Kibernetinis saugumas

Topical Requirement

Teminis reikalavimas

Naudotojo vadovas

The Institute of
Internal Auditors

Turinys

Teminių reikalavimų apžvalga

Teminiai reikalavimai yra esminė Tarptautinės profesinės praktikos sistemos (Professional Practices Framework®) sudedamoji dalis kartu su Pasauliniais vidaus audito standartais (Global Internal Audit Standards™) ir Pasaulinėmis gairėmis. Vidaus auditorių institutas reikalauja, kad Teminiai reikalavimai būtų naudojami kartu su Pasauliniais vidaus audito standartais, kurie yra autoritetingas reikalaujamos praktikos pagrindas. Šiame vadove pateikiamos nuorodos į Standartus kaip išsamesnės informacijos šaltinį.

Teminiai reikalavimai apibrėžia, kaip vidaus auditoriai sprendžia dažniausiai pasitaikančias rizikos sritis, kad būtų skatinama kokybė ir nuoseklumas profesijoje. Teminiai reikalavimai nustato pagrindą 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. Teminiai reikalavimai nėra skirti visiems galimiems aspektams, į kuriuos reikėtų atsižvelgti atliekant užtikrinimo paslaugas; veikiau jie skirti pateikti minimalų reikalavimų rinkinį, kad būtų galima nuosekliai ir patikimai įvertinti temą.

Teminiai reikalavimai aiškiai susieti su 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 siejamas su valdyba / valdymo organu, rizikos valdymas - su antrąja linija, o kontrolė arba kontrolės procesai - su pirmąja linija. Nors vadovybei atstovaujama ir pirmoje, ir antroje linijoje, vidaus audito funkcija vaizduojama trečioje linijoje kaip nepriklausomas ir objektyvus patikinimo teikėjas, atskaitingas valdybai / 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 per rizika pagrįsto vidaus audito planavimo procesą 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, ir į ją įtraukiama tema, privaloma įvertinti teminio reikalavimo taikymą.

Taikant teminį reikalavimą svarbiausias vaidmuo tenka profesiniam sprendimui. Rizikos vertinimai lemia vidaus audito vadovų sprendimus dėl to, kokias užduotis įtraukti į vidaus audito planą (9.4 standartas "Vidaus audito planas"). Be to, vidaus auditoriai, remdamiesi profesiniu sprendimu, nustato, kokie aspektai bus nagrinėjami kiekvienoje užduotyje (13.3 standartas "Užduoties tikslai ir apimtis", 13.4 standartas "Vertinimo kriterijai" ir 13.6 standartas "Darbo programa"). A priede "Praktinio taikymo pavyzdžiai" aprašyta, kaip vidaus auditoriai nustato, ar taikomas teminis reikalavimas.

Privaloma išsaugoti įrodymus, kad buvo įvertintas kiekvienas teminis reikalavimas , įskaitant pagrindimą, paaiškinantį, kodėl kuris nors reikalavimas buvo atmestas. Atitiktis teminiam reikalavimui privalo būti dokumentuojama remiantis auditoriaus profesiniu sprendimu, kaip aprašyta 14.6 standarte "Užduoties dokumentai".

Nors kibernetinio saugumo teminiame reikalavime pateikiami pagrindiniai kontrolės procesai, į kuriuos reikia atsižvelgti, organizacijoms, kurios kibernetinę riziką vertina kaip labai didelę, gali tekti įvertinti papildomus aspektus.

Jei vidaus audito vadovas nustato, kad vidaus audito tarnyba neturi reikiamų žinių, kad galėtų atlikti audito užduotį teminio reikalavimo tema, užduočiai atlikti gali užsakyti išorės auditorių paslaugas (3.1 standartas "Kompetencija", 7.2 standartas "Vidaus audito vadovo kvalifikacija", 10.2 standartas "Žmogiškųjų išteklių valdymas"). Net ir tokiu atveju užsakomosios užduotys neatleidžia vidaus audito funkcijos nuo atsakomybės už atitiktį teminiams reikalavimams. Galutinę atsakomybę už atitikties užtikrinimą ir toliau prisiima vidaus audito vadovas. Be to, jei vidaus audito vadovas nustato, kad vidaus audito išteklių nepakanka, jis privalo informuoti valdybą apie nepakankamų išteklių poveikį ir apie tai, kaip bus sprendžiamas išteklių trūkumo klausimas (8.2 standartas "Ištekliai").

Veikimas, dokumentavimas ir ataskaitų teikimas

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

Teminio reikalavimo aprėptis gali būti dokumentuojama vidaus audito plane arba užduoties dokumentuose, remiantis auditorių profesiniu sprendimu. Reikalavimus gali apimti viena ar kelios vidaus audito užduotys. Be to, gali būti taikomi ne visi reikalavimai. Privaloma išsaugoti įrodymus, kad buvo įvertintas teminis reikalavimas , įskaitant bet kokias išimtis paaiškinantį pagrindimą.

C priede pateiktą neprivalomą priemonę galima naudoti kaip nuorodą ir dokumentuoti vidaus auditorių atliekamą darbą.

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"). Apie rezultatus turi būti pranešama valdybai ir vyresniajai vadovybei. Pranešimuose privalo būti pateikiama informacija apie vidaus audito funkcijos atitiktį Standartams ir veiklos tikslų pasiekimą.

Atitiktis teminiams reikalavimams bus vertinama atliekant kokybės vertinimą. Ruošdamiesi kokybės vertinimui, vidaus auditoriai gali naudotis C priede pateikta priemone.

