Sajber bezbednost

Tematski zahtev

Topical Requirement

Prevedeno od strane:

The Institute of Internal Auditors

Udruženje internih revizora Srbije

Tematski zahtev za sajber bezbednost

Tematski zahtevi su obavezna komponenta Međunarodnog okvira profesionalnih praksi (International Professional Practices Framework®), zajedno sa Globalnim standardima interne revizije™ (Global Internal Audit Standards™) i Globalnim smernicama. Tematske zahteve treba koristiti zajedno sa Globalnim standardima interne revizije, koji obezbeđuju merodavnu osnovu za zahtevane prakse.

Tematski zahtevi pružaju jasna očekivanja od internih revizora, postavljanjem minimalne osnove za reviziju određenih tema rizika. Profil rizika organizacije može zahtevati od internih revizora da razmotre dodatne aspekte određene teme.

Usklađenost sa Tematskim zahtevima povećaće doslednost u pružanju usluga interne revizije i poboljšaće kvalitet i pouzdanost usluga i rezultata interne revizije. Iznad svega, Tematski zahtevi unapređuju profesiju interne revizije.

Interni revizori moraju da primenjuju Tematske zahteve u skladu sa Globalnim standardima interne revizije. Usklađenost sa Tematskim zahtevima je obavezna za usluge uveravanja i preporučuje se za savetodavne usluge.

Tematski zahtev je primenljiv kada je određena tema:

A. Predmet angažovanja u planu interne revizije.
B. Identifikovana tokom sprovođenja angažmana.
C. Predmet angažovanja koje nije bilo u originalnom planu interne revizije.

Dokazi da je svaki zahtev iz Tematskog zahteva procenjen u smislu primenljivosti moraju biti dokumentovani i sačuvani. Ne mogu se svi pojedinačni zahtevi primeniti u svakom angažmanu; ako se određeni zahtevi izuzmu, obrazloženje mora biti dokumentovano i sačuvano. Usklađenost sa Tematskim zahtevom je obavezno i biće vrednovano prilikom procena kvaliteta.

Za više informacija, pogledajte Vodič za korisnike Tematskog zahteva za sajber bezbednost.

Sajber bezbednost

Nacionalni institut za standarde i tehnologiju (*National Institute of Standards and Technology* - NIST) definiše sajber bezbednost jednostavno kao „Sposobnost zaštite ili odbrane upotrebe sajber prostora od sajber napada“. Sajber bezbednost je podskup sveobuhvatne bezbednosti informacija, koju NIST definiše kao „Zaštitu informacija i informacionih sistema od neovlašćenog pristupa, upotrebe, otkrivanja, prekida, modifikacije ili uništenja kako bi se obezbedili poverljivost, integritet i dostupnost.“

Sajber bezbednost smanjuje rizik jačanjem celokupnog kontrolnog okruženja i zaštitom informacionih dobara organizacije od neovlašćenog pristupa, ometanja, izmene ili uništenja. Sajber napadi mogu dovesti do direktnih i indirektnih uticaja koji su često značajni, pošto su računari, mreže, programi, podaci i osetljive informacije ključne komponente većine organizacija.

Vrednovanje i procena upravljanja sajber bezbednošću, upravljanja rizicima i kontrolnih procesa

Ovaj Tematski zahtev pruža dosledan i sveobuhvatan pristup proceni dizajna i primene upravljanja sajber bezbednošću, upravljanja rizicima i kontrolnih procesa. Zahtevi predstavljaju minimalnu osnovu za procenu sajber bezbednosti u organizaciji.

UPRAVLJANJE: Vrednovanje i procena upravljanja sajber bezbednošću

Zahtevi:

Interni revizori moraju proceniti sledeće u vezi sa upravljanjem sajber bezbednošću organizacije:

A. Formalna strategija i ciljevi sajber bezbednosti su uspostavljeni i periodično se ažuriraju. Informacije o postizanju ciljeva sajber bezbednosti se periodično saopštavaju i pregledaju od strane odbora, uključujući resurse i budžet za podršku strategiji sajber bezbednosti.

B. Politike i procedure koje se odnose na sajber bezbednost su uspostavljene i periodično se ažuriraju kako bi se ojačalo kontrolno okruženje.

C. Određene su uloge i odgovornosti koje podržavaju ciljeve sajber bezbednosti, a postoji i proces za periodičnu procenu znanja, veština i sposobnosti pojedinaca koji obavljaju te uloge.

D. Relevantne zainteresovane strane su angažovane da razgovaraju i reaguju na postojeće ranjivosti i rastuće pretnje u oblasti sajber bezbednosti. Zainteresovane strane uključuju najviše rukovodstvo, operacije, upravljanje rizicima, ljudske resurse, pravne poslove, usklađenost poslovanja, dobavljače i druge.

UPRAVLJANJE RIZICIMA: Vrednovanje i procena upravljanja rizikom sajber bezbednosti

Zahtevi:

U vezi sa upravljanjem rizikom sajber bezbednosti u organizaciji, interni revizori moraju proceniti sledeće:

A. Procena rizika organizacije i procesi upravljanja rizicima uključuju identifikaciju, analizu, ublažavanje i praćenje pretnji sajber bezbednosti i njihovog uticaja na postizanje strateških ciljeva.

