Organizacijos atsparumas

Teminis reikalavimas

Topical Requirement

Naudotojo vadovas

The Institute of Internal Auditors

Išvertė

Institute of Internal Auditors Lithuania

Turinys

Teminių reikalavimų apžvalga

Teminiai reikalavimai yra esminė Tarptautinės profesinės praktikos sistemos („International Professional Practices Framework®“) sudedamoji dalis kartu su Pasauliniais vidaus audito standartais („Global Internal Audit Standards™“) ir Visuotinėmis gairėmis. Vidaus auditorių institutas reikalauja, kad Teminiai reikalavimai būtų taikomi kartu su Pasauliniais vidaus audito standartais (4.1 standartas „Pasaulinių vidaus audito standartų laikymasis“), kurie suteikia autoritetingą pagrindą reikalaujamai praktikai. Šiame vadove pateikiamos nuorodos į Standartus kaip išsamesnės informacijos šaltinį.

Teminiai reikalavimai apibrėžia, kaip vidaus auditoriai turi vertinti konkrečias rizikos sritis, taip siekiant užtikrinti nuoseklią bei kokybišką vidaus audito praktiką.. Vidaus audito įgaliojimai aiškiai apibrėžia vidaus audito funkcijos teikiamų paslaugų apimtį ir pobūdį, įskaitant ir Teminių reikalavimų taikymą (6.1 standartas „Vidaus audito įgaliojimai“). Teminiai reikalavimai nustato pagrindinius reikalavimus ir pateikia atitinkamus kriterijus, pagal kuriuos teikiamos užtikrinimo paslaugos, susijusios su Teminio reikalavimo tema (13.4 standartas „Vertinimo kriterijai“). Atitiktis Teminiams reikalavimams yra privaloma teikiant užtikrinimo paslaugas ir rekomenduojama vertinti teikiant konsultavimo paslaugas. Teminiais reikalavimais nesiekiama aprėpti visų galimų aspektų, į kuriuos reikėtų atsižvelgti atliekant užtikrinimo užduotis; veikiau jie skirti pateikti minimalų reikalavimų rinkinį, kad būtų galima nuosekliai ir patikimai įvertinti temą.

Teminiai reikalavimai aiškiai susieti su VAI (IIA) trijų linijų modeliu ir Pasauliniais vidaus audito standartais. Valdysenos, rizikos valdymo ir kontrolės procesai yra pagrindiniai Teminių reikalavimų komponentai, atitinkantys 9.1 standartą „Valdysenos, rizikos valdymo ir kontrolės procesų supratimas“. Atsižvelgiant į Trijų linijų modelį, valdysena siejama su valdyba / valdymo organu, rizikos valdymas – su antrąja linija, o kontrolė arba kontrolės procesai – su pirmąja linija. Nors vadovybei atstovaujama tiek pirmoje, tiek ir antroje linijoje, vidaus audito funkcija vaizduojama trečioje linijoje kaip nepriklausomas ir objektyvus užtikrinimo paslaugų teikėjas, atskaitingas valdybai ir (arba) valdymo organui (8 principas „Valdybos vykdoma priežiūra“).

Taikomumas, rizika ir profesinis sprendimas

Teminių reikalavimų privaloma laikytis, kai vidaus audito funkcijos atlieka užtikrinimo užduotis, susijusias su temomis, kurioms taikomas Teminis reikalavimas, arba kai Teminio reikalavimo aspektai nustatomi kitose užtikrinimo užduotyse.

Kaip aprašyta Standartuose, rizikos įvertinimas yra svarbi vidaus audito vadovo veiklos planavimo dalis. Nustatant, kokias užtikrinimo užduotis įtraukti į vidaus audito planą, reikia bent kartą per metus įvertinti organizacijos strategijas, tikslus ir riziką (9.4 standartas „Vidaus audito planas“). Planuodami atskiras užtikrinimo užduotis, vidaus auditoriai privalo įvertinti su užduotimi susijusią riziką (13.2 standartas „Užduoties rizikos vertinimas“).

Kai Teminio reikalavimo tema nustatoma rizika pagrįsto vidaus audito planavimo proceso metu ir įtraukiama į audito planą, tuomet šį Teminį reikalavimą privaloma taikyti vertinant temą per atitinkamas užduotis. Be to, kai vidaus auditoriai atlieka užduotį (įtrauktą arba neįtrauktą į planą) ir išaiškėja Teminio reikalavimo elementai, privaloma įvertinti Teminio reikalavimo taikymą atliekant užduotį. Galiausiai, jei prašoma atlikti užduotį, kuri iš pradžių nebuvo įtraukta į planą, bet apima temą,, privaloma įvertinti Teminio reikalavimo taikymą. (Žr. 9.4 standartą „Vidaus audito planas“).Taikant Teminį reikalavimą svarbiausias vaidmuo tenka profesiniam vertinimui. Rizikos vertinimai lemia vidaus audito vadovų sprendimus dėl to, kokias užduotis įtraukti į vidaus audito planą (9.4 standartas). Be to, vidaus auditoriai, remdamiesi profesiniu vertinimu, nustato, kokie aspektai bus nagrinėjami kiekvienos užduoties metu (13.3 standartas „Užduoties tikslai ir apimtis“, 13.4 standartas „Vertinimo kriterijai“ ir 13.6 standartas „Darbo programa“), ir nustato išteklius, reikalingus užduoties tikslams pasiekti (13.5 standartas „Užduoties ištekliai“). A priede „Taikymo scenarijai“ aprašoma, kaip vidaus auditoriai taiko Teminį reikalavimą.Ne visi atskiri reikalavimai gali būti taikomi kiekvienai užduočiai, taip pat kai kuriuos jų galima įgyvendinti taikant kitokius metodus. Jei reikalavimas netaikomas arba pakeičiamas kitais teisės aktų ar sutartiniais reikalavimais arba įgyvendinamas taikant procedūras, atitinkančias Standartus, tokį pagrindimą būtina dokumentuoti ir saugoti. Atitiktis bus vertinama kokybės vertinimo metu.

Atitiktis Teminiam reikalavimui turi būti dokumentuojama remiantis auditorių profesiniu vertinimu, kaip aprašyta 14.6 standarte „Užduoties dokumentai“.

Nors šis Teminis reikalavimas pateikia pagrindinius kontrolės procesus, į kuriuos reikia atsižvelgti, organizacijoms, kurios šią rizikos temą vertina kaip labai aukštą, gali tekti įvertinti papildomus aspektus.

Jei vidaus audito vadovas nustato, kad vidaus audito funkcija neturi reikiamų žinių auditavimo užduotims, susijusioms su Teminio reikalavimo sritimi, atlikti, užduoties vykdymas gali būti perduotas išoriniam paslaugų teikėjui pagal sutartį (Standartai 3.1 „Kompetencija“, 7.2 „Vidaus audito vadovo kvalifikacija“, 10.2 „Žmogiškųjų išteklių valdymas“). Vidaus audito vadovams gali būti naudingas Tarptautinio Vidaus auditorių instituto Vidaus audito kompetencijų modelio („Internal Auditing Competency Framework™“) šaltinis. Standartai taikomi bet kuriam asmeniui ar funkcijai, teikiančiai vidaus audito paslaugas, nepriklausomai nuo to, ar organizacija vidaus auditorius įdarbina tiesiogiai, ar jų paslaugas perka iš išorės paslaugų teikėjo, ar taiko abu šiuos būdus. Vidaus audito vadovui tenka galutinė atsakomybė už atitikties užtikrinimą. Be to, jei vidaus audito vadovas nustato, kad vidaus audito ištekliai yra nepakankami, jis turi informuoti valdybą apie nepakankamų išteklių poveikį ir apie tai, kaip bus sprendžiamas išteklių trūkumo klausimas (8.2 standartas „Ištekliai“).

Vykdymas, dokumentavimas ir ataskaitų teikimas

Taikydami Teminius reikalavimus, vidaus auditoriai taip pat privalo laikytis Standartų ir savo darbą atlikti pagal jų V sritį: Vidaus audito paslaugų teikimas. V srities standartuose aprašomas užduočių planavimas (13 principas „Veiksmingai planuoti užduotis“), užduočių vykdymas (14 principas „Atlikti užduoties darbą“) ir užduočių rezultatų komunikavimas (15 principas „Pranešti apie užduoties rezultatus ir vykdyti veiksmų planų stebėseną“).