Kibernetinis saugumas

Kibernetinis saugumas yra plati tema, susijusi su daugeliu technologinių bet kurios organizacijos aspektų. Be informacinių technologijų, kibernetinis saugumas paprastai yra verslo procesų dalis, todėl vidaus auditoriai, planuodami, nustatydami apimtį ir atlikdami užtikrinimo užduotis, turi įvertinti su kibernetiniu saugumu susijusią riziką.

Nacionalinis standartų ir technologijų institutas (NIST), priklausantis JAV prekybos departamentui, kibernetinį saugumą apibrėžia tiesiog kaip: "Gebėjimą apsaugoti arba apginti kibernetinės erdvės naudojimą nuo kibernetinių atakų". Kibernetinio saugumo teminiame reikalavime daugiausia dėmesio skiriama išoriniam perimetrui, kurį organizacijos apsaugo, kad sumažintų riziką, kylančią dėl neįgaliotų naudotojų ir kenkėjiškų kibernetinių grėsmių. Kibernetinis saugumas yra visa apimančio informacijos saugumo pogrupis, kurį NIST apibrėžia kaip "Informacijos ir informacinių sistemų apsaugą nuo neteisėtos prieigos, naudojimo, atskleidimo, sutrikdymo, pakeitimo ar sunaikinimo, siekiant užtikrinti konfidencialumą, vientisumą ir prieinamumą".

Kibernetinio saugumo teminiai reikalavimai:

- Valdysena - aiškiai apibrėžti baziniai kibernetinio saugumo tikslai ir strategijos, kuriais remiami organizacijos tikslai, politika ir procedūros.
- Rizikos valdymas - kibernetinių grėsmių nustatymo, analizės, valdymo ir stebėsenos procesai, įskaitant skubaus kibernetinės rizikos eskalavimo procesą.
- Kontrolė - vadovybės nustatyti, periodiškai vertinami kontrolės procesai, skirti kibernetinei rizikai mažinti.

Aspektai

Vidaus auditoriai, norėdami lengviau įvertinti kibernetinio saugumo teminius reikalavimus, gali remtis toliau nurodytais argumentais. Šie aspektai, kuriuose pateikiamos nuorodos į reikalavimus, yra pavyzdiniai, bet neprivalomi. Nustatydami, ką įtraukti į savo vertinimus, vidaus auditoriai turi remtis profesiniu sprendimu.

Valdysenos aspektai

Siekdami įvertinti, kaip valdysenos procesai taikomi kibernetinio saugumo tikslams, vidaus auditoriai gali peržiūrėti:

A. formalizuotas, dokumentais pagrįstas kibernetinio saugumo strateginis planas ir tikslai, įskaitant įrodymus, kad valdyba periodiškai (paprastai kas ketvirtį) peržiūri informacijos saugumo funkcijos vadovo, pavyzdžiui, vyriausiojo informacijos saugumo pareigūno (CISO), pateiktus atnaujintus kibernetinio saugumo duomenis. Įrodymai gali apimti ataskaitas apie:
   - Strateginių tikslų pasiekimo stebėsena.
   - Biudžeto poreikiai kibernetinio saugumo tikslams ir uždaviniams įgyvendinti.
   - Dėmesys rizikos veiksniams ir vidaus kontrolei, įskaitant gerinimo pažangą.
   - Pagrindiniai veiklos rodikliai (KPI) nustatytų tikslų pasiekimui matuoti.
   - Žmogiškieji ištekliai, reikalingi kibernetinio saugumo darbuotojams samdyti, mokyti ir ugdyti.

B. Politika, procedūros ir kiti susiję dokumentai, naudojami kibernetinio saugumo procesams valdyti, įskaitant:
   - Politika bent kartą per metus peržiūrima ir atnaujinama . Dėl kylančios kibernetinės rizikos gali prireikti peržiūrėti ir atnaujinti dažniau.
   - Procesas, skirtas nustatyti, ar politika ir procedūros yra pakankamos kibernetinio saugumo operacijoms palaikyti.
   - Plačiai priimtinos gairės (NIST, COBIT ir kt.), skirtos kibernetinio saugumo procesams ir vidaus kontrolei stiprinti.

C. Vaidmenys ir pareigos, padedantys siekti kibernetinio saugumo tikslų, įskaitant struktūrą, užtikrinančią, kad kibernetinio saugumo funkcija būtų pavaldi tokiam organizacijos lygmeniui, kuris yra pakankamai matomas, kad būtų pasiektas organizacinis palaikymas.
   - Procesas, skirtas periodiškai vertinti kibernetinio saugumo funkcijas atliekančių darbuotojų žinias, įgūdžius ir gebėjimus.

D. Įrodymai, kad bendradarbiaujama su atitinkamomis suinteresuotosiomis šalimis (pavyzdžiui, aukščiausiaja vadovybe, operacijų, rizikos valdymo, žmogiškųjų išteklių, teisės, atitikties užtikrinimo, strateginių pardavėjų ir kitais subjektais), įskaitant informavimą apie esamą ir kylančią kibernetinę riziką ir žinomas galimas

pažeidžiamumo vietas. Bendravimo įrodymai gali būti susitikimų protokolai, ataskaitos arba el. laiškai.

Rizikos valdymo aspektai

Siekdami įvertinti, kaip rizikos valdymo procesai taikomi kibernetinio saugumo tikslams, vidaus auditoriai gali peržiūrėti:

A. Kaip organizacija vertina ir valdo kibernetinio saugumo riziką, įskaitant tai, kaip vertinamos grėsmės ir pažeidžiamumai:
   - Pirmiausiai nustatoma ir pranešama.
   - Analizuojama siekiant įvertinti riziką organizacijos tikslams pasiekti.
   - Mažinama, įskaitant veiksmų planus, skirtus rizikai sumažinti iki priimtino lygio.
   - Stebima, įskaitant nuolatinio ataskaitų teikimo planą, kol grėsmės bus visiškai pašalintos.

