnosti (KPI-je) ili druge informacije koje upućuju na opažanja ili trendove. Izvješća pružaju informacije o statusu ostvarivanja strateških ciljeva organizacijske otpornosti, uključujući strateški nadzor, praćenje i dugoročno planiranje. Izvještavanje može obuhvaćati rezultate praćenja:

- ostvarivanja strateških ciljeva organizacijske otpornosti te izazova koji mogu otežati njihovo ostvarenje
- iznosa potrebnih financijskih sredstava za potporu ciljevima i zadacima organizacijske otpornosti, kao što su potrebe za tehnološkom imovinom
- statusa rizika organizacijske otpornosti, uključujući sve značajne promjene u okruženju rizika organizacijske otpornosti koje bi mogle utjecati na utvrđene razine tolerancije na rizik
- učinkovitosti internih kontrola organizacijske otpornosti, uključujući napredak u provedbi korektivnih mjera
- ključnih pokazatelja uspješnosti za mjerenje uspješnosti organizacijske otpornosti
- potreba za ljudskim resursima radi zapošljavanja, osposobljavanja i razvoja zaposlenika s odgovornostima u području organizacijske otpornosti.

C. Politike, procedure i druga relevantna dokumentacija koriste se za upravljanje operativnim, tehnološkim i financijskim procesima organizacijske otpornosti, uključujući:

- način na koji se identificiraju ključni procesi organizacijske otpornosti te kako se oni periodično analiziraju kako bi se utvrdilo odražavaju li i dalje najvažnije procese organizacije
- periodično preispitivanje i ažuriranje politika najmanje jednom godišnje (ili češće, ovisno o višoj razini rizika), kao i češće ažuriranje kada to zahtijevaju novi rizici organizacijske otpornosti ili spoznaje proizašle iz testiranja odnosno stvarnih poremećaja
- proces preispitivanja primjerenosti i dostatnosti politika i procedura za podršku aktivnostima organizacijske otpornosti
- utvrđivanje doprinosi li primjena široko prihvaćenih okvira za povezana područja, poput upravljanja rizicima, informacijske tehnologija ili korporativnog upravljanja, jačanju procesa organizacijske otpornosti i internim kontrolama. Primjeri okvira, koje može biti korisno razmotriti, uključuju okvire organizacija kao što su NIST, COSO ili ISO, posebno norme iz serije ISO 22300 (npr. ISO 22316 ili ISO 22336).

D. Uspostavljena je i dokumentirana struktura upravljanja incidentima koja opisuje rukovodne uloge i odgovornosti povezane s ostvarivanjem ciljeva organizacijske otpornosti. Dokazi mogu uključivati postojanje jasno utvrđenih hijerarhija donošenja odluka, primjerice određivanje osoba odgovornih za donošenje odluka povezanih s organizacijskom otpornošću tijekom poremećaja, kao i potrebna odobrenja za operativne odluke, poput isplate sredstava ili sklapanja ugovora s trećim stranama radi pružanja pomoći organizaciji tijekom poremećaja. Dodatna razmatranja uključuju dokumentirane postupke eskalacije te privremene ovlasti za donošenje odluka tijekom poremećaja, uključujući financijske ovlasti za delegiranje odlučivanja i definirane pragove za ugovaranje usluga s trećim stranama.

E. Uspostavljen je proces za periodičnu (primjerice godišnju ili polugodišnju) procjenu znanja, vještina i sposobnosti osoba odgovornih za provedbu i upravljanje procesima organizacijske otpornosti. Proces može uključivati identificiranje programa osposobljavanja, kao što su edukacije uživo ili na daljinu, konferencije, online tečajeve na zahtjev ili profesionalne certifikacije. Dokazi mogu uključivati postojanje planova nasljeđivanja ključnih funkcija radi identificiranja ključnih uloga u području organizacijske otpornosti, uključujući testiranje scenarija kojim se utvrđuju aktivnosti koje može obavljati samo jedna osoba ili ograničen broj osoba. Također, definirani su zahtjevi u pogledu kvalifikacija za osobe koje bi preuzele te uloge kao zamjena.

F. Uspostavljen je proces za identificiranje, određivanje prioriteta i uključivanje relevantnih internih i eksternih dionika, prema potrebi, i uspostavljanje informacijskih i izvještajnih struktura radi prepoznavanja i odgovora na postojeće ranjivosti i nove prijetnje koje bi mogle utjecati na ostvarenje ciljeva organizacijske otpornosti. Dokazi mogu uključivati sudjelovanje dionika u raspravama o ranjivostima organizacijske otpornosti. Takvi dokazi mogu biti elektronička pošta, zapisnici sa sastanaka ili izvješća, uključujući pokazatelje primjene pokazatelja na razini cijele organizacije za mjerenje i praćenje učinkovitosti organizacijske otpornosti.

Razmatranja upravljanja rizicima

Kako bi procijenili način na koji se procesi upravljanja rizicima primjenjuju na ciljeve organizacijske otpornosti, interni revizori mogu pregledati dokaze o sljedećem:

A. Procesi procjene i upravljanja rizicima organizacije uključuju identificiranje rizika organizacijske otpornosti te se provode kontinuirano i dokumentiraju, a rezultati se komuniciraju unutar organizacije. Proces upravljanja rizicima organizacijske otpornosti uključuje procjenu ključnih područja i procesa, kao što su poslovne operacije, upravljanje rizicima na razini cijele organizacije, informacijska tehnologija, upravljanje lancem opskrbe i nabava, upravljanje poslovnim prostorima infrastrukturom, ljudski resursi, financije, pravni poslovi, usklađenost, regulatorni zahtjevi, odnosi s javnošću, ključni dobavljači, ugled organizacije, rizici u nastajanju i druga relevantna područja. Osim identificiranja rizika organizacijske otpornosti, procesi uključuju procjenu načina na koji se prijetnje i ranjivosti koje mogu poremetiti poslovanje:

- inicijalno identificiraju i prijavljuju
- analiziraju radi procjene rizika za ostvarenje ciljeva organizacije
- ublažavaju, uključujući provedbu akcijskih planova za smanjenje rizika na prihvatljivu razinu
- prate, uključujući plan kontinuiranog izvještavanja sve dok prijetnje ne budu u potpunosti uklonjene.