Teminiai reikalavimai yra skirti nuosekliai ir kokybiškai vidaus audito praktikai palaikyti. Jie yra taikomi kartu su galiojančiais vietos įstatymais, kitais teisės aktais, priežiūros institucijų lūkesčiais ir kitomis profesinėje praktikoje pripažintomis nuostatomis, kurios gali nustatyti

papildomus arba išsamesnius reikalavimus. Vidaus auditoriai, remdamiesi šiais teisės aktais, reikalavimais ir metodikomis, gali būti jau parengę audito užduočių darbo programas ir testavimo procedūras. Vidaus auditoriai turėtų suderinti numatytą organizacijos atsparumo kontrolės priemonių testavimą ir bet kokį patikimą kitų vidaus bei išorės užtikrinimo paslaugų teikėjų atliktą testavimą (9.5 standartas „Koordinavimas ir rėmimasis paslaugų teikėjų darbu“) su Teminiu reikalavimu, kad būtų užtikrinta pakankama aprėptis. Teminio reikalavimo apimtis gali būti dokumentuojama vidaus audito plane arba užduoties darbo programoje, remiantis auditorių profesiniu vertinimu. Reikalavimus gali apimti viena ar kelios vidaus audito užduotys. Be to, gali būti taikomi ne visi reikalavimai. Privaloma išsaugoti įrodymus, patvirtinančius, kad buvo įvertintas Teminio reikalavimo pritaikomumas, įskaitant bet kokių išimčių taikymo pagrindimą. Rengiant vidaus auditorių darbo dokumentus, rekomenduojama remtis D priede pateikta metodine priemone.

Kokybės užtikrinimas

Standartuose reikalaujama, kad vidaus audito vadovas parengtų, įgyvendintų ir palaikytų kokybės užtikrinimo ir tobulinimo programą, apimančią visus vidaus audito funkcijos aspektus (8.3 standartas „Kokybė“, 8.4 standartas „Išorės kokybės vertinimas“, 12.1 standartas „Vidaus kokybės vertinimas“). Rezultatai privalo būti pateikti valdybai ir vyresniajai vadovybei. Komunikacijoje privaloma pateikti informaciją apie vidaus audito funkcijos atitiktį Standartams ir veiklos tikslų pasiekimą.

Teminių reikalavimų atitiktis turi būti užtikrinama užduoties lygmens priežiūros metu (12.3 standartas „Užduočių vykdymo priežiūra ir tobulinimas“) ir tikrinama kokybės vertinimų metu. Ruošdamiesi kokybės peržiūrai, vidaus auditoriai gali naudotis D priede pateikta metodine medžiaga.

Organizacijos atsparumas

Organizacijos atsparumas – tai organizacijos gebėjimas atlaikyti pokyčius ir prie jų prisitaikyti, ypač nestabilios veiklos sąlygomis. Pagal Tarptautinės standartizacijos organizacijos ISO 22316 standartą jis apibrėžiamas kaip „organizacijos gebėjimas įsisavinti ir prisitaikyti kintančioje aplinkoje“. Nors šis apibrėžimas nusako siektiną organizacijos atsparumo lygį, visgi praktikoje organizacijos nevienodai geba numatyti pokyčius ir veiklos sutrikimus, į juos reaguoti, prie jų prisitaikyti ir atkurti veiklą. Kadangi organizacijos atsparumas apima strateginę, veiklos, technologinę, žmogiškųjų išteklių, socialinę ir finansinę sritis, vienos organizacijos geba veiksmingai prisitaikyti prie pokyčių, o kitos tai daro sunkiau arba, susidūrusios su neapibrėžtumu, pasirenka kitokius veikimo būdus.

Praktine prasme, atsparios organizacijos yra geriau pasirengusios išgyventi netikėtus iššūkius ir, su jais susidūrusios, ne tik išlaikyti veiklą, bet ir toliau vystytis.

Organizacijai siekti strateginių tikslų gali sutrukdyti įvairūs trikdžiai, įskaitant, bet neapsiribojant:

- Stichinės nelaimės, pavyzdžiui, žemės drebėjimai, gaisrai, potvyniai, uraganai, cunamiai, atogrąžų audros ir kiti ekstremalūs meteorologiniai reiškiniai.

- Kibernetinės atakos, pavyzdžiui, išpirkos reikalaujanti programinė įranga, kenkėjiškos programos, atsisakymas teikti paslaugas, duomenų saugumo pažeidimai, grėsmės iš vidaus ir kiti kenkėjiški veiksmai, kuriais siekiama pakenkti organizacijai arba sutrukdyti jai vykdyti veiklą.
- Geopolitiniai konfliktai, pavyzdžiui, ekonominės sankcijos, muitai, terorizmas, karas ir kiti konfliktai tarp valstybių.
- Aplinkos spaudimas, pavyzdžiui, išteklių trūkumas, visuomenės sveikatos krizės, tvarumo veiksniai arba klimato kaita.
- Kintantys išorės veiksniai, pavyzdžiui, besivystančios technologijos (įskaitant dirbtinį intelektą), atitikties (teisinės, reguliavimo ir finansinės atskaitomybės), užimtumo lygio, vartotojų paklausos ir reputacijos pokyčiai.
- Finansiniai iššūkiai, tokie kaip infliacija ar defliacija, palūkanų normos, valiutų kursai ir vyraujančios rinkos sąlygos, pavyzdžiui, nuosmukis ar ekonomikos plėtra.
- Veiklos sunkumai, pavyzdžiui, sudėtingi procesai, didelė priklausomybė nuo trečiųjų šalių, geografinė padėtis, kultūriniai sunkumai, ribotos galimybės naudotis darbo jėga, neveiksmingas vadovavimas ar rizikos valdymas.
- Tiekimo grandinės problemos, pavyzdžiui, negalėjimas apsirūpinti žaliavomis, įvairių tiekėjų trūkumas ir nepastovios prekių kainos.
- Vidaus įvykiai, pavyzdžiui, pagrindinių darbuotojų kaita ir veiklos klaidos.

Kad ir koks būtų veiklą trikdantis veiksnys, organizacija turėtų turėti aiškiai apibrėžtą organizacijos atsparumo strategiją ir formalizuotus procesus, leidžiančius nuolat numatyti pokyčius, jiems pasirengti, į juos reaguoti ir prie jų prisitaikyti. Organizacijos atsparumas yra platus terminas, apimantis skirtingus, nuo organizacijos pobūdžio priklausančius elementus, tokius kaip veiklos tęstinumo valdymas, veiklos atkūrimas po veiklos sutrikimų, kritinių funkcijų matricos, kritinių funkcijų pakeičiamumo planai ir atkūrimo testavimas.

Organizacijos atsparumo Teminiai reikalavimai apima:

- **Valdymas** – aiškiai apibrėžti baziniai atsparumo tikslai ir strategijos, padedantys įgyvendinti organizacijos misiją ir viziją.
- **Rizikos valdymas** – procesai, skirti nustatyti, analizuoti, valdyti ir stebėti atsparumo grėsmes, įskaitant mechanizmą, užtikrinantį laiku teikiamą pranešimą apie atsparumo incidentus.
- **Kontrolė** – vadovybės nustatyti, periodiškai vertinami kontrolės procesai, skirti atsparumo rizikai valdyti.

Aspektai

Vidaus auditoriai, vertindami Organizacijos atsparumo Teminio reikalavimo nuostatas, gali remtis toliau nurodytais argumentais. Kiekvienas vertinimo aspektas yra pažymėtas raidiniu žymėjimu ir susietas su tam tikru Teminio reikalavimo punktu. Šie aspektai yra pavyzdiniai ir nėra privalomi. Vidaus auditoriai, nustatydami, kas turi būti įtraukta į jų vertinimus, turėtų vadovautis profesiniu vertinimu.

Viešojo sektoriaus vidaus audito užduočių apribojimai, atsirandantys dėl teisės aktų, valdžios struktūros ar politinės aplinkos, gali riboti tam tikrus šio vertinimo aspektus. Viešojo sektoriaus vidaus auditoriai turėtų dokumentuoti tokius apimties apribojimus kaip rizikos vertinimo proceso dalį ir, vadovaudamiesi profesiniu sprendimu, aiškiai apibrėžti bei komunikuoti pritaikytą peržiūros apimtį.

Valdysenos aspektai

Siekiant įvertinti, kaip valdysenos procesai yra taikomi atsparumo tikslams, vidaus auditoriai gali peržiūrėti šiuos įrodymus:

A. Vadovybės parengtą ir valdybos patvirtintą bei prižiūrimą dokumentuotą atsparumo strategiją. Ji yra oficialiai komunikuojama visiems darbuotojams ir suderinta su organizacijos misija, vizija, kultūra bei rizikos valdymu, kuriuos ji taip pat palaiko. Valdyba tvirtina atsparumo strateginio plano tikslus, kurie yra suderinti su bendru organizacijos rizikos valdymo modeliu ir yra periodiškai testuojami bei peržiūrimi. Planas gali apimti operatyvinius, technologinius bei finansinius elementus, tokius kaip:

   - Veiklos [1]–- atsparumo koordinavimas visoje organizacijoje; atsparumo rizikos vertinimo procesai; veiklos tęstinumo planavimas, apimantis periodinį testavimą ir ataskaitų teikimą; krizių valdymas; darbuotojų prisitaikomumas (pvz., nuotolinio papildomo pajėgumo didinimas, minimalus darbuotojų skaičius vietoje ir kryžminis svarbiausių vaidmenų mokymas); svarbiausių darbuotojų pakeičiamumo planavimas; tiekimo grandinės atsparumas; pagrindinių veiklos rodiklių (KPI) nustatymas; valdybos narių mokymas, siekiant užtikrinti informuotumą.
   - Technologiniai – IT infrastruktūros reikalavimai; kritinių duomenų identifikavimas (duomenų klasifikavimas); atsarginės duomenų kopijos; kibernetinio saugumo stiprinimas ir grėsmių stebėsena; kritinio technologinio turto priežiūra; apibrėžtas svarbiausių duomenų atkūrimo taško tikslas (RPO) ir atkūrimo laiko tikslas (RTO) (patvirtinta atliekant atkūrimo bandymus).