B. Kaip organizacija periodiškai gauna informaciją apie kibernetinio saugumo rizikos valdymą iš funkcinių sričių, pavyzdžiui, informacinių technologijų, įmonės rizikos valdymo, žmogiškųjų išteklių, teisės, atitikties, veiklos, apskaitos ir finansų. Informacijai gauti gali būti naudojama tarpfunkcinė kibernetinio saugumo grupė arba IT valdymo komitetas.

C. Kaip organizacija paskyrė atskaitomybę ir atsakomybę už kibernetinio saugumo rizikos valdymą asmeniui ar komandai.
   - Atsakingas (-i) asmuo (-enys) turi periodiškai (kas ketvirtį, kas mėnesį arba pagal poreikį) informuoti visą organizaciją apie nuolat atnaujinamą kibernetinio saugumo rizikos informaciją, taip pat gali nurodyti išteklių poreikį rizikos mažinimo strategijoms.

D. Kibernetinio saugumo rizikos eskalavimo procesai, įskaitant tai, kaip vertinamas, priskiriamas grėsmės ar rizikos lygis ir nustatomi prioritetai. Peržiūra gali apimti nustatymą:
   - Organizacijos nustatyti rizikos lygiai, pavyzdžiui, didelis, vidutinis ir mažas, su išsamiais kiekvieno rizikos lygio paaiškinimais ir kiekvienos rizikos kategorijos eskalavimo procedūromis.
   - Šiuo metu nustatytų kibernetinio saugumo rizikų sąrašas ir kiekvieno rizikos įvykio mažinimo būklė.
   - Taikomi teisiniai, reguliavimo ir atitikties reikalavimai.
   - Finansinės ir nefinansinės (pvz., reputacijos) rizikos poveikis.

E. Vadovybės ir darbuotojų informavimo apie kibernetinio saugumo riziką procesas, kuris apima:

- Periodiniai (bent kartą per metus) darbuotojų kibernetinio saugumo mokymai, pvz., iš anksto nepraneštos imituojamos sukčiavimo kampanijos, kad būtų galima patikrinti ir stebėti organizacijos informuotumą.
- Atnaujinta informacija apie esamų kibernetinio saugumo problemų šalinimą, nurodant numatomas užbaigimo datas.
- Neatitikimų stebėsena, įskaitant valdybai ir vyresniajai vadovybei teikiamus atnaujintus duomenis.
- Pakartotinis grėsmių vertinimas, kai pasikeičia organizacijos rizikos apetitas ir rizikos tolerancija.

F. Procesai, kuriuos organizacija įgyvendino reagavimo į incidentus ir atkūrimo srityje, įskaitant:

- Dokumentuotas planas, kuris peržiūrimas ir atnaujinamas laikui bėgant keičiantis organizacijos veiklai. Į planą turi būti įtraukta:
  - Kaip nustatomi incidentai ir apie juos pranešama.
  - Kaip incidentai užkardomi, kad būtų išvengta tolesnės žalos.
  - Kaip organizacija atsigaus ir reaguos, kad atnaujintų veiklą.
  - Kaip incidentas bus analizuojamas, kad būtų galima nustatyti, ko išmokta ir kaip išvengti panašių įvykių ateityje.
- Periodiškas (bent kartą per metus) testavimas (stalo pratybos) ir rezultatų pateikimas aukščiausiajai vadovybei bei atitinkamoms suinteresuotosioms šalims. Atlikus testavimą gali būti parengti veiksmų planai.

Kontrolės proceso aspektai

Siekdami įvertinti, kaip kontrolės procesai taikomi kibernetinio saugumo tikslams, vidaus auditoriai gali peržiūrėti:

A. Vadovybės požiūris į veiksmingos kibernetinio saugumo vidaus kontrolės aplinkos kūrimą, įskaitant:
- Vidaus kontrolės priemonių, reikalingų padidėjusiai rizikai sumažinti ir jautriems, svarbiems, asmens ar konfidencialiems duomenims apsaugoti, vertinimas ir įgyvendinimas, remiantis organizacijos rizikos vertinimo procesu.
- Išteklių poreikio pagrindinėms kibernetinio saugumo kontrolės priemonėms palaikyti nustatymas.
- Atsižvelgimas į tiekėjų kontrolės priemones kaip į kontrolės aplinkos dalį, įskaitant tiekėjų paslaugų organizacijos kontrolės (SOC) ataskaitų peržiūrą prieš pradedant verslo santykius ir per visą santykių laikotarpį.
- Periodiškai tikrinama, ar kibernetinio saugumo kontrolės priemonės veikia taip, kad sumažintų riziką ir padėtų siekti kibernetinio saugumo tikslų.

- Vidaus kontrolės trūkumų šalinimo procesas arba vidaus audito funkcijos ar kitų užtikrinimo teikėjų atliktų vertinimų (pvz., įsibrovimo testų) išvadų nagrinėjimas.

B. Organizacijos talentų valdymo procesas, skirtas kibernetinio saugumo specialistų įdarbinimui ir mokymui, įskaitant tai, kaip organizacija nustato galimybes didinti kibernetinio saugumo specialistų gebėjimus, kad jie galėtų palaikyti technines žinias ir gerinti organizacijos informuotumą apie kylančias problemas.
   - Pavyzdžiai - dalyvavimas mokymuose, dalyvavimas dalijimosi žiniomis grupėse ir tęstinis profesinis mokymas, įskaitant su kibernetine sritimi susijusių sertifikatų įgijimą.