Dodatni dokazi mogu uključivati:

- dokumentaciju u obliku izvješća, elektroničke pošte ili zapisnika sa sastanaka koja pokazuje koja su poslovna područja sudjelovala u procesu procjene rizika te mogu biti uključeni čimbenici rizika kao što su učinak, vjerojatnost, brzina razvoja rizika i drugi relevantni aspekti.
- analizu visoko povezanih ili međusobno ovisnih čimbenika rizika radi utvrđivanja kumulativnog učinka višestrukih izloženosti riziku
- procjenu rizika koja uključuje vrednovanje slojeva zaštite ključne imovine i resursa radi sprječavanja nastanka jedinstvene točke otkaza (single point of failure)
- ažuriranje procjene rizika uključivanjem naučenih lekcija iz stvarnih kriza i poremećaja te rezultata testiranja i simuliranih scenarija
- određivanje prioriteta područja koja predstavljaju najveći rizik na temelju potencijalnog učinka i vjerojatnosti utvrđenih analizom utjecaja na poslovanje

B. Organizacija je dodijelila te periodično preispituje odgovornosti i zaduženja pojedinca ili tima zaduženog za praćenje i izvještavanje o rizicima organizacijske otpornosti. Pojedinac ili tim čine kvalificirane osobe s iskustvom u upravljanju organizacijskom otpornošću, idealno u djelatnosti u kojoj organizacija posluje (primjerice u zdravstvu, financijskim uslugama ili javnom sektoru). Pojedinac ili tim redovito sudjeluju u periodičnim programima osposobljavanja kako bi ostali upoznati s novim trendovima i prijetnjama u području rizika organizacijske otpornosti.

C. Organizacija je uspostavila proces za praćenje rizika organizacijske otpornosti (novonastalih ili prethodno identificiranih) te za njihovu brzu eskalaciju kada dosegnu razinu koja se smatra neprihvatljivom prema utvrđenim smjernicama za upravljanje rizicima i toleranciji na rizik organizacije ili prema primjenjivim zakonskim i regulatornim zahtjevima. Pri procjeni rizika organizacijske otpornosti uzimaju se u obzir njegovi učinci, uključujući financijske i nefinancijske pokazatelje utjecaja. Primjeri financijskih pokazatelja uključuju prihode, rashode, profitabilnost, novčani tok, zaduženost, cijenu dionice i ukupnu vrijednost organizacije. Primjeri nefinancijskih pokazatelja uključuju ugled brenda, zadovoljstvo korisnika, utjecaj na okoliš i fluktuaciju zaposlenika. Proces uključuje:

- početno identificiranje rizika i njegovu pravodobnu eskalaciju
- analizu rizika radi procjene njegove razine i utvrđivanja na koji način može spriječiti ostvarenje ciljeva organizacije

- predlaganje i usuglašavanje akcijskih planova za ublažavanje rizika, uključujući mjere za pravodobno smanjenje rizika na prihvatljivu razinu. Akcijski planovi temelje se na cjelokupnoj strategiji upravljanja rizicima na razini organizacije. Prijedlog treba uključivati resurse potrebne za ublažavanje rizika, kao što su financijska sredstva, radni sati zaposlenika te dodatna tehnologija i softver potrebni za povećanje sposobnosti organizacije za upravljanje rizikom.
- kontinuirano praćenje rizika i izvještavanje o ključnim pokazateljima rizika (Key Risk Indicators – KRIs) sve dok prijetnje ne budu u potpunosti uklonjene.

D. Organizacija je uspostavila proces odgovora na krize, poremećaje, izvanredne situacije i druge incidente te proces za oporavak nakon njihove pojave. Proces se periodično u cijelosti testira, primjerice tromjesečno ili godišnje, a može uključivati i češća djelomična testiranja, primjerice na mjesečnoj razini. Kritične usluge mogu zahtijevati učestalije testiranje. Proces odgovora na incidente i oporavka može uključivati:

- otkrivanje – kontinuirano praćenje kibernetičkih događaja. To može uključivati korištenje sustava za otkrivanje upada, sustava za praćenje i analizu prijetnji ili sustava za upravljanje sigurnosnim informacijama i događajima (Security Information and Event Management – SIEM). SIEM može koristiti umjetnu inteligenciju radi jačanja učinkovitosti procesa. U slučaju prirodnih katastrofa ili prekida u radu objekata i infrastrukture, organizacija ima uspostavljenu komunikacijsku mrežu (primjerice protokole za uzbunjivanje ili sustave obavješćivanja) radi pravodobnog obavještavanja i razmjene informacija. Za sve vrste događaja organizacija ima definiran proces za obavještavanje nadležnih hitnih službi i drugih mjerodavnih tijela. Događajima se dodjeljuje prioritet prema njihovoj kritičnosti.
- odgovor i ograničavanje učinaka incidenata – pristup odgovora na incidente uključuje analize scenarija i periodično stresno testiranje otpornosti na različite vrste poremećaja. Primjerice, kako bi se spriječila daljnja šteta tijekom kibernetičkih incidenata, organizacija je uspostavila proces izolacije kompromitirane imovine, kao što su preusmjeravanje mrežnog prometa ili ograničavanje korisničkih pristupa tijekom incidenta. Kod fizičkih događaja, organizacija je uspostavila proces fizičkog ograničavanja poremećaja radi smanjenja njihova utjecaja, uključujući premještanje zaposlenika na alternativnu lokaciju.
- oporavak – organizacija je za kibernetičke ili IT incidente uspostavila postupke kojima se prioritet daje oporavku ključne imovine potrebne za nastavak poslovanja (primjerice obnovi podataka iz sigurnosnih kopija ili ponovnom stavljanju poslužitelja u funkciju). I drugim resursima koji nisu povezani s IT-om, a nužni su za nastavak poslovanja, potrebno je dodijeliti prioritet u oporavku. To može uključivati planiranje postupnog povratka ključnog osoblja ili ponovne uspostave ključnih poslovnih funkcija.
- analizu nakon incidenta - organizacija analizira događaje kako bi utvrdila:
  - temeljne uzroke poremećaja i incidenata
  - učinkovitost poduzetih mjera
  - potrebna poboljšanja za jačanje procesa organizacijske otpornosti, poput ažuriranja politika, procedura, procjena rizika, strategija i drugih relevantnih

