Kibernetska varnost

Topical Requirement

Tematska zahteva

The Institute of
Internal Auditors

Tematska zahteva za kibernetsko varnost

Mednarodni okvir strokovnih praks (International Professional Practices Framework®) obsega Globalne standarde notranjega revidiranja (Global Internal Audit Standards™), Tematske zahteve in Globalne smernice. Tematske zahteve so obvezne in jih je treba uporabljati v povezavi s Standardi, ki so avtoritativna podlaga za zahtevane prakse.

Tematske zahteve podajajo jasna pričakovanja do notranjih revizorjev, saj določajo minimalno izhodišče za revidiranje določenih področij tveganj. Profil tveganj organizacije lahko od notranjih revizorjev zahteva, da upoštevajo dodatne vidike teme.

Skladnost s tematskimi zahtevami bo povečala doslednost izvajanja notranjerevizijskih storitev ter izboljšala kakovost in zanesljivost notranjerevizijskih storitev in izidov. Navsezadnje, Tematske zahteve dvigujejo raven notranjerevizijske stroke.

Notranji revizorji morajo upoštevati Tematske zahteve v skladu z Globalnimi standardi notranjega revidiranja. Skladnost s Tematskimi zahtevami je obvezna za storitve dajanja zagotovil in priporočljiva za svetovalne storitve.

Tematska zahteva je uporabna, če je tema ena od naslednjih:

A. Predmet notranjerevizijskega posla v notranjerevizijskem načrtu.
B. Prepoznana med izvajanjem posla.
C. Predmet zahteve za posel, ki ni bil vključen v prvotni notranjerevizijski načrt.

Dokumentirati in hraniti je potrebno dokazila, da se je uporabnost vsake zahteve Tematske zahteve ocenila. Vse posamezne zahteve ne veljajo za vsak posel; če se zahteve ne upoštevajo, je utemeljitev za to potrebno dokumentirati in hraniti. Skladnost s tematsko zahtevo je obvezna in bo ocenjena med ocenjevanjem kakovosti.

Za več informacij glejte Uporabniški priročnik Tematske zahteve za kibernetsko varnosti

Kibernetska varnost

Nacionalni inštitut za standarde in tehnologijo (NIST) opredeljuje kibernetsko varnost kot "Sposobnost zaščititi ali obraniti uporabo kibernetskega prostora pred kibernetskimi napadi." Kibernetska varnost je podmnožica splošne informacijske varnosti, ki jo NIST opredeljuje kot "zaščito informacij in informacijskih sistemov pred nepooblaščenim dostopom, uporabo,

razkritjem, motenjem, spreminjanjem ali uničenjem za zagotavljanje zaupnosti, celovitosti in razpoložljivosti".

Kibernetska varnost zmanjšuje tveganje s krepitvijo celotnega kontrolnega okolja in zaščito informacijskih sredstev organizacije pred nepooblaščenim dostopom, motnjami, spreminjanjem ali uničenjem. Kibernetski napadi lahko povzročijo neposredne in posredne vplive, ki so pogosto pomembni, saj so računalniki, omrežja, programi, podatki in občutljive informacije kritične sestavine večine organizacij.

Ocenjevanje in vrednotenje upravljanja kibernetske varnosti, obvladovanja tveganj in kontrolnih procesov

Ta Tematska zahteva zagotavlja dosleden in celovit pristop k vrednotenju zasnove in izvajanja upravljanja kibernetske varnosti, obvladovanja tveganj in kontrolnih procesov. Zahteve predstavljajo minimalno izhodišče za vrednotenje kibernetske varnosti v organizaciji.

UPRAVLJANJE: Ocenjevanje in vrednotenje upravljanja kibernetske varnosti

Zahteve:

Notranji revizorji morajo v zvezi z upravljanjem kibernetske varnosti v organizaciji vrednotiti naslednje:

A. Vzpostavljena je formalna strategija kibernetske varnosti in cilji, ki se redno posodabljajo. Spremljanje doseganja ciljev kibernetske varnosti se redno sporoča organu nadzora, ki jih pregleda, vključno z viri in proračunskimi vidiki v podporo strategiji kibernetske varnosti.
B. Politike in postopki, povezani s kibernetsko varnostjo, so vzpostavljeni in se redno posodabljajo zakrepitev kontrolnega okolja.
C. Določene so vloge in odgovornosti, ki podpirajo cilje kibernetske varnosti, ter proces za redno vrednotenje znanja, veščin in sposobnosti posameznikov, ki opravljajo te vloge.
D. Vsi ustrezni deležniki so vključeni v razpravo o obstoječih ranljivostih in novo nastajajočih grožnjah v okolju kibernetske varnosti ter ukrepanju v zvezi z njimi. Med deležnike štejemo poslovodstvo, izvedbene službe, obvladovanje tveganj, ravnanje s človeškimi viri, pravno službo, skladnost, nabavno službo in druge.