C. Vadovybės procesas, skirtas nuolat nustatyti, prioretizuoti, stebėti ir pranešti apie kylančias kibernetinio saugumo grėsmes ir pažeidžiamumą, kuris yra orientuotas į kasdienę veiklą. Peržiūra gali apimti tai, ar yra nustatyti procesai, skirti grėsmėms ir pažeidžiamumams, susijusiems su naujomis ar atsirandančiomis technologijomis, pavyzdžiui, dirbtinio intelekto naudojimu, vertinti.

D. Vadovybės procesai ir kontrolės priemonės, nustatytos IT turtui valdyti ir apsaugoti per visą jo gyvavimo ciklą, įskaitant techninės ir programinės įrangos bei pardavėjų paslaugų atranką, naudojimą, priežiūrą ir eksploatavimo nutraukimą. Į techninę įrangą įeina serveriai, tinklo įranga (pvz., maršrutizatoriai ar saugasienės), staliniai kompiuteriai, nešiojamieji kompiuteriai, mobilieji telefonai, planšetiniai kompiuteriai ir periferiniai įrenginiai. Programinė įranga apima operacines sistemas (pvz., "Windows"), įmonių išteklių planavimo programinę įrangą, taikomąsias programas, antivirusines programas ir kt. Techninė ir programinė įranga gali būti tokia:
   - Organizacijos naudojamas šifravimas, antivirusinė programinė įranga, mobiliųjų įrenginių valdymas, sudėtingi slaptažodžių reikalavimai, virtualaus privataus tinklo (VPN) / nulinio pasitikėjimo tinklo (ZTN) autentifikavimas ir periodiškas programinės įrangos atnaujinimas.
   - Turto valdymo procesas, kuriuo užtikrinama, kad suteikiant įmonės išduodamą techninę įrangą būtų nustatyta tinkama saugumo konfigūracija, o turtą nurašant - tinkamai sunaikinama.
   - Su duomenų bazėmis susijusios kontrolės priemonės, kurios apima naudotojų ir administratorių prieigos ribojimą, šifravimo naudojimo užtikrinimą, atsarginių duomenų bazių kopijų darymą ir testavimą bei griežtą tinklo saugumo kontrolę.
   - Kaip į kibernetinio saugumo grėsmes ar pažeidžiamumus atsižvelgiama sistemos kūrimo gyvavimo cikle (SDLC).
   - Kūrimo, saugumo ir operacijų (DevSecOps) metodas, taikomas siekiant užtikrinti, kad į programinės įrangos kūrimo procesą būtų įtrauktas kibernetinis saugumas, kad būtų galima aktyviai nustatyti pažeidžiamumus.

E. Kibernetiniam saugumui stiprinti taikomi procesai, įskaitant:
   - Saugumo nustatymų konfigūravimas siekiant sumažinti kibernetinio saugumo riziką.

- Mobiliųjų įrenginių administravimas (įskaitant el. pašto ir programų naudojimą) yra sukonfigūruotas taip, kad būtų sumažinta kibernetinio saugumo rizika ir būtų galima nuotoliniu būdu valdyti, jei naudotojo įrenginys būtų pažeistas.
- Šifravimo naudojimas "ramybės būsenoje" esantiems duomenims, pavyzdžiui, kietajame diske saugomai informacijai, arba "perduodamiems" duomenims, pavyzdžiui, elektroniniams laiškams šifruoti.
- Serverių ar programinės įrangos (pvz., operacinės sistemos) atnaujinimas naudojant naujausias saugumo versijas.
- Naudotojo prieigos valdymas, pvz., daugiafaktorinis autentiškumo patvirtinimas (MFA) ir unikalūs naudotojo ID su sudėtingais slaptažodžiais, kurių galiojimas periodiškai baigiasi.
- Įdiegtos stebėsenos kontrolės priemonės, skirtos nustatyti, ar prieinamumas ir išteklių naudojimas veikia tinkamai, leidžiančios peržiūrėti ir analizuoti galimas kibernetinio saugumo problemas, keliančias grėsmę veiklos rezultatams.
- Kibernetinio saugumo integravimas į SDLC, siekiant nustatyti ir pašalinti kibernetinio saugumo spragas prieš perkeliant į produkciją programinę įrangą.

F. Su tinklu susijusios kontrolės priemonės, užtikrinančios organizacijos perimetro apsaugą, įskaitant tai, kaip organizacija naudoja:
   - Tinklo segmentavimas.
   - Saugasienės.
   - Naudotojo prieigos kontrolė.
   - Išorinių ir vidinių jungčių apribojimai.
   - Daiktų interneto (IoT) kontrolė, susijusi su tarpusavyje sujungtais tinklais.
   - Įsilaužimo aptikimo ir (arba) prevencijos sistemos, skirtos užkirsti kelią kibernetinio saugumo atakoms, jas aptikti ir atkurti.

G. Galinių įrenginių ir komunikacijos saugumo kontrolės priemonės, taikomos tokioms paslaugoms kaip el. paštas, interneto naršyklės, vaizdo konferencijos, pranešimų siuntimas ("Zoom", "MS Teams" ir kt.), socialinė žiniasklaida, debesys ir dalijimosi failais protokolai. Kontrolės priemonės gali apimti tam tikrų failų plėtinių (pvz., .exe failų) naudojimo apribojimą ir daugiafaktorinį autentiškumo patvirtinimą dalijantis failais.

