Kibernetička sigurnost

Topical Requirement

Tematski zahtjev

The Institute of
Internal Auditors

Tematski zahtjev za kibernetičku sigurnost

Međunarodni okvir profesionalnog djelovanja (International Professional Practices Framework®) uključuje Globalne standarde interne revizije (Global Internal Audit Standards™), Tematske zahtjeve i Globalne smjernice. Tematski zahtjevi su obvezni i moraju se koristiti zajedno sa Standardima, koji pružaju mjerodavnu osnovu za zahtijevane prakse.

Tematski zahtjevi pružaju jasna očekivanja za interne revizore postavljanjem minimalne osnove za reviziju određenih tema vezanih uz rizike. Profil rizika organizacije može zahtijevati od internih revizora da razmotre dodatne aspekte teme.

Sukladnost s tematskim zahtjevima povećat će dosljednost s kojom se obavljaju usluge interne revizije i poboljšati kvalitetu i pouzdanost usluga i rezultata interne revizije. Naposljetku, tematski zahtjevi uzdižu profesiju interne revizije.

Interni revizori moraju primjenjivati tematske zahtjeve u skladu s Globalnim standardima interne revizije. Sukladnost s tematskim zahtjevima obvezna je za usluge izražavanja uvjerenja i preporučuje se za savjetodavne usluge.

Tematski zahtjev primjenjiv je kada je tema jedno od sljedećeg:

A. Predmet angažmana u planu interne revizije.
B. Prepoznat tijekom angažmana.
C. Predmet zahtjeva za angažman nije dio prvobitnog plana interne revizije.

Dokaz da je ocijenjena primjenjivost svakog zahtjeva u tematskom zahtjevu mora se dokumentirati i čuvati. Svi pojedinačni zahtjevi ne moraju biti primjenjivi u svakom angažmanu; ako se pojedini zahtjevi izostave, obrazloženje o tome se mora dokumentirati i sačuvati. Sukladnost s Tematskim zahtjevom obvezna je i ocjenjivat će se tijekom procjena kvalitete.

Za više informacija, pogledajte Korisnički vodič za Tematski zahtjev za kibernetičku sigurnost.

Kibernetička sigurnost

Nacionalni institut za standarde i tehnologiju (NIST) kibernetičku sigurnost definira jednostavno kao "Sposobnost zaštite ili obrane korištenja kibernetičkog prostora od

kibernetičkih napada." Kibernetička sigurnost je podskup sveobuhvatne informacijske sigurnosti, koju NIST definira kao, "Zaštita informacija i informacijskih sustava od neovlaštenog pristupa, korištenja, otkrivanja, ometanja, izmjene ili uništenja kako bi se osigurala povjerljivost, *integritet* i dostupnost."

Kibernetička sigurnost smanjuje rizik jačanjem sveukupnog kontrolnog okruženja i zaštitom informacijske imovine organizacije od neovlaštenog pristupa, ometanja, izmjene ili uništenja. Kibernetički napadi mogu dovesti do izravnih i neizravnih učinaka koji su često značajni, jer su računala, mreže, programi, podaci i osjetljive informacije kritične komponente većine organizacija.

Vrednovanje i procjena procesa upravljanja kibernetičkom sigurnošću, upravljanja rizikom i kontrolnim procesima

Ovaj Tematski zahtjev pruža dosljedan, sveobuhvatan pristup procjeni dizajna i provedbe upravljanja kibernetičkom sigurnošću, upravljanja rizicima i kontrolnim procesima. Zahtjevi predstavljaju minimalnu razinu za procjenu kibernetičke sigurnosti u organizaciji.

KORPORATIVNO UPRAVLJANJE: Vrednovanje i procjena upravljanja kibernetičkom sigurnošću

Zahtjevi:

Interni revizori moraju procijeniti sljedeće, vezano uz upravljanje kibernetičkom sigurnošću organizacije:

A. Službena strategija i ciljevi kibernetičke sigurnosti su uspostavljeni i ažurirani u redovnim vremenskim intervalima. Ažuriranja o postizanju ciljeva kibernetičke sigurnosti povremeno se priopćuju i pregledavaju od strane odbora, uključujući razmatranja resursa i budžeta za podršku strategiji kibernetičke sigurnosti.
B. Politike i procedure vezane uz kibernetičku sigurnost su uspostavljene i ažuriraju se u redovnim vremenskim intervalima kako bi se ojačalo kontrolno okruženje.
C. Uspostavljene su uloge i odgovornosti koje podupiru ciljeve kibernetičke sigurnosti, a postoji i proces za povremenu procjenu znanja, vještina i sposobnosti pojedinaca koji popunjavaju te uloge.
D. Relevantni dionici uključeni su u raspravu i djelovanje u vezi s postojećim ranjivostima i nadolazećim prijetnjama u okruženju kibernetičke sigurnosti. Dionici uključuju više rukovodstvo, operacije, upravljanje rizikom, ljudske resurse, pravne poslove, usklađenost, dobavljače i druge.

