Organizacijos atsparumas

Teminis reikalavimas

Topical requirement

The Institute of Internal Auditors

Išvertė

Institute of Internal Auditors Lithuania

Organizacijos atsparumo teminis reikalavimas

Tarptautinę profesinės praktikos sistemą (*International Professional Practices Framework®*) sudaro Pasauliniai vidaus audito standartai (*Global Internal Audit Standards™*), Teminiai reikalavimai ir Visuotinės gairės. Teminiai reikalavimai turi būti naudojami kartu su Pasauliniais vidaus audito standartais, kurie yra autoritetingas privalomos praktikos pagrindas.

Teminiai reikalavimai pateikia aiškius lūkesčius vidaus auditoriams, nustatydami minimalius reikalavimus konkrečių rizikos sričių auditams. Atsižvelgiant į organizacijos rizikos profilį, vidaus auditoriams gali tekti apsvarstyti papildomus temos aspektus, įskaitant vietos teisės aktus.

Atitiktis teminiams reikalavimams padidins vidaus audito paslaugų atlikimo nuoseklumą ir pagerins vidaus audito paslaugų ir rezultatų kokybę bei patikimumą. Galiausiai teminiai reikalavimai kelia vidaus audito profesijos lygį. Vidaus auditoriai privalo taikyti teminius reikalavimus pagal Pasaulinius vidaus audito standartus. Atitiktis teminiams reikalavimams yra privaloma teikiant užtikrinimo paslaugas ir rekomenduojama teikiant konsultavimo paslaugas. Teminis reikalavimas taikomas, kai audito tema yra viena iš šių:

- Vidaus audito plano užduoties objektas.
- Nustatyta atliekant užduotį.
- Prašoma atlikti užduotį, kuri nebuvo įtraukta į pradinį vidaus audito planą.

Ne visi atskiri reikalavimai gali būti taikomi kiekvienai užduočiai, o kai kuriuos galima įvykdyti taikant kitus metodus. Jei reikalavimas yra netaikomas arba pakeičiamas kitais teisės aktų ar sutartiniais reikalavimais arba įgyvendinamas taikant procedūras, atitinkančias Pasaulinius vidaus audito standartus, toks pagrindimas turi būti dokumentuotas ir saugomas. Atitiktis bus vertinama atliekant kokybės vertinimus.

Daugiau informacijos rasite Organizacijos atsparumo teminio reikalavimo Naudotojo vadove.

Organizacijos atsparumas

Tarptautinė standartizacijos organizacija organizacijos atsparumą apibrėžia kaip „organizacijos gebėjimą įsisavinti ir prisitaikyti kintančioje aplinkoje“ (ISO 22316:2017). Nors ši apibrėžtis yra aiškus siekis, praktikoje organizacijos labai skiriasi pagal tai, kaip jos numato pokyčius ir trikdžius, reaguoja į juos, prisitaiko prie jų ir atsigauna po jų. Kadangi organizacijos atsparumas apima strateginius, veiklos, technologinius, žmogiškuosius, socialinius ir finansinius aspektus, vienos organizacijos gali veiksmingai priimti pokyčius, o kitos – sunkiau arba gali pasirinkti kitokius metodus, susidūrusios su neapibrėžtumu.

Organizacijos atsparumas – tai plati sąvoka, apimanti rizikas, kurios gali reikšmingai sutrikdyti ar susilpninti organizacijos gebėjimą teikti pagrindinius produktus ir paslaugas, išlaikyti suinteresuotųjų šalių pasitikėjimą ar įgyvendinti strateginius tikslus. Šios rizikos gali kilti dėl staiga prasidedančių įvykių (pavyzdžiui, stichinių nelaimių, kibernetinių atakų ir geopolitinių konfliktų), ilgalaikio aplinkos spaudimo (pavyzdžiui, išteklių trūkumo ir visuomenės sveikatos krizių) arba išorinio konteksto pokyčių (pavyzdžiui, technologinių trikdžių, reguliavimo pokyčių ir reputacijos pablogėjimo).