elemenata.

Testiranje procesa odgovora i oporavka, radi procjene njihove temeljitosti i učinkovitosti, provođenjem vježbi temeljenih na simulaciji kriznih scenarija, simulacija i praktičnih vježbi koje obuhvaćaju ključne usluge odnosno funkcije i njihove međuovisnosti, može biti usklađeno s razinama tolerancije organizacije na rizik. Ti događaji mogu proizlaziti iz internih ili eksternih incidenata. Rezultate tih vježbi mogu pregledavati odbor i viši menadžment, a provedba utvrđenih mjera za poboljšanje kontinuirano se prati te se o njihovu statusu periodično izvještava. Preporuke trebaju biti provedive, uz jasno definirane nositelje odgovornosti i rokove za provedbu.

Razmatranja kontrolnih procesa

Kako bi procijenili način na koji se kontrolni procesi primjenjuju na ciljeve organizacijske otpornosti, interni revizori mogu pregledati dokaze o sljedećem:

A. Uspostavljen je proces za identificiranje i procjenu ključnih pružatelja usluga trećih strana (dobavljača i isporučitelja) te minimalnih razina zaliha potrebnih za održavanje ključnih poslovnih aktivnosti. Procjena može uključivati razmatranje organizacijske otpornosti i kontinuiteta poslovanja trećih strana te dodjeljivanje ocjenu rizika svakom dobavljaču. Osim procjene dobavljača prije sklapanja formalnog ugovornog odnosa, organizacija može periodično procjenjivati postojeće dobavljače kako bi kontinuirano procjenjivala njihove razine rizika. Organizacija održava popis potencijalnih alternativnih dobavljača za slučaj prestanka suradnje s postojećim dobavljačima.

B. Menadžment je proveo klasifikaciju podataka, pri čemu je posebno identificirao ključne podatke potrebne za oporavak nakon poremećaja i nastavak poslovanja. Organizacija je uspostavila učinkovite interne kontrole za zaštitu ključnih podataka, uključujući ograničavanje pristupa ovlaštenom osoblju te osiguravanje da su ključni podaci sigurnosno kopirani i da se mogu pravodobno obnoviti.

C. Menadžment je uspostavio ključne IT kontrole i procese kontinuiranog praćenja radi ublažavanja rizika informacijske sigurnosti (uključujući kibernetičke rizike) te zaštite osjetljivih podataka tijekom poremećaja. Osjetljivi podaci zaštićeni su enkripcijom. Kontinuirano praćenje i korištenje sustava za praćenje i analizu prijetnji u stvarnom vremenu (real-time threat intelligence) omogućuju pravodobno upozoravanje, a identificirani problemi rješavaju se bez odgađanja. U tu svrhu mogu se koristiti široko prihvaćeni kontrolni okviri organizacija kao što su NIST, COSO, ISO i drugi.

D. Organizacija je evidentirala i vodi inventar ključne IT imovine, uključujući hardver, softver i usluge potrebne za podršku poslovanju tijekom kriza, poremećaja i izvanrednih situacija. IT imovina koju je teško brzo nabaviti ili zamijeniti, identificirana je kao imovina visokog prioriteta.

E. Uspostavljeni su plan kontinuiteta poslovanja i plan oporavka od katastrofa i određeni su članovi timova za oporavak na temelju analize utjecaja na poslovanje. Planovi se periodično testiraju, primjerice tromjesečno ili godišnje, provođenjem vježbi temeljenih na simulaciji kriznih scenarija ili stresnih testiranja, pri čemu se simuliraju poremećaji koji oponašaju stvarne izvanredne situacije te se testiraju komunikacijski protokoli s internim i eksternim dionicima. Rezultati testiranja, uključujući utvrđene mogućnosti za poboljšanje, dostavljaju se odboru i višem menadžmentu.

F. Uspostavljen je proces za prilagodbu radnog okruženja tijekom poremećaja. Prilagodbe mogu uključivati korištenje alternativnih lokacija za rad, primjerice rad od kuće ili pravodobno i učinkovito uspostavljanje privremenog ureda na drugoj lokaciji. Organizacija može koristiti hibridne ili udaljene oblike rada kao zamjenu za rad na lokaciji. Drugi aspekti mogu uključivati protokole za pravodobnu i učinkovitu mobilizaciju te preraspodjelu resursa, uključujući IT resurse i ljudske potencijale.