UPRAVLJANJE RIZICIMA: Vrednovanje i procjena upravljanja rizicima kibernetičke sigurnosti

Zahtjevi:

Interni revizori moraju procijeniti sljedeće vezano uz upravljanje rizicima kibernetičke sigurnosti organizacije:

A. Procesi procjene rizika i upravljanja rizicima u organizaciji uključuju prepoznavanje, analiziranje, ublažavanje i praćenje prijetnji kibernetičkoj sigurnosti i njihovog učinka na postizanje strateških ciljeva.

B. Upravljanje rizicima kibernetičke sigurnosti provodi se u cijeloj organizaciji i može uključivati sljedeća područja: informacijsku tehnologiju, upravljanje rizicima poduzeća, ljudske resurse, pravne poslove, usklađenost, operacije, lanac opskrbe, računovodstvo, financije i druga.

C. Uspostavljena je odgovornost (eng. „*accountability and responsibility*“) za upravljanje rizikom kibernetičke sigurnosti. Utvrđen je pojedinac ili tim koji će u redovnim vremenskim intervalima nadzirati i izvještavati o upravljanju rizicima kibernetičke sigurnosti, uključujući resurse potrebne za ublažavanje rizika i prepoznavanje novih i nadolazećih prijetnji kibernetičkoj sigurnosti.

D. Uspostavljen je proces za brzu eskalaciju bilo kojeg rizika kibernetičke sigurnosti (koji će se tek pojaviti ili je prethodno uočen) koji dosegne neprihvatljivu razinu u skladu s utvrđenim smjernicama organizacije za upravljanje rizikom ili primjenjivim zakonskim i regulatornim zahtjevima. Treba razmotriti financijske i nefinancijske učinke rizika kibernetičke sigurnosti.

E. Uspostavljen je proces za osvješćivanje o rizicima kibernetičke sigurnosti prema menadžmentu i zaposlenicima te redovni proces pregleda problema, nedostataka ili propusta kontrola od strane menadžmenta uz pravodobno izvješćivanje i saniranje.

F. Organizacija je implementirala odgovor na incidente kibernetičke sigurnosti i proces oporavka koji uključuje otkrivanje, ograničavanje, oporavak i analizu nakon rješavanja incidenta. Odgovor na incidente i proces oporavka se testiraju u redovnim vremenskim intervalima.

KONTROLE: Vrednovanje i procjena procesa kontrole kibernetičke sigurnosti

Interni revizori moraju procijeniti sljedeće vezano uz procese kontrole kibernetičke sigurnosti organizacije:

A. Uspostavljen je proces kojim se osigurava postojanje internih kontrola i kontrola dobavljača radi zaštite povjerljivosti, integriteta i dostupnosti sustava i podataka organizacije. Procjene se provode povremeno kako bi se utvrdilo funkcioniraju li kontrole na način koji promiče postizanje organizacijskih ciljeva kibernetičke sigurnosti i brzo rješavanje problema.

B. Uspostavljen je proces upravljanja talentima koji uključuje obuku za razvoj i održavanje tehničkih kompetencija vezanih uz operacije kibernetičke sigurnosti. Proces se povremeno pregledava.

C. Uspostavljen je proces za kontinuirano praćenje i izvješćivanje o novim i nadolazećim prijetnjama i ranjivostima kibernetičke sigurnosti te za prepoznavanje, određivanje prioriteta i implementaciju prilika za poboljšanje operacija kibernetičke sigurnosti.

D. Kibernetička sigurnost je uključena u upravljanje životnim ciklusom (odabir, korištenje, održavanje i stavljanje van upotrebe) sve IT imovine, uključujući hardver, softver i usluge dobavljača.

E. Uspostavljeni su procesi za jačanje kibernetičke sigurnosti, uključujući konfiguraciju, administraciju korisničkih uređaja, enkripciju, primjenu zakrpa (eng. patching), upravljanje korisničkim pristupom te praćenje dostupnosti i performansi. Načela kibernetičke sigurnosti uključena su u razvoj softvera (DevSecOps).

F. Uspostavljene su mrežne kontrole, kao što su kontrole pristupa mreži (eng. network-access controls) i segmentacija; korištenje i postavljanje vatrozida (eng. firewalls); ograničene veze od i prema vanjskim mrežama; virtualna privatna mreža (VPN) / pristup mreži s nultim povjerenjem (eng. zero trust network access, ZTNA); mrežne kontrole interneta stvari (eng. Internet of Things, IoT); i sustave za otkrivanje/sprečavanje upada (eng. intrusion detection/prevention systems, IDS i IPS).

G. Sigurnosne kontrole komunikacije krajnjih točaka (eng. endpoint-communication security controls) uspostavljene su za usluge kao što su e-pošta, internetski preglednici, videokonferencije, slanje poruka, društveni mediji, oblak i protokoli za dijeljenje datoteka.

About The Institute of Internal Auditors

The Institute of Internal Auditors (The IIA) is an international professional association that serves more than 255,000 global members and has awarded more than 200,000 Certified Internal Auditor® (CIA®) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information, visit www.theiia.org.

Copyright

February 2025

The Institute of Internal Auditors

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