- Finansiniai – atsparumui užtikrinti skirti biudžeto ištekliai; grynųjų pinigų atsargos, skirtos veiklai palaikyti sutrikimo metu; finansinės atskaitomybės procesai, skirti tiksliai fiksuoti su veiklos sutrikimu susijusias operacijas; draudimo polisai, skirti veiklos sutrikimo rizikai mažinti; galimybė pasinaudoti kredito linijomis, skirtomis skubiam skolinimuisi.

B. Periodiškai (pvz., kas mėnesį ar kas ketvirtį) valdybai teikiami atnaujinti duomenys apie organizacijos atsparumą, kuriuos rengia už organizacijos atsparumą atsakingas asmuo arba komanda. Šie duomenys gali apimti nustatytus rizikos tolerancijos kriterijus, KPI rodiklius ar kitą informaciją, atskleidžiančią pastebėjimus bei tendencijas. Šie duomenys parodo organizacijos atsparumo strategijos tikslų įgyvendinimo statusą, įskaitant strateginę priežiūrą, stebėseną ir ilgalaikį planavimą. Ataskaitos gali apimti šių sričių stebėsenos rezultatus:

   - Strateginių atsparumo tikslų pasiekimo lygis ir galimi jų įgyvendinimo kliūčių veiksniai.
   - Biudžeto poreikiai atsparumo tikslams ir uždaviniams įgyvendinti, pavyzdžiui, technologinio turto poreikis.
   - Atsparumo rizikų būklė, įskaitant reikšmingus pokyčius atsparumo rizikos aplinkoje, galinčius paveikti nustatytus rizikos tolerancijos lygius.
   - Atsparumo vidaus kontrolės priemonių veiksmingumas, įskaitant ištaisymo veiksmų pažangą.
   - KPI, skirti atsparumo veiksmingumui matuoti.
   - Žmogiškųjų išteklių poreikiai, susiję su darbuotojų, atsakingų už atsparumą, įdarbinimu, mokymu ir kompetencijų ugdymu.

C. Politikos, procedūros ir kiti susiję dokumentai, taikomi operaciniams, technologiniams ir finansiniams atsparumo procesams valdyti, įskaitant:

   - Kaip identifikuojami kritiniai atsparumo procesai ir periodiškai vertinami, ar jie vis dar tiksliai atspindi svarbiausius organizacijos procesus.
   - Politikos peržiūrimos ir atnaujinamos ne rečiau kaip kartą per metus (ar dažniau, esant aukštesniam rizikos lygiui), taip pat dažniau, kai atsiranda naujų atsparumo rizikų arba atsižvelgiant į patirtį, įgytą atliekant testavimą ar įvykus realiems veiklos sutrikimams.
   - Peržiūros procesas, skirtas politikų ir procedūrų pakankamumui atsparumo veiklos palaikymui įvertinti.
   - Ar atsparumo procesai ir vidaus kontrolės priemonės stiprinami taikant plačiai pripažintas susijusių procesų, pavyzdžiui, rizikos valdymo, informacinių technologijų ar valdysenos, sistemas. Pavyzdžiai gali apimti tokių organizacijų kaip NIST, COSO ar ISO praktiką, ypač ISO 22300 standartus (pvz., ISO 22316 ar ISO 22336).

D. Nustatyta ir dokumentais pagrįsta incidento valdymo struktūra, kurioje aprašyti vadovų vaidmenys ir pareigos, susijusios su atsparumo tikslų įgyvendinimu. Įrodymai apie nustatytą sprendimų priėmimo hierarchiją, pavyzdžiui, darbuotojai, atsakingi už su atsparumu susijusius sprendimus veiklos sutrikdymo metu, ir tvirtinimai, reikalingi operatyviniams sprendimams, tokiems kaip lėšų skyrimas ar sutarčių su trečiosiomis

šalimis sudarymas siekiant pagalbos veiklos sutrikimų metu. Taip pat reikėtų atsižvelgti į dokumentais patvirtintus incidentų eskalavimo būdus ir laikinus sprendimų priėmimo įgaliojimus veiklos sutrikimo metu, įskaitant finansinių įgaliojimų delegavimą ir trečiųjų šalių sutarčių sudarymo limitus.

E. Nustatytas procesas, pagal kurį periodiškai (pvz., kartą per metus ar kas pusmetį) vertinamos darbuotojų, atsakingų už organizacijos atsparumo procesų įgyvendinimą ir valdymą, žinios, įgūdžiai ir gebėjimai. Šis procesas gali apimti mokymo poreikių nustatymą ir tinkamų kvalifikacijos tobulinimo priemonių parinkimą, pavyzdžiui, kontaktinius ar nuotolinius mokymus, konferencijas, savarankiško mokymosi kursus ar profesinį sertifikavimą. Įrodymai, kad vykdomas kritinių atsparumo funkcijų pakeičiamumo planavimas, įskaitant scenarijų testavimą, siekiant nustatyti veiklas, kurias gali atlikti tik vienas arba nedidelis skaičius darbuotojų. Reikalavimai darbuotojų, galinčių perimti šias funkcijas, kvalifikacijai yra apibrėžti.

F. Nustatytas procesas, pagal kurį identifikuojamos, prioretizuojamos ir prireikus įtraukiamos atitinkamos vidaus ir išorės suinteresuotosios šalys, siekiant sukurti informacijos teikimo ir atskaitomybės mechanizmą, leidžiantį nustatyti esamus pažeidžiamumus, kylančias grėsmes ir tinkamai į jas reaguoti. Įrodymai, kad suinteresuotosios šalys dalyvauja svarstant organizacijos atsparumo pažeidžiamumus ir galimas grėsmes. Įrodymai gali būti elektroniniai laiškai, posėdžių protokolai arba ataskaitos, įskaitant nuorodas į organizacijos mastu taikomų rodiklių naudojimą atsparumo veiksmingumui vertinti ir stebėti.

Rizikos valdymo aspektai

Siekdami įvertinti, kaip rizikos valdymo procesai taikomi organizacijos atsparumo tikslams pasiekti, vidaus auditoriai gali peržiūrėti įrodymus, kad:

A. Organizacijos rizikos vertinimo ir rizikos valdymo procesai apima organizacijos atsparumo rizikų nustatymą, yra vykdomi nuolat ir dokumentuojami, o rezultatai komunikuojami visoje organizacijoje. Atsparumo rizikos valdymo procesas apima pagrindinių procesų vertinimą, įskaitant veiklą, organizacijos rizikos valdymą, IT, tiekimo grandinę ir (arba) pirkimus, patalpas, žmogiškuosius išteklius, finansus, teisę, atitiktį, reguliavimą, viešuosius ryšius, svarbiausius tiekėjus, reputaciją, kylančias rizikas ir kitus procesus. Be atsparumo rizikos nustatymo, procesai apima ir grėsmių bei pažeidžiamumų, galinčių sutrikdyti verslo veiklą, vertinimą, siekiant nustatyti, kaip jie yra:
    - Iš pradžių nustatomi ir apie juos pranešama.
    - Analizuojami siekiant įvertinti riziką organizacijos tikslų pasiekimui.
    - Mažinami, įskaitant veiksmų planus, skirtus rizikai sumažinti iki priimtino lygio.
    - Stebimi, įskaitant nuolatinio ataskaitų teikimo planą, kol grėsmės bus visiškai pašalintos.

Papildomi įrodymai gali būti:

- Ataskaitos, el. laiškai ar susitikimų protokolai, kuriuose nurodomi dalyvaujantys veiklos padaliniai (arba organizacijos sritys). Gali būti įtraukti tokie rizikos veiksniai kaip poveikis, tikimybė, pasireiškimo greitis ir kiti aspektai.
- Glaudžiai susiję arba tarpusavyje priklausomi rizikos veiksniai analizuojami siekiant nustatyti bendrą kelių rizikos veiksnių sukeltą poveikį.
- Rizikos vertinimas apima kritinio turto apsaugos lygių ir išteklių vertinimą, siekiant išvengti vieno gedimo taško.
- Rizikos vertinimas atnaujinamas atsižvelgiant į patirtį, įgytą iš faktinių krizių, sutrikimų ir testavimų bei scenarijų rezultatų.
- Organizacija, remdamasi galimu poveikiu ir tikimybe, nustatytais atlikus poveikio verslui analizę, prioritetą teikia didžiausią riziką keliančioms sritims.