G. Uspostavljen je proces za kontinuirano praćenje i izvještavanje o novim prijetnjama i ranjivostima povezanima s organizacijskom otpornošću te za prepoznavanje, određivanje prioriteta i provedbu mjera za unapređenje procesa organizacijske otpornosti. Aktivnosti praćenja mogu uključivati ključne pokazatelje rizika, nadzorne ploče za praćenje rizika i aktivnosti sustavnog praćenja budućih rizika. Organizacija može svim zaposlenicima pružati informacije o novim prijetnjama radi podizanja svijesti, uključujući informacije o mjerama za ublažavanje rizika i uspostavljenim kontrolama. Sve prijave nepravilnosti se evidentiraju, analiziraju i pravodobno rješavaju, a o njima se izvještava viši menadžment. Za rješavanje pojedinih pitanja može biti potrebno kontinuirano praćenje, što može zahtijevati dodatno izvještavanje.

H. Uspostavljen je proces za edukaciju i osposobljavanje zaposlenika o politikama i procedurama organizacijske otpornosti koje treba primjenjivati u slučaju kriza, poremećaja i izvanrednih situacija. Proces uključuje vježbe osposobljavanja u kojima se simuliraju različiti scenariji poremećaja. Edukacije se provode periodično, primjerice tromjesečno ili godišnje. Ključne usluge mogu zahtijevati češće testiranje.

I. Uspostavljen je proces kojim se osigurava da su potrebni operativni, ljudski, tehnološki i financijski resursi planirani i dostupni tijekom kriza, poremećaja i izvanrednih situacija. Menadžment periodično, primjerice tromjesečno ili godišnje, preispituje raspoložive resurse kako bi utvrdilo jesu li primjereni procijenjenim razinama rizika te o potrebama izvještava odbor. Ključne usluge mogu zahtijevati češće testiranje. Analiza uključuje procjenu: likvidnosti, adekvatnosti pokrića osiguranjem, rezervnih odnosno alternativnih izvora financiranja. Potrebe za financijskim resursima planiraju se na temelju čimbenika kao što su veličina organizacije, složenost poslovanja, djelatnost i profil rizika. Proces može uključivati i prethodno odobravanje financijskih sredstava.

J. Uspostavljen je proces za pregled i procjenu kriza, poremećaja i izvanrednih situacija nakon njihova nastanka te za analizu događaja kroz postupak utvrđivanja naučenih lekcija. Pregledi i analize trebaju biti dokumentirani u formalnim izvješćima, a stečene spoznaje trebaju biti uključene u buduće aktivnosti planiranja organizacijske otpornosti.

Prilog A. Scenariji za primjenu Tematskog zahtjeva

Sljedeći scenariji opisuju situacije u kojima se primjenjuje Tematski zahtjev za organizacijsku otpornost. Osim toga, donesene „Smjernice za primjenu tematskih zahtjeva" od strane IIA pružaju praktične upute za primjenu obveznih zahtjeva, postupanje u slučaju ograničenja te utvrđivanje kritičnih pragova rizika.

Scenarij 1: Organizacijska otpornost identificirana je kao predmet revizijskog angažmana uključenog u plan interne revizije

Kada funkcija interne revizije dovrši postupak planiranja temeljen na rizicima i u plan interne revizije uključi jedan ili više angažmana povezanih s organizacijskom otpornošću, Tematski zahtjev mora se primijeniti prilikom provedbe takvih angažmana. Usklađenost s Tematskim zahtjevom može se postići uključivanjem njegovih zahtjeva u jedan ili više angažmana predviđenih planom interne revizije.

Organizacijska otpornost široko je područje te se svi zahtjevi iz Tematskog zahtjeva ne moraju nužno primjenjivati u svakom pojedinom angažmanu. Kada interni revizori primjenom profesionalne prosudbe utvrde da jedan ili više zahtjeva Tematskog zahtjeva za organizacijsku otpornost nisu primjenjivi te ih stoga treba isključiti iz angažmana, dužni su dokumentirati i čuvati obrazloženje za njihovo isključivanje. Primjerice, obrazloženje za isključivanje pojedinih zahtjeva može biti činjenica da funkcija interne revizije provodi različite angažmane povezane s organizacijskom otpornošću primjenom rotacijskog pristupa ili u slučaju da je procijenjeno kako je značaj predmetnog rizika u okviru angažmana nizak.

Scenarij 2: Rizici organizacijske otpornosti identificirani su tijekom revizijskog angažmana koji nije usmjeren na organizacijsku otpornost

Interni revizori mogu identificirati rizike organizacijske otpornosti tijekom procjene procesa koji nisu izravno povezani s organizacijskom otpornošću. Primjerice, interni revizori mogu provoditi procjenu procesa upravljanja ljudskim resursima (kao što su zapošljavanje i zadržavanje zaposlenika) u okviru angažmana koji nije usmjeren na organizacijsku otpornost te tijekom planiranja angažmana nisu utvrdili rizike organizacijske otpornosti. Međutim, nakon provedbe početnog upoznavanja s procesom, interni revizori mogu zaključiti da su takvi rizici ipak obuhvaćeni angažmanom. Primjerice, mogu identificirati rizike povezane s planiranjem nasljeđivanja ključnih funkcija koji proizlaze iz načina na koji organizacija zadržava zaposlenike (Standard 13.2 – Procjena rizika angažmana).

Nakon što su relevantni rizici identificirani, interni revizori moraju pregledati Tematski zahtjev za organizacijsku otpornost i utvrditi koji su zahtjevi primjenjivi. U ovom primjeru mogli bi se

usredotočiti samo na zahtjev E u području Korporativnog upravljanja te izuzeti ostale zahtjeve koji se odnose na upravljanje rizicima i kontrole. Interni revizori moraju u radnoj dokumentaciji angažmana dokumentirati obrazloženje za isključivanje ostalih zahtjeva Tematskog zahtjeva za organizacijsku otpornost te čuvati tu dokumentaciju.