A priedas. Praktinio taikymo pavyzdžiai

Toliau pateiktuose pavyzdžiuose aprašyti scenarijai, kai būtų taikomas kibernetinio saugumo teminis reikalavimas:

1 pavyzdys: Kibernetinis saugumas nustatytas vidaus audito užduočiai, įtrauktai į vidaus audito planą.

Kai vidaus audito funkcija užbaigia rizika pagrįstą planavimo procesą ir į vidaus audito planą įtraukia vieną ar daugiau kibernetinio saugumo užduočių, atliekant tokias užduotis privaloma laikytis teminio reikalavimo. Atitiktis gali būti pasiekta į vidaus audito planą įtraukiant vieną ar daugiau užduočių.

Kibernetinis saugumas yra plati tema, todėl ne kiekvienas teminis reikalavimas gali būti taikomas kiekvienai užduočiai. Kai vidaus auditoriai taiko profesinį sprendimą ir nustato, kad vienas ar daugiau kibernetinio saugumo teminių reikalavimų nėra taikytini ir todėl turi būti neįtraukti į užduotį, vidaus auditoriai privalo dokumentuoti ir išsaugoti šių reikalavimų neįtraukimo pagrindimą. Pavyzdžiui, kai kurių reikalavimų netaikymo pagrindimas gali būti toks, kad vidaus audito tarnyba rotacijos principu atlieka įvairias kibernetinio saugumo užduotis arba nustatė, kad rizikos reikšmė užduotyje yra maža.

2 pavyzdys: Kibernetinio saugumo rizika nustatoma atliekant audito užduotį, kuri nėra orientuota į kibernetinį saugumą.

Vidaus auditoriai gali nustatyti kibernetinio saugumo riziką vertindami procesą, tiesiogiai nesusijusį su kibernetiniu saugumu. Pavyzdžiui, vidaus auditoriai gali vertinti atsiskaitymų su kreditoriais procesą užduoties, nesusijusios su kibernetiniu saugumu, metu ir planuodami užduotį nenustatyti, kad kibernetinio saugumo rizika patenka į jos apimtį. Tačiau atlikę pradinį patikrinimą vidaus auditoriai nustato, kad tokia rizika turi būti įtraukta į užduoties apimtį; pavyzdžiui, jie nustato kibernetinio saugumo riziką, susijusią su internetiniu būdu teikiamu pirminiu pirkimo užsakymo prašymu (13.2 standartas "Užduoties rizikos vertinimas").

Nustačius atitinkamą riziką, vidaus auditoriai privalo peržiūrėti kibernetinio saugumo teminį reikalavimą ir nustatyti, kurie reikalavimai yra taikytini. Šiame pavyzdyje jie gali neįtraukti kibernetinio saugumo valdymo proceso arba kibernetinio saugumo rizikos valdymo proceso. Užduoties darbo dokumentuose jie privalo dokumentais pagrįsti, kodėl neįtraukė kitų kibernetinio saugumo teminių reikalavimų, ir išsaugoti dokumentus.

3 pavyzdys: Prašoma atlikti kibernetinio saugumo užduotį, kuri iš pradžių nebuvo įtraukta į vidaus audito planą.

Suinteresuotoji šalis, pavyzdžiui, valdyba, vadovybė arba reguliavimo institucija, gali paprašyti vidaus auditorių atlikti kibernetinio saugumo vertinimus, kurie neįtraukti į pradinį audito planą. Pavyzdžiui, kai organizacijos tampa kibernetinės atakos taikiniu, valdyba gali paprašyti vidaus audito įvertinti kibernetinio saugumo kontrolės priemones. Taikomas teminis reikalavimas, reikalavimai privalo būti įvertinti, o visos išimtys dokumentuotos.

B priedas. Susiejimas su sistemomis

Organizacija gali pati imtis kibernetinio saugumo priemonių, naudodama rizikos valdymo ir valdymo gairėmis kaip COBIT ar NIST. Vidaus auditoriai jau gali būti parengę audito programas ir testavimo procedūras, paremtas šiomis sistemomis. Siekdami užtikrinti tinkamą aprėptį, vidaus auditoriai turi suderinti numatytus kibernetinio xsaugumo kontrolės testus su teminiu reikalavimu. Toliau pateiktoje diagramoje kibernetinio saugumo teminis reikalavimas susietas su trimis dažniausiai naudojamomis sistemomis: NIST Kibernetinio saugumo sistema 2.0, COBIT 2019 ir NIST 800-53. Šios sistemos buvo atvaizduotos, nes jos yra lengvai ir nemokamai prieinamos.

Valdysenos reikalavimai	Sistemų nuorodos		
	NIST CSF 2.0	NIST 800-53	COBIT 2019
A. Nustatyta ir periodiškai atnaujinama oficiali kibernetinio saugumo strategija ir tikslai. Apie kibernetinio saugumo tikslų įgyvendinimo atnaujinimus periodiškai pranešama ir juos peržiūri valdyba, įskaitant kibernetinio saugumo strategijai paremti skirtus išteklius ir biudžeto lėšas.	GV.RM-01; GV.RM-02; GV.RM-03; GV.RM-04; GV.OC-02; GV.RR-03; GV.RR-04; GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-03	PM-1, PM-4; AT-2; AT-3; PM-9; PM-28	EDM01; EDM03; EDM04; APO06; APO01; APO10; APO12
B. Su kibernetiniu saugumu susijusi politika ir procedūros yra nustatytos, periodiškai atnaujinamos ir stiprina kontrolės aplinką.	GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-02; GV.OV-03; GV.SC-01; GV.SC-03; GV.RR-03	AC-1, PM-9; AC-1; AT-1; CA-1; CM-1; IA-1; IR-1; MP-1; PE-1	EDM01; EDM02; EDM03; APO01; APO11
C. Nustatytos kibernetinio saugumo tikslus padedančios įgyvendinti funkcijos ir pareigos, taip pat nustatytas procesas, pagal kurį periodiškai vertinamos šias funkcijas atliekančių asmenų žinios, įgūdžiai ir gebėjimai.	GV.RR-02; GV.RR-04; GV.SC-02; GV.OC-02	PM-13; AT-2; AT-3	EDM02; APO01; APO07