B. Upravljanje rizikom sajber bezbednosti sprovodi se u celoj organizaciji i može uključivati sledeće oblasti: informacionu tehnologiju, upravljanje rizicima na nivou organizacije, ljudske resurse, pravne poslove, usklađenost poslovanja, operacije, lanac snabdevanja, računovodstvo, finansije i druge.

C. Nadležnost i odgovornost za upravljanje rizikom sajber bezbednosti je uspostavljena. Identifikovan je pojedinac ili tim koji periodično nadgledaju i izveštavaju o tome kako se upravlja rizicima sajber bezbednosti, uključujući resurse potrebne za ublažavanje rizika i identifikovanje rastućih pretnji po sajber bezbednost.

D. Uspostavljen je proces za brzu eskalaciju svakog rizika sajber bezbednosti (bilo da je u nastajanju ili je već identifikovan) koji dostigne neprihvatljiv nivo u skladu sa utvrđenim smernicama za upravljanje rizicima organizacije ili važećim zakonskim i regulatornim zahtevima. Treba uzeti u obzir finansijske i nefinansijske uticaje rizika sajber bezbednosti.

E. Uspostavljen je proces da se rukovodstvu i zaposlenima podigne svest o riziku sajber bezbednosti i da rukovodstvo povremeno pregleda probleme, manjkavosti, nedostatke ili neuspehe kontrola uz blagovremeno izveštavanje i korektivne mere.

F. Organizacija je primenila proces za odgovor i oporavak od incidenata u sajber bezbednosti koji uključuje otkrivanje, ograničavanje, oporavak i analizu nakon incidenta. Reakcija na incident i proces oporavka se periodično testiraju.

KONTROLE: Vrednovanje i procena kontrolnih procesa sajber bezbednosti

Zahtevi:

U vezi sa kontrolnim procesima sajber bezbednosti u organizaciji interni revizori moraju proceniti sledeće:

A. Uspostavljen je proces kako bi se osiguralo da postoje i interne kontrole i kontrole na strani dobavljača / pružalaca usluga, kako bi se zaštitila poverljivost, integritet i dostupnost sistema i podataka organizacije. Vrednovanja se vrše periodično kako bi se utvrdilo da li kontrole funkcionišu na način koji promoviše postizanje ciljeva sajber bezbednosti organizacije i brzo rešavanje problema.

B. Uspostavljen je proces upravljanja talentima koji uključuje obuku za razvoj i održavanje tehničkih kompetencija u vezi sa operacijama sajber bezbednosti. Proces se periodično pregleda.

C. Uspostavljen je proces za kontinuirano praćenje i izveštavanje o rastućim pretnjama i ranjivostima u vezi sa sajber bezbednošću i za identifikaciju, određivanje prioriteta i korišćenje mogućnosti za poboljšanje operacija sajber bezbednosti.

D. Sajber bezbednost je uključena u upravljanje životnim ciklusom (izbor, korišćenje, održavanje i povlačenje iz upotrebe) sve IT imovine, uključujući hardver, softver i usluge dobavljača.

E. Uspostavljeni su procesi za jačanje sajber bezbednosti, uključujući konfiguraciju, administraciju uređaja krajnjih korisnika, enkripciju, instalaciju zakrpa (*patching*), upravljanje korisničkim pristupima i praćenje dostupnosti i performansi. Razmatranja o sajber bezbednosti su uključena u razvoj softvera (DevSecOps).

F. Uspostavljene su kontrole vezane za mrežu, kao što su kontrole pristupa mreži i segmentacija; korišćenje i postavljanje zaštitnih zidova (*firewalls*); ograničene veze prema spoljnim mrežama i iz njih; virtuelna privatna mreža (*Virtual Private Network* – VPN) / pristup mreži sa nultim poverenjem (*Zero Trust Network Access* – ZTNA); mrežne kontrole Interneta stvari (*Internet of Things* – IoT); i sistemi za otkrivanje / prevenciju upada (*Intrusion Detection System* – IDS i *Intrusion Prevention System* – IPS).

G. Kontrole bezbednosti komunikacije preko krajnjih tačaka uspostavljene su za usluge kao što su elektronska pošta, Internet pretraživači, video konferencije, razmena poruka, društvene mreže, klaud (*cloud*) usluge i protokoli za deljenje datoteka.

O Institutu internih revizora (IIA)

Institut internih revizora (IIA) je međunarodno profesionalno udruženje koje opslužuje više od 255.000 globalnih članova i koje je dodelilo više od 200.000 sertifikata Certified internal auditor - CIA® (Ovlašćeni interni revizor - CIA®) širom sveta. Osnovan 1941. godine, Institut internih revizora je priznat širom sveta kao lider profesije interne revizije u standardima, sertifikatima, obrazovanju, istraživanju i tehničkim smernicama. Za više informacija posetite www.theiia.org.

Autorska prava

Februar 2025

The Institute of Internal Auditors

Globalno sedište
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Telefon: +1-407-937-1111
Fax: +1-407-937-1101