Scenarij 3: Zatraženo je provođenje angažmana vezanog uz organizacijsku otpornost koji izvorno nije bio uključen u plan interne revizije

Dionici poput odbora, menadžmenta ili regulatornog tijela mogu zatražiti od internih revizora provedbu procjene organizacijske otpornosti koja nije bila predviđena izvornim planom interne revizije. Primjerice, ako je organizacija bila meta kibernetičkog napada, odbor može zatražiti provođenje revizijskog angažmana radi procjene kontrolnih procesa organizacijske otpornosti kako bi se ocijenilo koliko je organizacija spremna za oporavak nakon kibernetičkog napada. U takvom slučaju Tematski zahtjev je primjenjiv, njegovi zahtjevi moraju biti procijenjeni, a sva isključenja moraju biti dokumentirana (Standard 9.4 – Plan interne revizije)

Prilog B. Primjeri revizijskih angažmana temeljeno na scenarijima za primjenu

Scenarij 1: Tema je predmet angažmana uključenog u plan interne revizije

Subjekt u javnom sektoru odgovoran za središnju veletržnicu

Tijekom godišnjeg procesa planiranja temeljenog na rizicima, funkcija interne revizije identificira kontinuitet ključnih tržišnih aktivnosti kao područje visokog rizika zbog izloženosti logističkim poremećajima, poremećaja u javnom zdravstvu i ovisnosti o kritičnoj infrastrukturi. Na temelju te procjene interni revizori utvrđuju da je Tematski zahtjev za organizacijsku otpornost primjenjiv na planirani angažman.

Radi procjene korporativnog upravljanja, interni revizori pregledavaju zapisnike sjednica odbora, strateške planove i dokumentaciju koja se odnosi na proračun kako bi utvrdili jesu li ciljevi povezani s organizacijskom otpornošću formalno uspostavljeni i pod odgovarajućim nadzorom. Također procjenjuju dostavlja li menadžment periodična izvješća upravljačkom tijelu o ključnim ranjivostima, kao što su ovisnost o prijevozu, infrastrukturna ograničenja i rizici povezani sa zaštitom zdravlja. Ako ne postoji jedinstveni dokument koji uređuje strategiju organizacijske otpornosti, interni revizori procjenjuju jesu li elementi organizacijske otpornosti dosljedno integrirani u operativnu i stratešku dokumentaciju.

S aspekta upravljanja rizicima, interni revizori pregledavaju registar rizika organizacije i provode intervjue s operativnim menadžmentom kako bi potvrdili da su rizici koji mogu utjecati na kontinuitet opskrbe identificirani, procijenjeni i dodijeljeni odgovornim vlasnicima rizika. Također ispituju jesu li tijekom prethodnih događaja, poput privremenih zatvaranja ili ograničenja pristupa, aktivirani mehanizmi eskalacije te jesu li poduzete mjere odgovora bile usklađene s definiranim parametrima tolerancije na rizik.

Kontrolni postupci uključuju pregled uspostavljenih mjera za osiguravanje operativnog kontinuiteta, provjeru dokaza o periodičnim testiranjima te pregled dokumentacije o koordinaciji s tijelima javne vlasti tijekom poremećaja. Interni revizori također pregledavaju izvješća sastavljena nakon incidenata kako bi utvrdili jesu li naučene lekcije uključene u ažurirane procese. Ako pojedini zahtjevi Tematskog zahtjeva nisu primjenjivi zbog zakonskih ili organizacijskih ograničenja, interni revizori dokumentiraju obrazloženje za njihovo isključivanje u skladu sa Standardima.

Scenarij 2: Tema je identificirana tijekom provedbe angažmana

Globalno prisutna korporacija za pružanje profesionalnih usluga

Tijekom angažmana usmjerenog na korporativno upravljanje i upravljanje rizicima na razini cijele organizacije, interni revizori identificiraju ranjivosti povezane s decentraliziranim donošenjem

odluka, ovisnošću o ključnom lokalnom vodstvu te regulatornom izloženošću u različitim jurisdikcijama. Na temelju tih zapažanja, interni revizori utvrđuju da su određeni elementi Tematskog zahtjeva za organizacijsku otpornost primjenjivi na predmetni angažman.

Radi procjene korporativnog upravljanja, interni revizori pregledavaju globalne politike, materijale za izvještavanje odbora i protokole za upravljanje krizama kako bi utvrdili je li organizacija definirala način održavanja poslovanja tijekom regulatornih promjena, značajnog odlaska ključnih zaposlenika ili događaja koji narušavaju ugled u jednoj jurisdikciji, a koji mogu imati šire posljedice za organizaciju.

Također procjenjuju prima li upravljačko tijelo konsolidirana izvješća o ključnim rizicima iz različitih jurisdikcija te jesu li odgovornosti za nadzor organizacijske otpornosti jasno definirane.

S aspekta upravljanja rizicima, interni revizori pregledavaju okvir upravljanja rizicima na razini cijele organizacije kako bi potvrdili jesu li rizici povezani s ovisnošću o ključnim pojedincima, usklađenošću s prekograničnom regulativom i izloženošću reputacijskim rizicima povezani sa strateškim ciljevima društva. Provode testiranje na uzorku odabranih incidenata kako bi utvrdili jesu li lokalni događaji pravodobno eskalirani rukovodstvu odgovornom na globalnoj razini te jesu li odluke o odgovoru na rizike donesene u okviru definiranih razina ovlasti.

Revizijski postupci povezani s kontrolama uključuju pregled mjera za osiguravanje kontinuiteta poslovanja u različitim jurisdikcijama, procjenu jesu li ključne funkcije odgovarajuće pokrivene te postoje li zamjenske osobe ili odgovarajuće strukturirani procesi planiranja nasljeđivanja ključnih funkcija za postupanje u izvanrednim okolnostima. Također procjenjuju primjerenost tehnološke infrastrukture koja podržava koordinirani rad na daljinu.