B. Organizacija yra priskyrusi ir periodiškai peržiūri atsakomybę bei atskaitomybę asmeniui ar komandai, kuri stebi atsparumo riziką ir teikia apie ją ataskaitas. Asmenį arba komandą sudaro kvalifikuoti specialistai, turintys atsparumo valdymo patirties, pageidautina organizacijos veiklos srityje (pvz., sveikatos priežiūros, finansinių paslaugų ar viešajame sektoriuje). Asmuo arba komanda dalyvauja periodiniuose mokymuose, kad būtų informuoti apie naujai atsirandančias atsparumo rizikos tendencijas.

C. Organizacija yra nustačiusi procesą, skirtą organizacijos atsparumo rizikai (naujai atsirandančiai arba anksčiau nustatytai) stebėti ir greitai eskaluoti tas rizikas, kurios pasiekia nepriimtiną lygį, kaip apibrėžta organizacijos rizikos valdymo gairėse ir rizikos tolerancijoje arba taikomuose teisiniuose ir reguliavimo reikalavimuose. Vertinamas finansinių ir nefinansinių rodiklių poveikis organizacijos atsparumo rizikai. Finansinių rodiklių pavyzdžiai: pajamos, išlaidos, pelningumas, pinigų srautai, skola, akcijų kaina ir bendra vertė. Nefinansinių rodiklių pavyzdžiai: prekės ženklo reputacija, klientų pasitenkinimas, poveikis aplinkai ir personalo kaita. Procesas apima:

- Pirminį rizikos nustatymą ir savalaikį eskalavimą.
- Analizę, skirtą įvertinti riziką ir tai, kaip ji gali sutrukdyti pasiekti organizacijos tikslus.
- Pasiūlyti ir suderinti rizikos mažinimo veiksmų planai, įskaitant būdus laiku sumažinti riziką iki priimtino lygio. Veiksmų planai grindžiami bendrąja organizacijos rizikos valdymo strategija. Pasiūlyme turėtų būti nurodyti būtini rizikos mažinimo ištekliai, pavyzdžiui, finansiniai ištekliai, darbuotojų darbo valandos ir papildomos technologijos bei programinė įranga, reikalingos gebėjimams stiprinti.
- Nuolatinė rizikos stebėsena ir ataskaitų teikimas apie pagrindinius rizikos rodiklius, kol grėsmės bus visiškai pašalintos.

D. Organizacijoje įdiegtas procesas, skirtas reaguoti į krizes, veiklos sutrikimus, ekstremaliąsias situacijas ar kitus incidentus ir atsigauti po jų. Procesas periodiškai yra išsamiai testuojamas, pavyzdžiui, kas ketvirtį arba kasmet, ir gali būti atliekamas dažnesnis dalinis testavimas, pavyzdžiui, kas mėnesį. Kritinėms paslaugoms gali būti reikalingas dažnesnis testavimas. Reagavimo į incidentus ir atkūrimo procesas gali apimti:

- Aptikimas – nuolatinė kibernetinių įvykių stebėsena. Tai gali apimti įsilaužimų aptikimo sistemas, grėsmių žvalgybos arba saugumo informacijos ir įvykių valdymo (SIEM) sistemų naudojimą. SIEM sistemoje gali būti naudojamas dirbtinis intelektas, siekiant sustiprinti šį procesą. Stichinių nelaimių arba infrastruktūros ar patalpų sutrikimų atveju organizacija yra sukūrusi komunikacijos tinklą (pvz., perspėjimo protokolus ar pranešimus), kad būtų užtikrintas savalaikis informavimas ir dalijamasi informacija. Visų įvykių atveju organizacija yra nustačiusi procesą, kaip pranešti atitinkamoms pagalbos ir gelbėjimo tarnyboms bei teisėsaugos institucijoms. Įvykiai turėtų būti prioritetizuojami pagal jų kritiškumo lygį.
- Reagavimas ir suvaldymas – reagavimo į incidentus metodas apima scenarijų analizę ir periodinį testavimą nepalankiausiomis sąlygomis, atsižvelgiant į įvairius trikdančius įvykius. Pavyzdžiui, siekdama užkirsti kelią tolesnei žalai kibernetinių įvykių metu, organizacija yra įdiegusi procesą, skirtą pažeistam turtui izoliuoti, pavyzdžiui, nukreipiant tinklo srautą kitu maršrutu arba ribojant naudotojų prieigą įvykio metu. Fizinių incidentų atveju organizacija yra įdiegusi procesą, skirtą fiziškai izoliuoti veiklą trikdančius įvykius, siekiant apriboti jų poveikį, įskaitant darbuotojų perkėlimą į alternatyvią vietą.
- Atkūrimas – kibernetinių ar IT incidentų atveju organizacija yra nustačiusi procedūras, pagal kurias pirmenybė teikiama kritinių išteklių, reikalingų veiklai atnaujinti, atkūrimui (pvz., duomenų atkūrimui iš atsarginių kopijų ar serverių veikimo atkūrimui). Kitiems ne IT ištekliams, kurie reikalingi veiklai atnaujinti, taip pat turėtų būti nustatyti atkūrimo prioritetai. Tai gali apimti laipsniško pagrindinių darbuotojų arba esminių funkcijų veiklos atkūrimo planavimą.
- Analizė po incidento – organizacija analizuoja įvykius, kad nustatytų:
  - Esmines trikdančių įvykių priežastis.
  - Atliktų veiksmų veiksmingumą.
  - Patobulinimus, reikalingus atsparumo procesams stiprinti, pavyzdžiui, politikas, procedūrų, rizikos vertinimo ar strategijos atnaujinimą ir kt.

Reagavimo ir veiklos atkūrimo proceso išsamumo bei veiksmingumo testavimas, atliekant stalo pratybas, simuliacijas ir praktines pratybas, apimančias kritines paslaugas / funkcijas ir jų priklausomybes, gali būti suderintas su organizacijos rizikos tolerancijos lygiais. Šie įvykiai gali kilti dėl vidaus arba išorės incidentų. Šių pratybų rezultatus gali peržiūrėti valdyba ir vyresnioji vadovybė, o tobulinimo veiksmai gali būti stebimi ir apie juos periodiškai teikiamos ataskaitos. Rekomendacijos turėtų būti įgyvendinamos praktiškai, aiškiai nustačius atsakingus asmenis ir terminus.

Kontrolės proceso aspektai

Siekdami įvertinti, kaip kontrolės procesai taikomi organizacijos atsparumo tikslams pasiekti, vidaus auditoriai gali peržiūrėti įrodymus ir patikrinti, ar:

A. Įdiegtas procesas, skirtas nustatyti ir įvertinti kritinius trečiųjų šalių paslaugų teikėjus (tiekėjus ir pardavėjus) ir minimalius atsargų lygius, reikalingus gyvybiškai svarbiai veiklai. Atliekant vertinimą gali būti atsižvelgiama į trečiųjų šalių atsparumą ir veiklos tęstinumą

bei nustatomi kiekvieno tiekėjo rizikos reitingai. Organizacija gali ne tik vertinti tiekėjus prieš sudarydama sutartį, bet ir periodiškai juos peržiūrėti, kad nuolat vertintų jų rizikos reitingus. Organizacija turi potencialių pakaitinių tiekėjų sąrašą, jei bendradarbiavimas su esamu tiekėju nutrūktų.

B. Vadovybė atliko duomenų klasifikavimą, visų pirma nustatydama kritinius duomenis, kurie reikalingi atsigauti po trikdančių įvykių ir užtikrinti veiklos tęstinumą. Organizacija įdiegė veiksmingas vidaus kontrolės priemones, skirtas apsaugoti kritinius duomenis, įskaitant prieigos suteikimą tik įgaliotiems darbuotojams ir užtikrinimą, kad kritinių duomenų atsarginės kopijos būtų kuriamos ir prireikus galėtų būti laiku atkurtos.

C. Vadovybė nustatė svarbiausias IT kontrolės priemones ir nuolatinės stebėsenos procesus, skirtus informacijos saugumo rizikai (įskaitant su kibernetiniu saugumu susijusią riziką) mažinti ir užtikrinti, kad jautrūs duomenys būtų apsaugoti trikdžių metu. Jautrūs duomenys apsaugomi šifravimo priemonėmis. Nuolatinė stebėsena ir realaus laiko informacija apie grėsmes užtikrina, kad vadovybė būtų laiku įspėjama, o nustatytos problemos būtų sprendžiamos laiku. Gali būti naudojamos plačiai pripažintos kontrolės sistemos, kurias parengė tokios organizacijos kaip NIST, COSO, ISO ir kitos.

D. Organizacija inventorizavo kritinį IT turtą, įskaitant techninę ir programinę įrangą bei paslaugas, reikalingas veiklai palaikyti krizių, sutrikimų ir nepaprastųjų situacijų metu. IT turtas, kurį sunkiau greitai įsigyti, priskiriamas prie prioritetinių.

