Kyberturvallisuus

Aihekohtainen vaatimus

Topical Requirement

The Institute of
Internal Auditors

Kyberturvallisuuden aihekohtainen vaatimus

Sisäisen tarkastuksen ammatillinen viitekehys (IPPF, International Professional Practices Framework®) sisältää Kansainväliset sisäisen tarkastuksen standardit (Global Internal Audit Standards™), Aihekohtaiset vaatimukset (Topical Requirements) ja Kansainväliset ohjeet (Global Guidance). Aihekohtaiset vaatimukset ovat pakollisia ja niitä tulee käyttää yhdessä standardien kanssa, jotka antavat määräävän perustan vaadituille käytännöille.

Aihekohtaiset vaatimukset määrittävät sisäisille tarkastajille minimitason tiettyjen riskiaiheiden tarkastamiselle. Organisaation riskiprofiili voi edellyttää, että sisäiset tarkastajat tarkastelevat myös aiheeseen liittyviä lisänäkökohtia.

Aihekohtaisten vaatimusten noudattaminen lisää sisäisen tarkastuksen palvelujen johdonmukaisuutta ja parantaa sisäisen tarkastuksen palvelujen ja tulosten laatua ja luotettavuutta. Ennen kaikkea aihekohtaiset vaatimukset vahvistavat sisäisen tarkastuksen ammattikuntaa.

Sisäisten tarkastajien täytyy soveltaa aihekohtaisia vaatimuksia Kansainvälisten sisäisen tarkastuksen standardien mukaisesti. Aihekohtaisten vaatimusten noudattaminen on pakollista varmennuspalvelujen osalta ja suositeltavaa neuvonantopalvelujen osalta.

Aihekohtaista vaatimusta sovelletaan, kun aiheena on jokin seuraavista:

A. Sisäisen tarkastuksen suunnitelman mukaisen toimeksiannon kohde.
B. Toimeksiantoa toteutettaessa tunnistettu kohde.
C. Toimeksiantopyynnön kohde, joka ei ole alkuperäisessä sisäisen tarkastuksen suunnitelmassa.

Todisteet siitä, että kunkin aihekohtaisen vaatimuksen soveltuvuus on arvioitu, täytyy dokumentoida ja säilyttää. Kaikkia yksittäisiä vaatimuksia ei välttämättä sovelleta jokaiseen toimeksiantoon; jos vaatimuksia ei sovelleta, perustelut täytyy dokumentoida ja säilyttää. Aihekohtaisten vaatimusten noudattaminen on pakollista, ja sitä arvioidaan laadunarvioinneissa.

Lisätietoja löydät Kyberturvallisuus Aihekohtainen vaatimus – käyttöoppaasta (User Guide).

Kyberturvallisuus

Yhdysvaltain Kansallinen standardointi- ja teknologiainstituutti (NIST) määrittelee kyberturvallisuuden yksinkertaisesti seuraavasti: "Kyky suojella tai puolustaa kyberavaruuden käyttöä kyberhyökkäyksiltä." Kyberturvallisuus on osa yleistä tietoturvaa, jonka NIST määrittelee seuraavasti: "Tietojen ja tietojärjestelmien suojaaminen luvattomalta pääsyltä, käytöltä, paljastamiselta, häirinnältä, muokkaamiselta tai tuhoamiselta luottamuksellisuuden, eheyden ja käytettävyyden varmistamiseksi."

Kyberturvallisuus vähentää riskejä vahvistamalla yleistä kontrolliympäristöä ja suojaamalla organisaation tietovarantoja luvattomalta käytöltä, häirinnältä, muuttamiselta tai tuhoamiselta. Kyberhyökkäykset voivat johtaa suoriin ja epäsuoriin vaikutuksiin, jotka ovat usein merkittäviä, sillä tietokoneet, verkot, ohjelmat, data ja arkaluonteiset tiedot ovat useimpien organisaatioiden kriittisiä osa-alueita.

Kyberturvallisuuden hallinnoinnin, riskienhallinnan ja kontrolliprosessien (valvontaprosessien) arviointi

Tämä aihekohtainen vaatimus määrittää johdonmukaisen ja kattavan lähestymistavan kyberturvallisuuden hallinnointi-, riskienhallinta- ja kontrolliprosessien suunnittelun ja toteutuksen arviointiin. Vaatimukset määrittävät minimitason organisaation kyberturvallisuuden arvioimiseksi.

HALLINNOINTI: Kyberturvallisuuden hallinnoinnin arviointi

Vaatimukset:

Sisäisten tarkastajien täytyy arvioida seuraavat asiat organisaation kyberturvallisuuden hallinnoinnin osalta:

A. Virallinen kyberturvallisuusstrategia ja -tavoitteet on laadittu ja niitä päivitetään säännöllisesti. Hallitus tiedottaa säännöllisesti kyberturvallisuustavoitteiden saavuttamisesta ja käy niitä läpi, mukaan lukien resurssit ja talousarvioon liittyvät näkökohdat, jotka tukevat kyberturvallisuusstrategiaa.
B. Kyberturvallisuuteen liittyvät toimintaperiaatteet ja menettelytavat on määritetty ja niitä päivitetään säännöllisesti kontrolliympäristön vahvistamiseksi.
C. Kyberturvallisuustavoitteita tukevat roolit ja vastuualueet on määritetty, ja käytössä on prosessi, jonka avulla arvioidaan säännöllisesti näissä rooleissa toimivien tietoja, taitoja ja kykyjä.
D. Relevantit sidosryhmät ovat mukana keskustelemassa, ja he tunnistavat sekä varautuvat kyberturvallisuusympäristön olemassa oleviin haavoittuvuuksiin ja uusiin uhkiin. Sidosryhmiin kuuluvat ylin johto, liike- ja operatiivinen toiminta, riskienhallinta, henkilöstöhallinto, lakiasiat, compliance, toimittajat ja muut.