Interni revizori pregledavaju i dokumentaciju o analizama provedenima nakon događaja kako bi potvrdili da su korektivne mjere provedene. Ako su primjenjivi samo pojedini zahtjevi Tematskog zahtjeva, interni revizori dokumentiraju osnovu za njihovo uključivanje odnosno isključivanje.

Scenarij 3: Tema je predmet zahtijevanog revizijskog angažmana

Organizacija odgovorna za kritičnu nacionalnu infrastrukturu

Razorni uragan u susjednoj jurisdikciji je potaknuo člana odbora da zatraži od funkcije interne revizije uključivanje angažmana iz područja organizacijske otpornosti u plan revizije kako bi se procijenila izloženost organizacije prekidima u poslovanju, ovisnosti o specijaliziranim ugovornim partnerima, regulatornim obvezama i ekstremnim događajima u prirodnom okolišu. U ovom slučaju Tematski zahtjev za organizacijsku otpornost primjenjuje se u cijelosti.

Radi procjene korporativnog upravljanja, interni revizori pregledavaju strateški plan koji je odobrio odbor i povezanu dokumentaciju kako bi potvrdili da je kontinuitet ključnih usluga formalno uključen u dugoročno planiranje. Pregledavaju i izvješća dostavljena odboru kako bi utvrdili provodi li se periodično praćenje ključnih pokazatelja povezanih s neprekidnim obavljanjem poslovnih aktivnosti, održavanjem ključne imovine i planiranjem financijskih mjera za izvanredne okolnosti, uključujući adekvatnost pokrića osiguranjem i alokacije rezerviranih sredstava za takve slučajeve.

S aspekta upravljanja rizicima, interni revizori procjenjuju na koji se način rizici povezani s poremećajima u infrastrukturi, koncentracijom ugovornih pružatelja usluga, regulatornom usklađenošću i izloženošću okolišnim rizicima identificiraju, procjenjuju i prate u okviru sustava

upravljanja rizicima na razini cijele organizacije. Također pregledavaju jesu li odgovornosti za praćenje tih rizika jasno definirane te jesu li tijekom prethodnih prekida pružanja usluga poštovani protokoli eskalacije, uključujući koordinaciju s regulatornim tijelima i službama za izvanredne situacije.

Testiranje kontrolnih procesa uključuje provjeru postojanja planova kontinuiteta poslovanja i planova oporavka od katastrofa te njihova periodičnog testiranja, pregled inventara ključne imovine, pregled ugovornih aranžmana s alternativnim pružateljima usluga te analizu dokumentacije o postupcima nakon incidenta kako bi se utvrdilo jesu li korektivne mjere praćene i provedene. Ako pojedini zahtjevi nisu primjenjivi zbog regulatornih odredbi, interni revizori dokumentiraju obrazloženje za njihovo isključenje u skladu sa Standardima.

Prilog C. Povezanost s drugim okvirima

Organizacija može uspostaviti i provoditi vlastite aktivnosti i inicijative u području organizacijske otpornosti, pri čemu može primjenjivati okvire poput onih koje je razvila Međunarodna organizacije za standardizaciju (ISO). Interni revizori su možda već razvili revizijske programe i postupke testiranja temeljene na tim okvirima. Interni revizori trebaju uskladiti planirano testiranje kontrolnih procesa organizacijske otpornosti s Tematskim zahtjevom kako bi osigurali odgovarajuću pokrivenost angažmana (Standard 13.4 – Kriteriji ocjenjivanja). Tablica u nastavku prikazuje mapiranje (povezivanje) Tematskog zahtjeva za organizacijsku otpornost na okvir ISO 22336. Reference na druge relevantne okvire navedene su u Prilogu E.

Zahtjevi za korporativno upravljanje	Okvir ISO 22336
A. Menadžment je uspostavio formalnu strategiju za organizacijsku otpornost, koju 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.	4.1; 6.1; 6.2; 7.1; 8.4; 8.5; 9.1; 9.5
B. Informacije o ostvarivanju ciljeva organizacijske otpornosti periodično se dostavljaju odboru na razmatranje. Time se osigurava da je organizacijska otpornost integrirana u strateški nadzor, procese dugoročnog planiranja, planiranje nasljeđivanja ključnih funkcija te organizacijsku kulturu, uključujući razmatranja planiranja resursa i financijskih planova potrebnih za podršku ključnim poslovnim aktivnostima.	6.4; 8.6; 10.2
C. Uspostavljene su politike i procedure za ključne operativne, tehnološke i financijske procese te se periodično preispituju, testiraju i prema potrebi ažuriraju radi jačanja kontrolnog okruženja.	4.2; 6.3; 8.3; 8.4; 9.4
D. Uspostavljena je struktura upravljanja incidentima koja omogućuje nadzor nad ostvarivanjem ciljeva organizacijske otpornosti i pruža podršku njihovu ostvarenju. Struktura uključuje hijerarhiju donošenja odluka, protokole komunikacije i eskalacije te jasno definirane rukovodne i operativne uloge i odgovornosti.	5.4
E. Uspostavljen je proces za periodičnu provjeru kompetencija potrebnih za uspješno ostvarivanje organizacijske otpornosti te za ponovnu procjenu kompetencija osoba koje obnašaju ključne uloge u procesima organizacijske otpornosti.	9.6
F. Uspostavljen je proces kojim se osigurava da su svi relevantni interni i eksterni dionici identificirani, rangirani prema prioritetima i uključeni u uspostavljanje informacijskih i izvještajnih struktura radi ostvarivanja ciljeva organizacijske otpornosti. Dionici mogu uključivati viši menadžment, operativne funkcije, upravljanje rizicima, informacijsku tehnologiju (IT), upravljanje lancem opskrbe i nabavu, upravljanje poslovnim prostorima i infrastrukturom, ljudske resurse, financije, pravne poslove, pružatelje usluga s izražavanjem uvjerenja (uključujući internu reviziju), funkciju usklađenosti, odnose s javnošću, ključne	9.2; 9.5

dobavljače, klijente, regulatore i druge relevantne strane.	