E. Parengti veiklos tęstinumo planas ir veiklos atkūrimo planas, nustatomi atkūrimo komandų darbuotojai, kurie sudaromi remiantis veiklos poveikio analize. Planai periodiškai testuojami, pavyzdžiui, kas ketvirtį arba kasmet, atliekant stalo pratybas arba testavimą nepalankiausiomis sąlygomis, kai sutrikimai imituoja realias ekstremaliąsias situacijas ir tikrinami ryšių su vidaus ir išorės suinteresuotosiomis šalimis protokolai. Apie testavimo rezultatus, įskaitant nustatytas tobulinimo galimybes, pranešama valdybai ir vyresniajai vadovybei.

F. Nustatytas procesas, kaip pritaikyti darbo aplinką trikdžių metu. Pakeitimai gali apimti alternatyvias darbo vietas, pavyzdžiui, darbą namuose arba laikino biuro įsteigimą, užtikrinant savalaikį ir veiksmingą veiklos tęstinumą. Organizacija gali naudoti hibridinio ar nuotolinio darbo galimybes, kaip alternatyvą darbui vietoje. Kiti aspektai gali apimti savalaikio ir veiksmingo išteklių, įskaitant IT ir žmogiškuosius išteklius, mobilizavimo ir perskirstymo protokolus.

G. Įdiegtas procesas, skirtas nuolat stebėti ir pranešti apie kylančias grėsmes ir pažeidžiamumus, susijusius su organizacijos atsparumu, ir nustatyti, prioritetizuoti ir įgyvendinti organizacijos atsparumo veiklos gerinimo galimybes. Stebėsenos veikla gali apimti pagrindinius rizikos rodiklius (KRI), rizikos suvestines, rizikos horizonto stebėsenos veiklas. Organizacija gali visiems darbuotojams teikti naujausią informaciją apie kylančias grėsmes, siekdama didinti informuotumą, įskaitant informaciją apie rizikos mažinimo ar kontrolės priemones. Visa pranešėjų apie pažeidimus veikla yra registruojama, analizuojama, laiku išnagrinėjama ir komunikuojama vyresniajai vadovybei. Problemoms išspręsti gali prireikti nuolatinės stebėsenos, todėl gali būti reikalingas papildomas ataskaitų teikimas.

H. Įdiegtas procesas, skirtas darbuotojų švietimui ir mokymui apie organizacijos atsparumo politikas ir procedūras, kurių reikia laikytis krizių, sutrikimų ar ekstremalių situacijų atveju. Šis procesas apima mokomąsias pratybas, kurių metu imituojami trikdžių scenarijai. Mokymai vykdomi periodiškai, pavyzdžiui, kas ketvirtį arba kasmet. Kritinėms paslaugoms gali reikėti dažnesnio testavimo.

I. Nustatytas procesas, užtikrinantis, kad krizės, veiklos sutrikimų ir ekstremaliųjų situacijų metu būtini veiklos, žmogiškieji, technologiniai ir finansiniai ištekliai būtų suplanuoti biudžete ir prieinami. Vadovybė periodiškai, pavyzdžiui, kas ketvirtį ar kasmet, peržiūri išteklius, kad įsitikintų, jog jie yra pakankami, atsižvelgiant į nustatytą rizikos lygį, ir apie poreikius informuoja valdybą. Kritinėms paslaugoms gali reikėti dažnesnio testavimo. Analizė apima likvidumo, draudimo apsaugos ir nenumatytų finansavimo priemonių vertinimą. Finansinių išteklių poreikis planuojamas atsižvelgiant į tokius veiksnius kaip organizacijos dydis, sudėtingumas, veiklos sritis ir rizikos profilis. Šis procesas gali apimti išankstinį finansavimo patvirtinimą.

J. Įdiegtas procesas, skirtas krizėms, sutrikimams ir ekstremalioms situacijoms peržiūrėti po jų atsiradimo ir analizuoti po incidentų atliktas peržiūras, remiantis įgyta patirtimi. Peržiūrų rezultatai turėtų būti dokumentuojami oficialiose ataskaitose, o įgyta patirtis turėtų būti įtraukta į būsimą atsparumo planavimą.

A priedas. Taikymo scenarijai

Toliau pateikiami scenarijai, kuriais atvejais yra taikomas Organizacijos atsparumo Teminis reikalavimas. VAI (IIA) „Teminių reikalavimų taikymo gairėse“ tai pat pateikiami praktiniai patarimai, kaip taikyti privalomuosius reikalavimus, spręsti apribojimų klausimus ir nustatyti kritines rizikos ribas.

1 scenarijus: Organizacijos atsparumas į vidaus audito planą įtraukiamas kaip audito užduoties tema.

Kai vidaus audito funkcija užbaigia rizika pagrįstą planavimo procesą ir į savo vidaus audito planą įtraukia vieną ar daugiau užduočių, susijusių su organizacijos atsparumu, atliekant tokias užduotis turi būti taikomas Teminis reikalavimas. Atitiktis gali būti užtikrinama taikant reikalavimus vienoje ar keliose į vidaus audito planą įtrauktose užduotyse.

Organizacijos atsparumas yra plati tema, todėl ne kiekvienas Teminio reikalavimo reikalavimas gali būti taikomas kiekvienai užduočiai. Kai vidaus auditoriai, vadovaudamiesi profesiniu sprendimu, nustato, kad vienas ar keli Organizacijos atsparumo Teminio reikalavimo reikalavimai nėra taikytini ir todėl neturėtų būti įtraukti į užduotį, jie privalo dokumentuoti ir išsaugoti šių reikalavimų neįtraukimo pagrindimą. Pavyzdžiui, kai kurių reikalavimų netaikymas gali būti grindžiamas tuo, kad vidaus audito funkcija rotacijos principu atlieka įvairias organizacijos atsparumo audito užduotis arba yra nustačiusi, kad konkrečios rizikos reikšmingumas nagrinėjamoje užduotyje yra mažas.

2 scenarijus: Organizacijos atsparumo rizikos nustatomos atliekant audito užduotį, kuri nėra skirta organizacijos atsparumui vertinti.

Vidaus auditoriai gali nustatyti atsparumo rizikas vertindami procesą, kuris nėra tiesiogiai susijęs su organizacijos atsparumu. Pavyzdžiui, vertindami žmogiškųjų išteklių procesus, įskaitant darbuotojų samdymą ir išlaikymą, vidaus auditoriai gali nustatyti atsparumo rizikas, kurios planuojant audito užduotį nebuvo įtrauktos į jos apimtį. Tačiau atlikę pirminį proceso peržiūros etapą, vidaus auditoriai nustato, kad šios rizikos patenka į užduoties apimtį. Pavyzdžiui, jie nustato darbuotojų kaitos ir pareigų perėmimo planavimo rizikas, susijusias darbuotojų išlaikymu (13.2 standartas „Užduoties rizikos vertinimas“).

Nustačius atitinkamas rizikas, vidaus auditoriai turi peržiūrėti Organizacijos atsparumo Teminį reikalavimą ir nustatyti, kurie reikalavimai yra taikytini. Šiame pavyzdyje jie gali sutelkti dėmesį tik į E reikalavimą, susijusį su valdysena, ir netaikyti kitų rizikos valdymo ir kontrolės reikalavimų. Užduoties darbo dokumentuose jie turi pagrįsti ir dokumentuoti kitų Organizacijos atsparumo Teminio reikalavimo nuostatų netaikymą bei išsaugoti šiuos dokumentus.

3 scenarijus: Prašoma atlikti organizacijos atsparumo audito užduotį, kuri iš pradžių nebuvo įtraukta į vidaus audito planą.

Suinteresuotosios šalys, tokios kaip valdyba, vadovybė ar priežiūros institucija, gali paprašyti vidaus auditorių atlikti atsparumo vertinimą, nenumatytą pradiniame audito plane. Pavyzdžiui, organizacijai tapus kibernetinės atakos taikiniu, valdyba gali paprašyti atlikti vidaus audito užduotį, skirtą atsparumo kontrolės priemonėms įvertinti ir nustatyti, kaip gerai organizacija yra pasirengusi atsigauti po kibernetinės atakos. Teminis reikalavimas yra taikytinas, kriterijai turi būti įvertinti, o visos išimtys – dokumentuotos (9.4 standartas „Vidaus audito planas“).

B priedas. Audito užduočių pavyzdžiai pagal taikymo scenarijus

1 scenarijus: Tema numatyta kaip užduotis vidaus audito plane.

Viešojo sektoriaus subjektas, atsakingas už centrinę didmeninę rinką

Metinio rizika grindžiamo planavimo proceso metu vidaus audito funkcija esminių rinkos operacijų tęstinumą nustato kaip didelės rizikos sritį dėl logistinių sutrikimų poveikio, visuomenės sveikatos įvykių ir priklausomybės nuo kritinės infrastruktūros. Remdamiesi šiuo vertinimu, vidaus auditoriai nustato, kad planuojamai užduočiai taikytinas Organizacijos atsparumo Teminis reikalavimas.