D. Atitinkami suinteresuotieji subjektai įtraukiami aptarti esamus kibernetinio saugumo aplinkos pažeidžiamumus ir kylančias grėsmes bei imtis veiksmų. Suinteresuotosios šalys apima aukščiausiąją vadovybę, operacijas, rizikos valdymą, žmogiškuosius išteklius, teisinius, atitikties užtikrinimo klausimus, tiekėjus ir kt.	GV.OC-02; GV.RM-01; GV.RM-05; GV.RM-07; GV.OV-03; GV.SC-03	AC-1; CM-1	EDM05; EDM01.01; EDM03; MEA01.02; APO01; APO08; APO11; APO13; MEA02
Rizikos valdymo reikalavimai	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A. Organizacijos rizikos vertinimo ir valdymo procesai apima kibernetinio saugumo grėsmių ir jų poveikio strateginių tikslų įgyvendinimui nustatymą, analizę, mažinimą ir stebėseną.	GV.RM-01; GV.RM-03; GV.OC-01	AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
B. Kibernetinio saugumo rizikos valdymas atliekamas visoje organizacijoje, kuri gali apimti šias sritis: informacinių technologijų, įmonės rizikos valdymo, žmogiškųjų išteklių, teisės, atitikties, operacijų, tiekimo grandinės, apskaitos, finansų ir kitas.	GV.RM-01; GV.RM-05; GV.RR-01; GV.RR-02; GV.OC-03; GV.SC-07	PM-29; AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
C. Nustatyta atskaitomybė ir atsakomybė už kibernetinio saugumo rizikos valdymą ir paskirtas asmuo arba grupė, kuri periodiškai stebi ir praneša, kaip valdoma kibernetinio saugumo rizika, įskaitant išteklius, reikalingus rizikai mažinti ir naujoms kibernetinio saugumo grėsmėms nustatyti.	GV.RR-01; GV.RR-02; GV.RR-03; GV.0V-01; GV.OV-02; GV.OV-03	PM-9; PM-29	EDM03; APO01; APO10; APO12

D. Nustatytas procesas, skirtas greitai eskaluoti bet kokią kibernetinio saugumo riziką (kylančią ar anksčiau nustatytą), kuri išauga iki nepriimtino lygio, remiantis organizacijos nustatytomis rizikos valdymo gairėmis arba siekiant laikytis taikomų teisinių ir reguliavimo reikalavimų. Turi būti atsižvelgta ir į finansinį, ir į nefinansinį kibernetinio saugumo rizikos poveikį.	GV.RM; ID.RA; RS.MA-04	CA-7; RA-3; RA-7	EDM03; APO01, APO10; APO12
E. Nustatytas procesas, pagal kurį vadovybė ir darbuotojai informuojami apie kibernetinio saugumo riziką, o vadovybė periodiškai peržiūri problemas, spragas, trūkumus arba kontroliuoja savalaikiai pateiktus trūkumus ir jų šalinimą.	PR.AT; GV.RR.01; GV.RR-04; GV.PO	AT-2	APO01; APO02; EDM03; MEA03
F. Organizacija yra įdiegusi kibernetinio saugumo incidentų valdymo procesą, apimantį aptikimą, suvaldymą, atkūrimą ir analizę po incidento. Reagavimo į incidentus ir atkūrimo procesas periodiškai testuojamas.	RS; RC	IR-4; IR-5; IR-6; IR-7; IR-8; IR-10; SA-15	DSS02; DSS03; DSS04; DSS05.07
Kontrolės proceso reikalavimai	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A. Nustatytas procesas, kuriuo užtikrinama, kad būtų įdiegtos vidaus kontrolės priemonės ir tiekėjų kontrolės priemonės, skirtos organizacijos sistemų ir duomenų konfidencialumui, vientisumui ir prieinamumui apsaugoti. Kontrolės periodiškai vertinamos, siekiant nustatyti, ar jos veikia taip, kad būtų skatinama siekti organizacijos kibernetinio saugumo tikslų ir laiku spręsti problemas.	ID.IM-01; ID.IM-02; ID.IM-03; PR; DE; RS; RC; ID.RA06; GV.RM-05; GV.SC; ID.IM-02; RS.MA-01; DE.CM-06	AC-3; AC-4; AC-10; AC-13; AC-17; PM-30; RA-3; SA-9; SR-2	MEA02; MEA04; EDM03; APO09; APO10; DSS01