Šios rizikos taip pat gali būti laipsniški pokyčiai arba lėtai didėjantis spaudimas, kuris laikui bėgant gali pakenkti organizacijos stabilumui ir gebėjimui prisitaikyti. Tokios palaipsniui didėjančios rizikos dažnai gali likti nepastebėtos. Atsparios organizacijos numato ir prisitaiko tiek prie staigios, tiek prie mažiau pastebimos rizikos, kad galėtų sėkmingai veikti.

Būdingi rizikos veiksniai, didinantys grėsmę atsparumui, apima itin sudėtingą veiklą, globalizuotas tiekimo grandines, centralizuotą infrastruktūrą ar duomenų sistemas, ribotą darbuotojų prieinamumą, nepastovias rinkos sąlygas ir didelę priklausomybę nuo svarbiausių trečiųjų šalių ar geografinių vietovių. Didelio patikimumo sektoriuose veikiančios organizacijos arba organizacijos, kurioms taikoma griežta reguliacinė priežiūra, taip pat gali susidurti su iš esmės didesnėmis rizikomis dėl jų poveikio visuomenei ir atitikties įsipareigojimų.

Organizacijos atsparumas sutelktas į rizikos valdymą prieš sutrikimą, jo metu ir po jo. Vidaus auditoriai paprastai vertina informacinių technologijų (IT) procesus ir kontrolės priemones, susijusias su veiklos tęstinumu ir veiklos atkūrimu po sutrikimų. Veiklos tęstinumo plane išsamiai aprašomi veiksmai, kurių organizacija imasi, kad įvykus nelaimei būtų užtikrintas svarbiausių funkcijų vykdymas ir atkurtas įprastas veiklos režimas. Atkūrimo po incidento plane aprašoma, kaip organizacijos atkurs savo IT sistemas, svarbiausius duomenis ir operacijas po trikdančio įvykio, kad būtų atnaujinta įprasta verslo veikla.

Organizacijos atsparumui, apimančiam abu šiuos planus, reikia strateginio planavimo, įmonės rizikos valdymo, veiksmingo vadovavimo ir kultūros bei visos organizacijos kontrolės procesų. Turėdamos stiprius organizacinio atsparumo kontrolės procesus, organizacijos ne tik gali nuolat numatyti pokyčius, jiems pasirengti, į juos reaguoti ir prie jų prisitaikyti, bet ir išlikti bei klestėti.

Organizacijos atsparumo valdymo, rizikos valdymo ir kontrolės procesų vertinimas ir analizė

Šiame teminiame reikalavime pateikiamas nuoseklus ir išsamus požiūris į organizacijos atsparumo valdymo, rizikos valdymo ir kontrolės procesų kūrimo ir įgyvendinimo vertinimą. Šie reikalavimai yra minimalus organizacijos atsparumo vertinimo pagrindas.

Valdysena

Reikalavimai

Vidaus auditoriai turi įvertinti šiuos organizacijos atsparumo valdymo aspektus:

A. Vadovybė parengia oficialią organizacijos strategiją, apimančią atsparumą, o valdyba ją patvirtina ir prižiūri; joje numatomi veiklos, technologiniai ir finansiniai elementai, reikalingi pokyčiams valdyti ir veiklos tęstinumui užtikrinti. Atsparumo tikslai atitinka bendrą organizacijos požiūrį į rizikos valdymą.

B. Valdybai periodiškai pateikiama naujausia informacija apie atsparumo tikslų įgyvendinimą peržiūrai. Tai užtikrina, kad atsparumas būtų integruotas į strateginę priežiūrą, ilgalaikio planavimo procesus, vadovų kaitos planavimą ir organizacijos kultūrą, taip pat į išteklių ir biudžeto planavimą, reikalingą kritinėms veikloms palaikyti.

C. Nustatomos svarbiausių veiklos, technologinių ir finansinių procesų politikos ir procedūros, kurios periodiškai peržiūrimos, testuojamos ir prireikus atnaujinamos, siekiant stiprinti kontrolės aplinką.