Siekdami įvertinti valdyseną, vidaus auditoriai peržiūri valdybos posėdžių protokolus, strateginius planus ir biudžeto dokumentus, kad nustatytų, ar su atsparumu susiję tikslai yra oficialiai nustatyti ir prižiūrimi. Jie įvertina, ar vadovybė periodiškai teikia valdymo organui ataskaitas apie pagrindinius pažeidžiamumus, pavyzdžiui, transporto priklausomybę, infrastruktūros apribojimus ir su sveikata susijusią riziką. Jei nėra vieno bendro atsparumo strategijos dokumento, vidaus auditoriai įvertina, ar atsparumo elementai nuosekliai integruoti į veiklos ir strateginius dokumentus.

Rizikos valdymo požiūriu vidaus auditoriai nagrinėja organizacijos rizikos registrą ir kalbasi su veiklos vadovybe, kad įsitikintų, ar rizikos, galinčios turėti įtakos tiekimo tęstinumui, yra nustatytos, įvertintos ir priskirtos atsakingiems asmenims. Jie vertina, ar ankstesnių įvykių, pavyzdžiui, laikinų uždarymų ar prieigos apribojimų, metu buvo aktyvuoti eskalavimo mechanizmai, ir ar reagavimo veiksmai atitiko nustatytus rizikos tolerancijos parametrus.

Kontrolės procedūros apima veiklos tęstinumo priemonių peržiūrą, periodinių testavimo pratybų įrodymų tikrinimą ir dokumentacijos, susijusios su koordinavimu su valdžios institucijomis veiklą trikdančių įvykių metu, nagrinėjimą. Vidaus auditoriai taip pat peržiūri ataskaitas po incidentų, siekdami nustatyti, ar įgyta patirtis buvo įtraukta į atnaujintus procesus. Kai tam tikri Teminio reikalavimo reikalavimai netaikomi dėl teisinių ar struktūrinių apribojimų, vidaus auditoriai dokumentais pagrindžia netaikymo priežastis pagal Standartus.

2 scenarijus: Tema nustatoma atliekant užduotį.

Visame pasaulyje veikianti profesinių paslaugų įmonė

Atlikdami užduotį, skirtą valdysenai ir įmonės rizikos valdymui, vidaus auditoriai nustato pažeidžiamumus, susijusius su decentralizuotu sprendimų priėmimu, priklausomybe nuo pagrindinių vietos vadovų ir reguliavimo rizika įvairiose jurisdikcijose. Remdamiesi šiais pastebėjimais, vidaus auditoriai nustato, kad užduočiai taikomi tam tikri Organizacijos atsparumo Teminio reikalavimo elementai.

Siekdami įvertinti valdyseną, vidaus auditoriai peržiūri visuotines politikos nuostatas, valdybos ataskaitų medžiagą ir krizių valdymo protokolus, kad nustatytų, ar organizacija yra apibrėžusi, kaip bus tęsiama veikla pasikeitus reglamentavimui, įvykus didelei svarbių darbuotojų kaitai ar vienos jurisdikcijos įvykių, galinčių turėti platesnį poveikį reputacijai, metu. Jie vertina, ar valdymo organas gauna konsoliduotas ataskaitas apie kritines rizikas visose jurisdikcijose ir ar aiškiai apibrėžta atsakomybė už atsparumo priežiūrą.

Rizikos valdymo požiūriu vidaus auditoriai nagrinėja įmonės rizikos sistemą, kad patvirtintų, ar rizika, susijusi su pagrindinių asmenų priklausomybe, tarpvalstybinio reguliavimo reikalavimų laikymusi ir rizika reputacijai, yra susieta su įmonės strateginiais tikslais. Jie atlieka pasirinktų incidentų imties testavimą, siekdami nustatyti, ar informacija apie vietinius įvykius buvo tinkamai eskaluota aukščiausiajai vadovybei ir ar reagavimo sprendimai buvo priimti neviršijant nustatytų įgaliojimų ribų.

Su kontrole susijusios procedūros apima veiklos tęstinumo priemonių peržiūrą įvairiose jurisdikcijose, tikrinimą, ar kritinės funkcijos yra tinkamai padengiamos ir ar yra numatyti atsarginiai darbuotojai arba tinkamai struktūrizuoti pakeičiamumo procesai, taip pat technologinės infrastruktūros, palaikančios koordinuotas nuotolines operacijas, tinkamumo vertinimą. Vidaus auditoriai taip pat peržiūri po įvykių atliktos analizės dokumentaciją, kad patvirtintų, jog buvo įgyvendinti korekciniai veiksmai. Jei taikomi tik tam tikri Teminio reikalavimo reikalavimai, vidaus auditoriai dokumentuoja jų įtraukimo arba neįtraukimo pagrindą.

3 scenarijus: Tema yra prašomos atlikti užduotį

Už ypatingos svarbos nacionalinę infrastruktūrą atsakingas subjektas

Kaimyninėje jurisdikcijoje praūžęs pražūtingas uraganas paskatina valdybos narį paprašyti, kad vidaus audito tarnyba į savo audito planą įtrauktų organizacijos atsparumo užduotį, kuri patvirtintų, ar subjektas yra apsaugotas nuo veiklos pertrūkių, priklausomybės nuo specializuotų rangovų, teisės aktais nustatytų įpareigojimų ir sunkių aplinkosaugos įvykių. Šiuo atveju Organizacijos atsparumo Teminis reikalavimas taikomas visapusiškai.

Siekdami įvertinti valdyseną, vidaus auditoriai peržiūri valdybos patvirtintą strateginį planą ir susijusius dokumentus, kad įsitikintų, jog svarbiausių paslaugų tęstinumas oficialiai įtrauktas į ilgalaikį planavimą. Jie tikrina valdybos ataskaitas, siekdami nustatyti, ar periodiškai peržiūrimi pagrindiniai rodikliai, susiję su veiklos prieinamumu, ypatingos svarbos išteklių priežiūra ir finansiniu nenumatytų atvejų planavimu, įskaitant draudimo apsaugą ir rezervų paskirstymą.

Rizikos valdymo požiūriu vidaus auditoriai vertina, kaip organizacijos rizikos valdymo sistemoje identifikuojamos, vertinamos ir stebimos rizikos, susijusios su infrastruktūros sutrikimais, rangovų koncentracija, atitiktimi teisės aktams ir aplinkos poveikiu. Jie tikrina, ar aiškiai apibrėžta atskaitomybė už šios rizikos stebėseną ir ar ankstesnių paslaugų teikimo sutrikimų metu buvo laikomasi eskalavimo protokolų, įskaitant koordinavimą su reguliavimo institucijomis ir ekstremaliųjų situacijų valdymo institucijomis.

Kontrolės testavimas apima patikrinimą, ar yra parengti veiklos tęstinumo ir veiklos atkūrimo po nelaimės planai ir ar jie periodiškai testuojami, kritinio turto sąrašų peržiūrą, sutartinių susitarimų su alternatyviais paslaugų teikėjais nagrinėjimą bei analizės po incidento dokumentacijos vertinimą, siekiant nustatyti, ar korekciniai veiksmai buvo stebimi ir įgyvendinti. Kai tam tikri reikalavimai netaikomi dėl teisės aktų nuostatų, vidaus auditoriai dokumentuoja pagrindimą pagal Standartus.

C priedas. Susiejimas su sistemomis

Organizacija gali turėti savo organizacinių priemonių, pagrįstų tokiomis sistemomis kaip ISO standartai. Vidaus auditoriai jau gali būti parengę šiomis sistemomis pagrįstas audito programas ir testavimo procedūras. Vidaus auditoriai turėtų suderinti planuojamą organizacijos atsparumo kontrolės priemonių testavimą su Teminiu reikalavimu, kad užtikrintų tinkamą aprėptį (13.4 standartas „Vertinimo kriterijai“). Toliau pateiktoje lentelėje Organizacijos atsparumo Teminis reikalavimas yra susietas su ISO 22336 sistema. Papildomos nuorodos į sistemas pateiktos E priede.