B. Kibernetinio saugumo operacijoms nustatytas ir periodiškai peržiūrimas talentų valdymo procesas, apimantis mokymo galimybes, kad būtų ugdomos ir palaikomos techninės kompetencijos.	PR.AT-01; PR.AT-02; GV.RR-03	AT-2; AT-3; IR-2; PM-14	APOO7; DSS04
C. Nustatytas procesas, skirtas nuolat stebėti ir pranešti apie kylančias kibernetinio saugumo grėsmes ir pažeidžiamumus, taip pat nustatyti, prioretizuoti ir įgyvendinti kibernetinio saugumo gerinimo galimybes.	ID.RA-02; ID.RA-03, ID.RA-04	CA-7; PM-31; RA-5	DSS03.05
D. Kibernetinis saugumas įtraukiamas į viso IT turto, įskaitant techninę ir programinę įrangą bei pardavėjų paslaugas, gyvavimo ciklo valdymą (parinkimą, naudojimą, priežiūrą ir eksploatavimo nutraukimą).	ID.AM; PR.PS-03; PR.IR; DE.CM-09; ID.AM-08; ID.RA-09; PR.PS-06	AU-9; CM-7; SC-49; SC-51; CM-2; SA-3; SA-10; SA-15; SA-17; SA-20; AU-6; IR-7	DSS05.03; BAI03; BAI09; BAI03; BAI11; DSS05.01; DSS02; DSS03; DSS06.06
E. Nustatyti kibernetinį saugumą skatinantys procesai, įskaitant konfigūravimą, galutinio naudotojo įrenginių administravimą, šifravimą, spragų taisymus, naudotojų prieigos valdymą ir prieinamumo bei našumo stebėseną. Kibernetinio saugumo aspektai įtraukiami į programinės įrangos kūrimą (DevSecOps).	PR.PS-01; PR.PS-06; PR.DS-01; PR.DS-02; PR.PS-05; DE.CM-03	CM-6; SI-2; AC-3; CA-7; SA-4; AC-16; AC-18	BAI10; DSS05; DSS06.03; DSS01.03; MEA01
F. Nustatytos su tinklu susijusios kontrolės priemonės, pavyzdžiui, prieigos prie tinklo kontrolė ir segmentavimas, ugniasienių naudojimas ir išdėstymas, ribotas prisijungimas iš išorinių tinklų ir prie jų, virtualaus privataus tinklo (VPN) ir nulinio pasitikėjimo tinklo prieiga (ZTNA), daiktų interneto (IoT) tinklo kontrolės priemonių įtraukimas ir įsilaužimo aptikimo ir prevencijos sistemos (IDS ir IPS).	PR.IR; DE.CM-01	AC-6; AC-17; AC-18; AC-20; SC-7; SC-10; CA-8	DSS05.02

G. Nustatytos galutinių įrenginių ryšių saugumo kontrolės priemonės, susijusios su tokiomis paslaugomis kaip el. paštas, interneto naršyklės, vaizdo konferencijos, pranešimų siuntimas, socialinė žiniasklaida, debesijos ir dalijimosi failais protokolai.	PR.DS-01; PR.DS-02; PR.DS-10; PR.IR	AC-2; AC-16; AU-10; CA-3; SI-8; SI-20; SC-8	BAI10

C priedas. Papildoma dokumentavimo priemonė

Tikimasi, kad vidaus auditoriai, remdamiesi rizikos vertinimu, profesiniu sprendimu nustatys reikalavimų taikymą ir tinkamai dokumentuos tam tikrų reikalavimų išimtis. Teminis reikalavimas gali būti dokumentuojamas vidaus audito plane arba užduoties darbo dokumentuose, remiantis auditoriaus profesiniu sprendimu. Reikalavimus gali apimti viena ar kelios vidaus audito užduotys. Be to, gali būti taikomi ne visi reikalavimai. Toliau pateiktoje formoje pateikiama viena iš galimybių dokumentuoti atitiktį kibernetinio saugumo teminiam reikalavimui, tačiau jos naudojimas nėra privalomas.

Kibernetinis saugumas – valdysena

Reikalavimas	Įvykdyta aprėptis arba išimties pagrindimas	Dokumentų nuoroda
A. Nustatyta ir periodiškai atnaujinama oficiali kibernetinio saugumo strategija ir tikslai. Apie kibernetinio saugumo tikslų įgyvendinimo atnaujinimus periodiškai pranešama ir juos peržiūri valdyba, įskaitant kibernetinio saugumo strategijai paremti skirtus išteklius ir biudžeto lėšas.		
B. Su kibernetiniu saugumu susijusi politika ir procedūros yra nustatytos, periodiškai atnaujinamos ir stiprina kontrolės aplinką.		
C. Nustatytos kibernetinio saugumo tikslus padedančios įgyvendinti funkcijos ir pareigos, taip pat nustatytas procesas, pagal kurį periodiškai vertinamos šias funkcijas atliekančių asmenų žinios, įgūdžiai ir gebėjimai.		

Reikalavimas	Įvykdyta aprėptis arba išimties pagrindimas	Dokumentų nuoroda
D. Atitinkami suinteresuotieji subjektai įtraukiami aptarti esamus kibernetinio saugumo aplinkos pažeidžiamumus ir kylančias grėsmes bei imtis veiksmų. Suinteresuotosios šalys apima aukščiausiąją vadovybę, operacijas, rizikos valdymą, žmogiškuosius išteklius, teisinius, atitikties užtikrinimo klausimus, tiekėjus ir kt.		

Kibernetinis saugumas - rizikos valdymas

Reikalavimas	Įvykdyta aprėptis arba išimties pagrindimas	Dokumentų nuoroda
A. Organizacijos rizikos vertinimo ir valdymo procesai apima kibernetinio saugumo grėsmių ir jų poveikio strateginių tikslų įgyvendinimui nustatymą, analizę, mažinimą ir stebėseną.		
B. Kibernetinio saugumo rizikos valdymas vykdomas visoje organizacijoje ir gali apimti šias sritis: informacinių technologijų, įmonės rizikos valdymo, žmogiškųjų išteklių, teisės, atitikties, operacijų, tiekimo grandinės, apskaitos, finansų ir kitas.		
C. Nustatyta atskaitomybė ir atsakomybė už kibernetinio saugumo rizikos valdymą. Nustatytas asmuo arba grupė, kurie periodiškai stebi, kaip valdoma kibernetinio saugumo rizika, įskaitant išteklius, reikalingus rizikai mažinti ir naujoms kibernetinio saugumo grėsmėms nustatyti, ir teikia ataskaitas.		