Zahtjevi za upravljanje rizicima	Okvir ISO 22336
A. Rizici povezani s organizacijskom otpornošću periodično se identificiraju, procjenjuju i njima se upravlja na razini cijele organizacije. Ti su rizici povezani su sa strateškim ciljevima organizacije. Proces upravljanja rizicima organizacijske otpornosti uključuje procjenu ključnih procesa.	4.4; 5; 7.3; 7.4; 7.5, 7.6, 9.2, 9.3
B. Odgovornosti i 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.	4.3; 8.2; 9.6
C. Uspostavljen je proces za praćenje razina rizika organizacijske otpornosti (novih ili prethodno identificiranih rizika) te za njihovu brzu eskalaciju kada dosegnu razinu koja se smatra neprihvatljivom u skladu s utvrđenim smjernicama organizacije za upravljanje rizicima, tolerancijom na rizik ili primjenjivim zakonskim i regulatornim zahtjevima. Razmatraju se posljedice rizika povezanih s organizacijskom otpornošću.	7.2; 7.6; 10.1
D. Menadžment je uspostavio i periodično testira proces odgovora na krize, poremećaje i izvanredne situacije te proces oporavka nakon njihova nastanka. Proces odgovora na incidente i oporavka uključuje otkrivanje, određivanje prioriteta, stavljanje pod kontrolu, oporavak i analizu nakon incidenta. Pristup odgovoru na incidente uključuje analize scenarija i periodično stresno testiranje otpornosti na različite moguće poremećaje.	7.2; 7.6; 7.8

Zahtjevi za kontrolne procese	Okvir ISO 22336
A. Uspostavljen je proces za identificiranje ključnih pružatelja usluga trećih strana (dobavljača i isporučitelja) te za utvrđivanje minimalnih razina zaliha potrebnih za održavanje ključnih poslovnih aktivnosti. Proces također uključuje vođenje ažurnog popisa alternativnih dobavljača.	7.7
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.	6.1
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. Kontrolni procesi i kontinuirani nadzor uključuju korištenje sustava za praćenje i analizu prijetnji u stvarnom vremenu (real-time threat intelligence) te ograničavanje pristupa isključivo ovlaštenim korisnicima.	7.5

D. Ključna IT imovina evidentirana je u inventaru. Imovina uključuje hardver, softver i usluge potrebne za podršku poslovanju tijekom kriza, poremećaja i izvanrednih situacija.	9.2
E. Uspostavljeni su planovi kontinuiteta poslovanja i planovi oporavka od katastrofa, u kojima su jasno definirane uloge odgovornih osoba i timova za oporavak. Planovi se periodično testiraju (primjerice provođenjem vježbi temeljenih na simulaciji kriznog scenarija), a o rezultatima testiranja, uključujući mogućnosti za poboljšanje, izvještavaju se odbor i viši menadžment.	8.6; 9.6; 10.3
F. Uspostavljen je proces za prilagodbu radnog okruženja tijekom kriza, poremećaja i izvanrednih situacija.	9.3
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 procesa organizacijske otpornosti, uključujući sustave za prijavu nepravilnosti i prikupljanje i analizu informacija o rizicima (risk intelligence).	7.6
H. Uspostavljen je proces za edukaciju i osposobljavanje 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 osposobljavanja u kojima se simuliraju različiti scenariji poremećaja.	10.2; 10.3
I. Uspostavljen je proces kojim se osigurava da su potrebni operativni, ljudski, tehnološki i financijski resursi planirani i dostupni tijekom kriza, poremećaja i izvanrednih situacija. Financijski resursi potrebni za podršku organizacijskoj otpornosti periodično se analiziraju i o njima se izvještava odbor.	6.4; 7.6; 9.6
J. Uspostavljen je proces za pregled i analizu kriza, poremećaja i izvanrednih situacija nakon njihova nastanka te za analizu pregleda nakon incidenta kroz postupak utvrđivanja naučenih lekcija, uključujući njihovo uključivanje u buduće planiranje organizacijske otpornosti.	10.2, 10.3

Prilog D. Opcionalni alat za dokumentiranje

Od internih revizora očekuje se da primjenjuju profesionalnu prosudbu pri utvrđivanju primjenjivosti pojedinih zahtjeva na temelju procjene rizika te da na odgovarajući način dokumentiraju isključenje pojedinih zahtjeva. Primjena Tematskog zahtjeva može se dokumentirati u planu interne revizije ili u radnoj dokumentaciji angažmana, ovisno o profesionalnoj prosudbi internog revizora. Jedan ili više revizijskih angažmana mogu obuhvatiti zahtjeve Tematskog zahtjeva. Također, nisu nužno svi zahtjevi primjenjivi u svakom slučaju. Ovaj obrazac za ispis predstavlja jednu od mogućnosti dokumentiranja usklađenosti s Tematskim zahtjevom za organizacijsku otpornost, no njegova uporaba nije obvezna.