RISKIENHALLINTA: Kyberturvallisuusriskien hallinnan arviointi

Vaatimukset:

Sisäisten tarkastajien täytyy arvioida seuraavat asiat organisaation kyberturvallisuusriskien hallinnan osalta:

A. Organisaation riskiarvio- ja riskienhallintaprosesseissa tulee tunnistaa, arvioida, pienentää ja seurata kyberturvallisuusuhkia ja niiden vaikutusta strategisten tavoitteiden saavuttamiseen.
B. Kyberturvallisuusriskien hallintaa toteuttaa koko organisaatio, ja siihen voivat kuulua seuraavat osa-alueet: tietotekniikka, kokonaisvaltainen riskienhallinta (ERM), henkilöstöhallinto, lakiasiat, compliance, liike- ja operatiivinen toiminta, toimitusketjut, taloushallinto, rahoitus ja muut.
C. Kyberturvallisuusriskien hallintaan liittyvät vastuut on määritetty. On määritetty henkilö tai ryhmä, joka seuraa ja raportoi säännöllisesti, miten kyberturvallisuusriskejä hallitaan, mukaan lukien resurssit, joita tarvitaan riskien pienentämiseen ja uusien kyberturvallisuusuhkien tunnistamiseen.
D. Käytössä on prosessi, jonka avulla voidaan nopeasti eskaloida mikä tahansa (uusi tai aiemmin tunnistettu) kyberturvallisuusriski, joka on liian korkea organisaation riskienhallintaohjeiden tai sovellettavien oikeudellisten ja sääntelyvaatimusten mukaisesti. Kyberturvallisuusriskin taloudelliset ja muut kuin taloudelliset vaikutukset tulisi ottaa huomioon.
E. Käytössä on prosessi, jonka avulla kyberturvallisuusriskitietoisuudesta tiedotetaan johdolle ja työntekijöille.Tämän prosessin avulla johto käy läpi säännöllisesti kysymyksiä ja asioita, eroavaisuuksia, puutteita tai kontrollivirheitä ja raportoi niistä oikea-aikaisesti ja korjaa ne.
F. Organisaatio on ottanut käyttöön kyberturvallisuuden häiriötilanteisiin reagointi- ja palautumisprosessin, joka sisältää havaitsemisen, rajoittamisen, palautumisen ja tapahtuman jälkianalyysin. Kyberhäiriöiden reagointi- ja palautumisprosessi testataan säännöllisesti.

KONTROLLIT: Kyberturvallisuuden valvontaprosessien arviointi.

Vaatimukset:

Sisäisten tarkastajien on arvioitava seuraavat asiat organisaation kyberturvallisuuden valvontaprosessien osalta:

A. Käytössä on prosessi, jolla varmistetaan, että organisaation järjestelmien ja datan luottamuksellisuuden, eheyden ja saatavuuden suojaamiseksi on käytössä sekä organisaation sisäiset kontrollit että toimittajapohjainen valvonta. Arviointeja tehdään säännöllisesti sen määrittämiseksi, toimivatko kontrollit tavalla, joka edistää organisaation kyberturvallisuustavoitteiden saavuttamista ja esiin nousseiden ongelmien nopeaa ratkaisemista.

B. Käytössä on osaamisen johtamisen prosessi, johon sisältyy koulutusta kyberturvallisuustoimintaan liittyvän teknisen osaamisen kehittämiseksi ja ylläpitämiseksi Prosessia käydään läpi säännöllisesti.

C. Käytössä on prosessi, jonka avulla seurataan jatkuvasti uusia kyberturvallisuusuhkia ja -haavoittuvuuksia ja raportoidaan niistä. Tämän lisäksi tunnistetaan, priorisoidaan ja toteutetaan kyberturvallisuustoimien parannuksia.

D. Kyberturvallisuus sisältyy tietoteknisten laitteiden, kuten laitteistojen, ohjelmistojen ja toimittajapalvelujen, elinkaaren hallintaan (valinta, käyttö, ylläpito ja käytöstä poistaminen).

E. Käytössä on prosessit kyberturvallisuuden vahvistamiseksi, mukaan lukien konfigurointi, loppukäyttäjän laitteiden hallinta, salaus, päivittäminen, käyttäjien pääsynhallinta sekä käytettävyyden ja suorituskyvyn seuranta. Kyberturvallisuusnäkökohdat otetaan huomioon ohjelmistokehityksessä (DevSecOps).

F. Verkkoon liittyvät kontrollit, kuten verkon pääsynhallinta ja segmentointi, palomuurien käyttö ja sijoittaminen, rajoitetut yhteydet ulkoisista verkoista ja ulkoisiin verkkoihin, virtuaalinen yksityisverkko (VPN) / nollaluottamusverkkoyhteys (ZTNA), esineiden internetin (IoT) verkkokontrollit sekä tunkeutumisen havaitsemis- ja estämisjärjestelmät (IDS ja IPS).

G. Verkossa olevien laitteiden päätepisteviestinnän tietoturvatarkastukset on otettu käyttöön sähköpostin, internetselaimien, videoneuvottelujen, viestinvälityksen, sosiaalisen median, pilvipalvelun ja tiedostojen jakoprotokollien kaltaisille palveluille.

Helmikuu 2025

The Institute of Internal Auditors

The Institute of Internal Auditors, Inc.
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, Yhdysvallat
Puhelin: +1-407-937-1111
Faksi: +1-407-937-1101