D. Sukuriama ir taikoma incidentų valdymo struktūra, skirta organizacijos atsparumo tikslams prižiūrėti ir palaikyti. Ji apima sprendimų priėmimo hierarchijas, komunikacijos ir eskalavimo protokolus, vadovavimo ir veiklos vaidmenis bei atsakomybę.

E. Nustatytas procesas, kuriuo periodiškai patvirtinamos atsparumo tikslams pasiekti būtinos kompetencijos ir iš naujo įvertinamos asmenų, atliekančių svarbiausius vaidmenis atsparumo procesuose, kompetencijos.

F. Nustatytas procesas, kuriuo užtikrinama, kad visos svarbios vidaus ir išorės suinteresuotosios šalys būtų identifikuotos, nustatyti jų prioritetai ir jos būtų įtrauktos į informacijos ir ataskaitų teikimo struktūrų kūrimą, siekiant įgyvendinti organizacijos atsparumo tikslus. Suinteresuotosios šalys gali būti vyresnioji vadovybė, veiklos padaliniai, rizikos valdymo funkcija, IT, tiekimo grandinės ir (arba) pirkimų funkcijos, infrastruktūros ir patalpų valdymo funkcija, žmogiškieji ištekliai, finansų, teisės, atitikties ir viešųjų ryšių funkcijos, užtikrinimo paslaugų teikėjai, įskaitant vidaus auditą, kritiniai tiekėjai, klientai, priežiūros institucijos ir kiti subjektai.

Rizikos valdymas

Reikalavimai

Vidaus auditoriai privalo įvertinti šiuos organizacijos atsparumo rizikos valdymo aspektus:

A. Su organizacijos atsparumu susijusi rizika periodiškai nustatoma, vertinama ir valdoma visoje organizacijoje. Atsparumo rizika yra susieta su organizacijos strateginiais tikslais. Atsparumo rizikos valdymo procesas apima pagrindinių procesų vertinimą.

B. Aiškiai apibrėžta atskaitomybė ir atsakomybė už organizacijos atsparumo rizikos valdymą. Paskiriamas asmuo arba komanda, atsakingi už reguliarią organizacijos atsparumo rizikos valdymo stebėseną ir ataskaitų teikimą, įskaitant rizikos mažinimui reikalingų išteklių ir organizacijos atsparumui kylančių grėsmių nustatymą.

C. Nustatytas procesas, skirtas stebėti organizacijos atsparumo rizikos (kylančios ar anksčiau nustatytos) lygius ir operatyviai eskaluoti tas rizikas, kurios pasiekia nepriimtiną lygį, kaip apibrėžta organizacijos nustatytose rizikos valdymo gairėse ir rizikos tolerancijoje arba taikomuose teisės ir priežiūros reikalavimuose. Nagrinėjamas organizacijos atsparumo rizikos poveikis.

D. Vadovybė įdiegė ir periodiškai testuoja reagavimo į krizes, sutrikimus ir ekstremalias situacijas bei atsigavimo po jų procesą. Reagavimo į incidentus ir atkūrimo procesas apima aptikimą, prioritetų nustatymą, suvaldymą, atkūrimą ir analizę po incidento. Reagavimo į incidentus metodas apima scenarijų analizę ir periodinį testavimą nepalankiausiomis sąlygomis įvairių trikdžių atveju.

Kontrolės procesai

Reikalavimai

Vidaus auditoriai privalo įvertinti šiuos su organizacijos atsparumu susijusius kontrolės procesų aspektus:

A. Įdiegtas procesas, skirtas identifikuoti kritinius trečiųjų šalių paslaugų tiekėjus (tiekėjus ir pardavėjus) ir nustatyti minimalius atsargų lygius, reikalingus esminėms veikloms palaikyti. Šis procesas taip pat apima alternatyvių tiekėjų sąrašo atnaujinimą.