Organizacijska otpornost – korporativno upravljanje

Zahtjev	Pokrivenost (ispunjenje) zahtjeva ili obrazloženje isključenja	Referenca dokumentacije
A. Menadžment je uspostavio formalnu strategiju za organizacijsku otpornost, koju 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. Izvješća o ostvarivanju ciljeva organizacijske otpornosti periodično se dostavljaju odboru na razmatranje. Time se osigurava da je organizacijska otpornost integrirana u strateški nadzor, procese dugoročnog planiranja, planiranje nasljeđivanja ključnih funkcija te organizacijsku kulturu, uključujući odluke o resursima i financijskim sredstvima potrebnim za podršku ključnim poslovnim aktivnostima.		
C. Uspostavljene su politike i procedure za ključne 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 rukovodne i operativne uloge i odgovornosti.		
E. Uspostavljen je proces za periodičnu provjeru kompetencija potrebnih za uspješno ostvarivanje organizacijske otpornosti te za ponovnu procjenu kompetencija osoba koje obnašaju ključne uloge u procesima organizacijske otpornost		
F. Uspostavljen je proces kojim se osigurava da su svi relevantni interni i eksterni dionici identificirani, rangirani prema prioritetima i uključeni u uspostavu informacijskih i izvještajnih struktura radi ostvarivanja ciljeva organizacijske otpornosti. Dionici mogu uključivati viši menadžment, operativne funkcije, upravljanje rizicima, informacijsku tehnologiju (IT), upravljanje lancem opskrbe i nabavu, upravljanje poslovnim prostorima i infrastrukturom, ljudske resurse, financije, pravne poslove, pružatelje usluga s izražavanjem uvjerenja (uključujući internu reviziju), funkciju usklađenosti, odnose s javnošću, ključne dobavljače, korisnike odnosno klijente, regulatore i druge relevantne strane.		

Organizacijska otpornost – upravljanje rizicima

Zahtjev	Pokrivenost (ispunjenje) zahtjeva ili obrazloženje isključenja	Referenca dokumentacije
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 procesa.		

B. Odgovornosti i 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 razina rizika organizacijske otpornosti (novih ili prethodno identificiranih rizika) te za njihovu brzu eskalaciju kada dosegnu razinu koja se smatra neprihvatljivom u skladu s utvrđenim smjernicama organizacije za upravljanje rizicima, tolerancijom na rizik ili primjenjivim zakonskim i regulatornim zahtjevima. Razmatraju se učinci rizika povezanih s organizacijskom 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, stavljanje pod kontrolu, oporavak i analizu nakon incidenta. Pristup odgovora na incidente uključuje analize scenarija i periodično stresno testiranje otpornosti na različite moguće poremećaje.		

Organizacijska otpornost – kontrolni procesi

Zahtjev	Pokrivenost (ispunjenje) zahtjeva ili obrazloženje isključenja	Referenca dokumentacije
A. Uspostavljen je proces za identificiranje ključnih pružatelja usluga trećih strana (dobavljača i isporučitelja) te za utvrđivanje 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. Kontrolni procesi i kontinuirani nadzor uključuju korištenje sustava za pregled i analizu podataka o prijetnjama u stvarnom vremenu (real-time threat intelligence) te ograničavanje pristupa isključivo ovlaštenim korisnicima.		
D. Vodi se inventar ključne IT imovine. Ta imovina uključuje hardver, softver i usluge potrebne za održavanje poslovanja 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 utvrđene mogućnosti za poboljšanje, informira 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 procesa organizacijske otpornosti, uključujući sustave za prijavu nepravilnosti i prikupljanje i analizu informacija o rizicima (risk intelligence).		
H. Uspostavljen je proces za edukaciju i osposobljavanje 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 temeljene na simuliranim scenarijima u		

	kojima se simuliraju različiti poremećaji.		
I.	Uspostavljen je proces kojim se osigurava da su potrebni operativni, ljudski, tehnološki i financijski resursi planirani i dostupni tijekom kriza, poremećaja i izvanrednih situacija. Financijski resursi potrebni za podršku organizacijskoj otpornosti periodično se analiziraju, a o rezultatima provedenih analiza izvještava se odbor.		
J.	Uspostavljen je proces za procjenu i analizu kriza, poremećaja i izvanrednih situacija nakon njihova nastanka te za analizu rezultata pregleda provedenih nakon incidenta primjenom postupka utvrđivanja naučenih lekcija, uključujući uključivanje stečenih spoznaja u buduće planiranje organizacijske otpornosti.		

Prilog E. Reference na druge relevantne okvire

Područje	ISO Referenca	Opseg/Naslovi odredbi
Korporativno upravljanje	ISO 22316:2017	Politika i strategija, predanost rukovodstva, zajednička vizija, kultura, komunikacija, kontinuirano unapređenje
Upravljanje rizicima	ISO 31000:2018	Opseg/kontekst/kriteriji, procjena rizika, postupanje s rizicima, praćenje, komunikacija
Temelji za kontinuitet poslovanja i oporavak od katastrofa	ISO 22301: 2019; ISO/TS 22317:2021	Kontekst, vodstvo, planiranje i operativno djelovanje sustava za upravljanje kontinuitetom poslovanja; aktivnosti i rezultati analize utjecaja na poslovanje
Otpornost lanca opskrbe	ISO/TS 22318:2021	Analiza ovisnosti o dobavljačima, strategije kontinuiteta poslovanja, alternativni dobavljači, zahtjevi za izražavanje uvjerenja
Spremnost informacijske i komunikacijske tehnologije	ISO/IEC 27031	Kontinuitet informacijske i komunikacijske tehnologije; ciljevi oporavka; testiranje i unapređenje; usklađenost sa sustavom za upravljanje kontinuitetom poslovanja

O Institutu internih revizora

Institut internih revizora (The Institute of Internal Auditors -) IIA je međunarodno profesionalno udruženje koje okuplja više od 265.000 članova diljem svijeta i dodijelilo je više od 200.000 certifikata Certified Internal Auditor® (CIA®) diljem svijeta. Osnovano 1941. godine, IIA je diljem svijeta prepoznat kao vodeća organizacija u struci interne revizije u području u standardima, certifikatima, obrazovanju, istraživanju i tehničkim smjernicama. Za više informacija posjetite https://www.theiia.org.

Odricanje od odgovornosti

Autorska prava

April 202

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101