Valdysenos reikalavimai	ISO 22336 sistema
A. Vadovybė parengia organizacinę strategiją, apimančią atsparumą ir kurią prižiūri valdyba. Į ją įtraukiami veiklos, technologiniai ir finansiniai elementai, reikalingi pokyčiams valdyti ir veiklos tęstinumui užtikrinti. Atsparumo tikslai atitinka bendrą organizacijos požiūrį į rizikos valdymą.	4.1; 6.1; 6.2; 7.1; 8.4; 8.5; 9.1; 9.5
B. Naujausia informacija apie atsparumo tikslų įgyvendinimą periodiškai pateikiama valdybai peržiūrėti. Taip užtikrinama, kad atsparumas būtų įtrauktas į strateginę priežiūrą, ilgalaikio planavimo procesus, pakeičiamumo planavimą ir organizacijos kultūrą įskaitant išteklių ir biudžeto sprendimus, reikalingus ypatingos svarbos verslo veiklai palaikyti.	6.4; 8.6; 10.2
C. Parengtos kritinių technologinių ir finansinių procesų politikos ir procedūros yra periodiškai peržiūrimos, testuojamos ir prireikus atnaujinamos, kad būtų sustiprinta kontrolės aplinka.	4.2; 6.3; 8.3; 8.4; 9.4
D. Sukuriama incidentų valdymo struktūra, kuri naudojama organizacijos atsparumo tikslams prižiūrėti ir palaikyti. Ji apima sprendimų priėmimo hierarchiją, komunikacijos ir eskalavimo protokolus bei vadovaujamuosius ir veiklos vaidmenis ir atsakomybę.	5.4
E. Sukurtas procesas, kuriuo periodiškai patvirtinamos atsparumo sėkmei reikalingos kompetencijos ir iš naujo įvertinamos asmenų, atliekančių svarbiausius vaidmenis atsparumo procesuose, kompetencijos.	9.6
F. Nustatomas procesas, kuriuo siekiama užtikrinti, kad visos svarbios vidaus ir išorės suinteresuotosios šalys būtų identifikuotos, prioritetizuotos ir įtrauktos kuriant informacijos ir ataskaitų teikimo struktūras, organizacijos atsparumo tikslams pasiekti. Suinteresuotosios šalys gali būti subjektai, vyresnioji vadovybė, veiklos padaliniai, rizikos valdymas, IT, tiekimo grandinės / pirkimų, patalpų, žmogiškųjų išteklių, finansų, ir teisės, užtikrinimo paslaugų teikėjai (įskaitant vidaus auditą), atitikties ir viešųjų ryšių funkcijos, svarbiausi tiekėjai, klientai, reguliavimo institucijos ir kiti.	9.2; 9.5

Rizikos valdymo reikalavimai	ISO 22336 sistema
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.	4.4; 5; 7.3; 7.4; 7.5, 7.6, 9.2, 9.3
B. Aiškiai apibrėžta atskaitomybė ir atsakomybė už organizacijos atsparumo rizikos valdymą. Paskirtas asmuo arba komanda, kurie reguliariai stebi organizacijos atsparumo rizikos valdymą ir teikia apie jį ataskaitas, įskaitant rizikos mažinimui reikalingus išteklius ir kylančių grėsmių organizacijos atsparumui identifikavimą.	4.3; 8.2; 9.6
C. Nustatytas procesas, skirtas stebėti organizacijos atsparumo rizikos (kylančios ar anksčiau nustatytos) lygius ir greitai eskaluoti tas rizikas, kurios pasiekia organizacijos rizikos valdymo gairėse ir rizikos tolerancijoje arba taikomuose teisiniuose ir reguliavimo reikalavimuose apibrėžtą nepriimtiną lygį. Atsižvelgiama į organizacijos atsparumo rizikos poveikį.	7.2; 7.6; 10.1
D. Vadovybė įdiegė ir periodiškai testuoja reagavimo į krizes, veiklos sutrikimus ir ekstremaliąsias situacijas bei veiklos atkūrimo 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, atsižvelgiant į įvairius tikėtinus trikdžius.	7.2; 7.6; 7.8

Kontrolės procesų reikalavimai	ISO 22336 sistema
A. Įdiegtas procesas, skirtas nustatyti ypatingos svarbos trečiųjų šalių paslaugų teikėjus (tiekėjus ir pardavėjus) ir minimalius atsargų lygius, reikalingus pagrindinėms operacijoms palaikyti. Šis procesas taip pat apima nuolat atnaujinamo alternatyvių tiekėjų sąrašo palaikymą.	7.7
B. Identifikuojami ir klasifikuojami operacijoms svarbūs duomenys. Duomenų klasifikavimas apima nustatymą, kur duomenys saugomi, kam reikalinga prieiga prie jų, kaip jie pasiekiami ir ar daromos jų atsarginės kopijos bei ar juos galima atkurti ekstremalios situacijos metu.	6.1
C. Siekiant sumažinti informacijos saugumo riziką (įskaitant su kibernetiniu saugumu susijusią riziką) ir užtikrinti, kad jautrūs duomenys būtų apsaugoti krizių, veiklos sutrikimų ir ekstremalių situacijų metu, įdiegtos ypatingos svarbos IT kontrolės priemonės ir vykdoma nuolatinė stebėsena. Kontrolė ir nuolatinė stebėsena apima grėsmių žvalgybą realiuoju laiku ir prieigos suteikimą tik įgaliotiems naudotojams.	7.5
D. Inventorizuojamas ypatingos svarbos IT turtas. Turtas apima techninę ir programinę įrangą bei paslaugas, reikalingas operacijoms palaikyti krizių, sutrikimų ir ekstremalių situacijų metu.	9.2

E.	Parengti veiklos tęstinumo ir atkūrimo po nelaimių planai, kuriuose apibrėžtos paskirtų darbuotojų ir atkūrimo komandų funkcijos ir atsakomybės. Planai periodiškai testuojami (pavyzdžiui, „stalo pratybos“), o testavimo rezultatai, įskaitant tobulinimo galimybes, pranešami valdybai ir vyresniajai vadovybei.	8.6; 9.6; 10.3
F.	Nustatytas procesas, skirtas darbo aplinkai pritaikyti krizių, veiklos sutrikimų ir ekstremalių situacijų metu.	9.3
G.	Nustatytas procesas, skirtas nuolat stebėti kylančias grėsmes ir pažeidžiamumus, galinčius paveikti organizacijos atsparumą, ir apie juos pranešti. Šis procesas naudojamas siekiant nustatyti galimybes tobulinti organizacijos atsparumo veiklą, suteikti joms prioritetus ir jas įgyvendinti, įskaitant pranešimų apie pažeidimus teikimo ar informacijos apie riziką rinkimo sistemas.	7.6
H.	Nustatytas darbuotojų švietimo ir mokymo apie organizacijos atsparumą procesas, užtikrinantis, kad jie žinotų politiką ir procedūras, kurių reikia laikytis, ir veiksmus, kurių reikia imtis įvykus krizėms, sutrikimams ir ekstremalioms situacijoms. Šis procesas apima mokymo pratybas, kurių metu imituojami trikdžių scenarijai.	10.2; 10.3
I.	Nustatytas procesas, kuriuo užtikrinama, kad būtini veiklos, žmogiškieji, technologiniai ir finansiniai ištekliai būtų numatyti biudžete ir prieinami krizių, veiklos sutrikimų ir ekstremaliųjų situacijų metu. Finansiniai ištekliai, reikalingi organizacijos atsparumui palaikyti, periodiškai analizuojami ir apie juos pranešama valdybai.	6.4; 7.6; 9.6
J.	Nustatytas procesas, pagal kurį po krizių, veiklos sutrikimų ir ekstremaliųjų situacijų atliekamos peržiūros, o peržiūrų po incidentų rezultatai analizuojami taikant įgytos patirties procesą, įskaitant šios patirties integravimą į būsimą organizacijos atsparumo planavimą.	10.2, 10.3

D priedas. Papildoma atitikties dokumentavimo forma

Tikimasi, kad vidaus auditoriai, remdamiesi rizikos vertinimu, profesiniu vertinimu nustatys reikalavimų taikymą ir tinkamai dokumentuos tam tikrų reikalavimų netaikymą. Teminis reikalavimas gali būti dokumentuojamas vidaus audito plane arba užduoties darbo dokumentuose, remiantis auditoriaus profesiniu vertinimu. Reikalavimus gali apimti viena ar kelios vidaus audito užduotys. Be to, gali būti taikomi ne visi reikalavimai. Ši forma yra viena iš galimybių dokumentuoti atitiktį Organizacijos atsparumo Teminiam reikalavimui, tačiau jos naudojimas nėra privalomas.

Organizacijos atsparumas – valdysena

Reikalavimas	Įvykdyta aprėptis arba netaikymo pagrindimas	Nuoroda į dokumentus
A. Vadovybė parengia organizacijos strategiją, kurioje atsižvelgiama į organizacijos atsparumą ir kurią prižiūri valdyba; strategija apima veiklos, technologinius ir finansinius elementus, reikalingus pokyčiams valdyti ir veiklai tęsti. Atsparumo tikslai atitinka bendrą organizacijos požiūrį į rizikos valdymą.		
B. Valdybai periodiškai teikiama peržiūrėti atnaujinta informacija apie atsparumo tikslų įgyvendinimą. Taip užtikrinama, kad atsparumas būtų integruotas į strateginę priežiūrą, ilgalaikio planavimo procesus, pakeičiamumo planavimą ir organizacijos kultūrą įskaitant išteklių ir biudžeto aspektus, reikalingus kritinei verslo veiklai palaikyti.		
C. Nustatytos ypatingos svarbos veiklos, technologinių ir finansinių procesų politikos ir procedūros, kurios periodiškai peržiūrimos, testuojamos ir prireikus atnaujinamos, kad būtų sustiprinta kontrolės aplinka.		