B. Nustatomi ir klasifikuojami operacijoms svarbūs duomenys. Duomenų klasifikavimas apima duomenų buvimo vietos nustatymą, kam reikalinga prieiga prie duomenų, kaip jie pasiekiami, ar yra atsarginės duomenų kopijos ir ar jas galima atkurti avariniu atveju.

C. Siekiant sumažinti informacijos saugumo rizikas (įskaitant su kibernetiniu saugumu susijusias rizikas) ir užtikrinti neskelbtinų duomenų apsaugą krizių, sutrikimų ir nepaprastųjų situacijų metu, įdiegtos svarbios IT kontrolės priemonės ir vykdoma nuolatinė stebėsena. Kontrolės priemonės ir nuolatinė stebėsena apima realiojo laiko grėsmių žvalgybą ir prieigos suteikimą tik įgaliotiems naudotojams.

D. Inventorizuojamas kritinis IT turtas. Turtas apima techninę ir programinę įrangą bei paslaugas, reikalingas veiklai užtikrinti krizių, sutrikimų ir ekstremaliųjų situacijų metu.

E. Parengti veiklos tęstinumo ir atkūrimo po incidento planai, kuriuose apibrėžti paskirtų darbuotojų ir atkūrimo komandų vaidmenys bei atsakomybės. Planai periodiškai

testuojami (pavyzdžiui, „stalo pratybos“), o apie testavimo rezultatus, įskaitant tobulinimo galimybes, pranešama valdybai ir vyresniajai vadovybei.

F. Nustatytas procesas, skirtas darbo aplinkai keisti krizių, sutrikimų ir ekstremalių situacijų metu.

G. Nustatytas procesas, skirtas nuolat stebėti ir pranešti apie kylančias grėsmes ir pažeidžiamumus, kurie gali turėti įtakos organizacijos atsparumui. Šis procesas naudojamas identifikuoti, nustatyti prioritetus ir įgyvendinti galimybes pagerinti organizacijos atsparumo veiklą, įskaitant pranešimų apie pažeidimus ar rizikos informacijos rinkimo sistemas.

H. Nustatytas darbuotojų švietimo ir mokymo apie organizacijos atsparumą procesas, užtikrinantis, kad jie žinotų apie politiką ir procedūras, kurių reikia laikytis, ir veiksmus, kurių reikia imtis įvykus krizėms, sutrikimams ir ekstremaliosioms situacijoms. Šis procesas apima mokymo pratybas, kurių metu simuliuojami trikdžių scenarijai.

I. Nustatytas procesas, užtikrinantis, kad į biudžetą būtų įtraukti būtini veiklos, žmogiškieji, technologiniai ir finansiniai ištekliai, kurie būtų prieinami krizių, sutrikimų ir ekstremaliųjų situacijų metu. Finansiniai ištekliai, reikalingi organizacijos atsparumui palaikyti, periodiškai analizuojami ir apie juos pranešama valdybai.

J. Nustatytas procesas, skirtas po įvykio peržiūrėti krizes, sutrikimus ir nepaprastąsias situacijas bei analizuoti po incidentų atliekamų peržiūrų rezultatus taikant išmoktos patirties procesą, įskaitant šių pamokų integravimą į būsimą organizacijos atsparumo planavimą.

Apie Vidaus auditorių institutą

Vidaus auditorių institutas (VAI) yra tarptautinė profesinė asociacija, vienijanti daugiau nei 265 000 narių visame pasaulyje ir suteikusi daugiau nei 200 000 sertifikuotų vidaus auditorių (CIA®) pažymėjimų visame pasaulyje. Įkurtas 1941 m., VAI visame pasaulyje pripažįstamas vidaus audito profesijos lyderiu standartų, sertifikavimo, švietimo, mokslinių tyrimų ir metodinių rekomendacijų srityje. Daugiau informacijos rasite svetainėje theiia.org.

Autorinės teisės

2026 m. balandžio mėn.

The Institute of Internal Auditors

Pasaulinė būstinė
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Telefonas: +1-407-937-1111
Faksas: +1-407-1101