Reikalavimas	Įvykdyta aprėptis arba išimties pagrindimas	Dokumentų nuoroda
D. Nustatytas procesas, skirtas greitai eskaluoti bet kokią kibernetinio saugumo riziką (kylančią ar anksčiau nustatytą), kuri pasiekia nepriimtiną lygį pagal organizacijos nustatytas rizikos valdymo gaires arba taikomus teisinius ir reguliavimo reikalavimus. Reikėtų atsižvelgti į finansinį ir nefinansinį kibernetinio saugumo rizikos poveikį.		
E. Nustatytas procesas, pagal kurį vadovybė ir darbuotojai informuojami apie kibernetinio saugumo riziką, o vadovybė periodiškai peržiūri problemas, spragas arba kontroliuoja savalaikiai pateiktus trūkumus ir jų šalinimą. .		
F. Organizacija yra įdiegusi kibernetinio saugumo incidentų ir valdymo procesą, įskaitant aptikimą, suvaldymą, atkūrimą ir analizę po incidento. Reagavimo į incidentus ir atkūrimo procesas periodiškai testuojamas.		

Kibernetinis saugumas - kontrolės procesai

Reikalavimas	Įvykdyta aprėptis arba išimties pagrindimas	Dokumentų nuoroda
A. Nustatytas procesas, užtikrinantis, kad būtų įdiegtos vidaus kontrolės priemonės ir tiekėjų kontrolės priemonės, skirtos organizacijos sistemų ir duomenų konfidencialumui, vientisumui ir prieinamumui apsaugoti. Periodiškai atliekami vertinimai, siekiant nustatyti, ar kontrolės priemonės veikia taip, kad būtų skatinama siekti organizacijos kibernetinio saugumo tikslų ir greitai spręsti problemas.		
B. Nustatytas talentų valdymo procesas, apimantis mokymus, skirtus techninei kompetencijai, susijusiai su kibernetinio saugumo operacijomis, ugdyti ir palaikyti. Procesas periodiškai peržiūrimas.		
C. Nustatytas procesas, skirtas nuolat stebėti ir pranešti apie kylančias kibernetinio saugumo grėsmes ir pažeidžiamumus, taip pat nustatyti, prioretizuoti ir įgyvendinti kibernetinio saugumo gerinimo galimybes.		
D. Kibernetinis saugumas įtraukiamas į viso IT turto, įskaitant techninę ir programinę įrangą bei pardavėjų paslaugas, gyvavimo ciklo valdymą (parinkimą, naudojimą, priežiūrą ir eksploatavimo nutraukimą).		

Reikalavimas	Įvykdyta aprėptis arba išimties pagrindimas	Dokumentų nuoroda
E. Nustatyti kibernetinį saugumą skatinantys procesai, įskaitant konfigūravimą, galutinio naudotojo įrenginių administravimą, šifravimą, spragų taisymus, naudotojų prieigos valdymą ir prieinamumo bei našumo stebėjimą. Kibernetinio saugumo aspektai įtraukiami į programinės įrangos kūrimą (DevSecOps).		
F. Nustatytos su tinklu susijusios kontrolės priemonės, pavyzdžiui, prieigos prie tinklo kontrolė ir segmentavimas, saugiasienių naudojimas ir išdėstymas, ribotas prisijungimas iš išorinių tinklų ir prie jų, virtualaus privataus tinklo (VPN) / nulinio pasitikėjimo tinklo prieigos (ZTNA), daiktų interneto (IoT) tinklo kontrolė ir įsilaužimo aptikimo / prevencijos sistemos (IDS ir IPS).		
G. Nustatytos galutinio taško ryšių saugumo kontrolės priemonės tokioms paslaugoms kaip el. paštas, interneto naršyklės, vaizdo konferencijos, pranešimų siuntimas, socialinė žiniasklaida, debesijos ir dalijimosi failais protokolai.		

Apie Vidaus auditorių institutą

Vidaus auditorių institutas (IIA) yra tarptautinė profesinė asociacija, vienijanti daugiau nei 255 000 narių visame pasaulyje ir suteikusi daugiau nei 200 000 sertifikuotų vidaus auditorių (CIA®) pažymėjimų visame pasaulyje. Įkurtas 1941 m., IIA visame pasaulyje pripažįstamas kaip vidaus audito profesijos lyderis standartų, sertifikavimo, švietimo, mokslinių tyrimų ir techninių rekomendacijų srityje. Daugiau informacijos www.theiia.org.

Atsakomybės apribojimas

IIA šį dokumentą skelbia informaciniais ir švietimo tikslais. Šioje medžiagoje nesiekiama pateikti galutinių atsakymų konkrečiomis individualiomis aplinkybėmis, todėl ja galima naudotis tik kaip vadovu. IIA rekomenduoja kreiptis į nepriklausomus ekspertus dėl konsultacijos, tiesiogiai susijusios su bet kokia konkrečia situacija. IIA neprisiima jokios atsakomybės už asmenis, kurie remiasi tik šia medžiaga.

Autorinės teisės

2025 m. vasaris

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