D.	Sukuriama incidentų valdymo struktūra, kuri naudojama organizacijos atsparumo tikslams prižiūrėti ir palaikyti. Ji apima sprendimų priėmimo hierarchiją, komunikacijos ir eskalavimo protokolus bei vadovaujamuosius ir veiklos vaidmenis ir atsakomybę.		
E.	Nustatomas procesas, kuriuo periodiškai patvirtinamos atsparumo sėkmei reikalingos kompetencijos ir iš naujo įvertinamos asmenų, atliekančių svarbiausius vaidmenis atsparumo procesuose, kompetencijos.		
F.	Nustatomas procesas, kuriuo užtikrinama, kad visos svarbiausios vidaus ir išorinės suinteresuotosios šalys būtų nustatytos, joms būtų suteikti prioritetai ir jos būtų įtrauktos į informacijos ir ataskaitų teikimo struktūrų kūrimą organizacijos atsparumo tikslams pasiekti. Suinteresuotosios šalys gali būti vyresnioji vadovybė, veiklos padaliniai, rizikos valdymo, IT, tiekimo grandinės ir (arba) pirkimų, ūkio, žmogiškųjų išteklių, finansų ir teisės padaliniai, užtikrinimo paslaugų teikėjai (įskaitant vidaus auditą), atitikties ir viešųjų ryšių tiekėjai, svarbiausi tiekėjai, klientai, reguliavimo institucijos ir kiti.		

Organizacijos atsparumas – rizikos valdymas

Reikalavimas	Įvykdyta aprėptis arba netaikymo pagrindimas	Nuoroda į dokumentus
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. Paskirtas asmuo arba komanda, kurie reguliariai stebi organizacijos atsparumo rizikos valdymą ir teikia apie jį ataskaitas, įskaitant išteklius, reikalingus rizikai mažinti, ir kylančių grėsmių organizacijos atsparumui nustatymą.		

C.	Nustatytas procesas, skirtas stebėti organizacijos atsparumo rizikos (kylančios ar anksčiau nustatytos) lygius ir greitai eskaluoti riziką, kuri pasiekia lygį, laikomą nepriimtinu, kaip apibrėžta organizacijos nustatytose rizikos valdymo gairėse ir rizikos tolerancijoje arba taikomuose teisiniuose ir reguliavimo reikalavimuose. Atsižvelgiama į organizacijos atsparumo rizikos poveikį.		
D.	Vadovybė įdiegė ir periodiškai testuoja reagavimo į krizes, veiklos sutrikimus bei ekstremaliąsias situacijas ir 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, atsižvelgiant į įvairius trikdančius įvykius.		

Organizacijos atsparumas – kontrolė

Reikalavimas	Įvykdyta aprėptis arba netaikymo pagrindimas	Nuoroda į dokumentus
A. Įdiegtas procesas, skirtas nustatyti ypatingos svarbos trečiųjų šalių paslaugų teikėjus (tiekėjus ir pardavėjus) ir minimalius atsargų lygius, reikalingus esminei veiklai palaikyti. Šis procesas taip pat apima nuolat atnaujinamo alternatyvių tiekėjų sąrašo tvarkymą.		
B. Nustatomi ir klasifikuojami veiklai ypač svarbūs duomenys. Duomenų klasifikavimas apima nustatymą, kur duomenys saugomi, kam reikalinga prieiga prie jų, kaip jie pasiekiami ir ar daromos jų atsarginės kopijos bei ar juos galima atkurti ekstremaliosios situacijos metu.		
C. Siekiant sumažinti informacijos saugumo riziką (įskaitant su kibernetiniu saugumu susijusią riziką) ir užtikrinti, kad jautrūs duomenys būtų apsaugoti krizių, veiklos sutrikimų ir ekstremaliųjų situacijų metu, įdiegtos ypatingos svarbos IT kontrolės priemonės ir vykdoma nuolatinė stebėsena. Kontrolės priemonės ir nuolatinė stebėsena apima grėsmių žvalgybą realiuoju laiku ir prieigos suteikimą tik įgaliotiems naudotojams.		

D.	Inventorizuojamas ypatingos svarbos IT turtas. Turtas apima techninę ir programinę įrangą bei paslaugas, reikalingas veiklai palaikyti krizių, sutrikimų ir nepaprastųjų situacijų metu		
E.	Parengti veiklos tęstinumo ir veiklos atkūrimo po nelaimių planai, kuriuose apibrėžtos paskirtų darbuotojų ir atkūrimo komandų funkcijos. Planai periodiškai testuojami (pavyzdžiui, „stalo pratybos“), o testavimo rezultatai, įskaitant tobulinimo galimybes, pranešami valdybai ir vyresniajai vadovybei.		
F.	Nustatytas procesas, skirtas darbo aplinkai pritaikyti krizių, sutrikimų ir ekstremalių situacijų metu.		
G.	Nustatytas procesas, skirtas nuolat stebėti kylančias grėsmes ir pažeidžiamumus, kurie gali turėti įtakos organizacijos atsparumui, ir apie juos pranešti. Šis procesas naudojamas siekiant nustatyti galimybes tobulinti organizacijos atsparumo veiklą, suteikti joms prioritetus ir jas įgyvendinti, įskaitant pranešimų apie pažeidimus teikimo ar informacijos apie riziką rinkimo sistemas.		
H.	Nustatytas darbuotojų švietimo ir mokymo organizacijos atsparumo klausimais procesas, kuriuo užtikrinama, kad jie žinotų, kokių politikų ir procedūrų reikia laikytis ir kokių veiksmų imtis kilus krizėms, veiklos sutrikimams ir ekstremaliosioms situacijoms. Šis procesas apima mokymo pratybas, kurių metu imituojami trikdžių scenarijai.		
I.	Nustatytas procesas, kuriuo užtikrinama, kad būtini veiklos, žmogiškieji, technologiniai ir finansiniai ištekliai būtų numatyti biudžete ir prieinami krizių, veiklos sutrikimų ir ekstremaliųjų situacijų metu. Finansiniai ištekliai, reikalingi organizacijos atsparumui palaikyti, periodiškai analizuojami ir apie juos pranešama valdybai.		
J.	Nustatytas procesas, pagal kurį įvykusios krizės, veiklos sutrikimai ir ekstremaliosios situacijos yra peržiūrimi, o peržiūrų po incidentų rezultatai analizuojami taikant įgytos patirties procesą, įskaitant patirties integravimą į būsimą organizacijos atsparumo planavimą.		

E priedas. Papildomos nuorodos į sistemas

Sritis	ISO nuoroda	Apimtis ir (arba) straipsnių
VALDYSENA	ISO 22316:2017	Politika ir strategija; vadovybės įsipareigojimas; bendra vizija; kultūra; bendravimas; nuolatinis tobulėjimas.
Rizikos valdymas	ISO 31000:2018	Apimtis / kontekstas / kriterijai; rizikos vertinimas; valdymo priemonės; stebėsena; komunikacija.
Verslo tęstinumo ir (arba) atkūrimo po nelaimės pagrindai	ISO 22301: 2019; ISO/TS 22317:2021	BCMS kontekstas, lyderystė, planavimas, veikla; BIA veiklos ir rezultatai.
Tiekimo grandinės atsparumas	ISO/TS 22318:2021	Tiekėjų priklausomybės analizė; tęstinumo strategijos; alternatyvos; užtikrinimo reikalavimai.
Informacinių ir ryšių technologijų parengtis	ISO/IEC 27031	IRT tęstinumas; atkūrimo tikslai; testavimas ir tobulinimas; suderinamumas su BCMS.

Apie Vidaus auditorių institutą

VAI yra tarptautinė profesinė asociacija, vienijanti daugiau nei 265 000 narių visame pasaulyje ir suteikusi daugiau nei 200 000 sertifikuotų vidaus auditorių (CIA®) sertifikatų visame pasaulyje. Įkurtas 1941 m., VAI visame pasaulyje pripažįstamas kaip vidaus audito profesijos lyderis standartų, sertifikavimo, švietimo, mokslinių tyrimų ir techninių rekomendacijų srityje. Jei norite gauti daugiau informacijos, apsilankykite theiia.org.

Atsakomybės apribojimas

VAI šį dokumentą skelbia informaciniais ir švietimo tikslais. Šia medžiaga nesiekiama pateikti galutinių atsakymų dėl konkrečių individualių aplinkybių, todėl ji skirta naudoti tik kaip gairės. VAI rekomenduoja kreiptis į nepriklausomus ekspertus dėl konsultacijų, tiesiogiai susijusių su konkrečia situacija. VAI neprisiima jokios atsakomybės už asmenis, kurie remiasi šia medžiaga.

Autorių teisės

2026 m. balandžio mėn.

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