OBVLADOVANJE TVEGANJ: Ocenjevanje in vrednotenje obvladovanja tveganj kibernetske varnosti

Zahteve:

Notranji revizorji morajo v zvezi z obvladovanjem tveganj kibernetske varnosti v organizaciji vrednotiti naslednje:

A. Procesi organizacije za vrednotenje in obvladovanje tveganj vključujejo prepoznavanje, analiziranje, zmanjševanje in spremljanje groženj kibernetske varnosti in njihovega učinka na doseganje strateških ciljev.

B. Obvladovanje tveganj kibernetske varnosti se izvaja čez celotno organizacijo in lahko vključuje naslednja področja: informacijsko tehnologijo, celovito obvladovanje tveganj, človeške vire, pravno službo, skladnost, izvedbene službe, dobavno verigo, računovodstvo, finance in druga.

C. Določene so odgovornosti in pristojnosti za obvladovanje tveganj kibernetske varnosti. Določen je posameznik ali skupina, ki redno spremlja in poroča, kako se obvladujejo tveganja kibernetske varnosti, vključno z viri, ki so potrebni za zmanjševanje tveganj in prepoznavanje novih groženj kibernetski varnosti.

D. Vzpostavljen je proces za hitro reševanje tveganj kibernetske varnosti (nastajajočih ali predhodno ugotovljenih) na višjo stopnjo odločanja, ko presežejo raven sprejemljivosti v skladu z vzpostavljenimi smernicami organizacije za obvladovanje tvveganj ali veljavnimi zakonskimi in regulativnimi zahtevami. Upoštevati je treba finančne in nefinančne vplive tveganja kibernetske varnosti.

E. Vzpostavljen je proces za ozaveščanje vodstva in zaposlenih o tveganjih kibernetske varnosti. Vodstvo redno pregleduje izzive, vrzeli, pomanjkljivosti in napake kontrol s pravočasnim poročanjem in odpravljanjem pomanjkljivosti.

F. Vzpostavljen je proces odzivanja na incidente kibernetske varnosti in okrevanja, ki vključuje odkrivanje, obvladovanje, obnovitev in analizo po incidentu. Postopek odzivanja na incidente in okrevanje se redno preizkuša.

KONTROLE: Ocenjevanje in vrednotenje kontrolnih procesov kibernetske varnosti

Zahteve:

Notranji revizorji morajo s kontrolnimi procesi kibernetske varnosti v organizaciji vrednotiti naslednje:

A. Vzpostavljen je postopek za zagotavljanje notranjih kontrol in kontrol na strani dobaviteljev za zaščito zaupnosti, celovitosti in razpoložljivosti sistemov in podatkov organizacije. Ocenjevanja se izvajajo redno, da se ugotovi, ali kontrole delujejo na način, ki spodbuja doseganje organizacijskih ciljev kibernetske varnosti in hitro reševanje težav.

B. Vzpostavljen je proces obvladovanja talentov, ki vključuje usposabljanje za razvoj in ohranjanje tehničnih kompetenc, povezanih z delovnimi nalogami kibernetske varnosti. Proces se redno pregleduje.

C. Vzpostavljen je proces za stalno spremljanje in poročanje o nastajajočih grožnjah in ranljivostih na področju kibernetske varnosti ter za prepoznavanje, prednostno razvrščanje in vpeljavo priložnosti za izboljšanje kibernetske varnosti.

D. Kibernetska varnost je vključena v obvladovanje življenjskega cikla (izbira, uporaba, vzdrževanje in razgradnja) vseh sredstev IT, vključno s strojno in programsko opremo ter storitvami dobaviteljev.

E. Vzpostavljeni so procesi za krepitev kibernetske varnosti, vključno s konfiguracijo, administracijo naprav za končne uporabnike, šifriranjem, popravki, obvladovanjem dostopov uporabnikov ter spremljanjem razpoložljivosti in uspešnosti. Kibernetska varnost je vključena v razvoj programske opreme (angl. DevSecOps).

F. Vzpostavljene so kontrole, povezane z omrežjem, kot so kontrole in segmentacija dostopa do omrežja, uporaba in postavitev požarnih pregrad, omejitve povezav iz zunanjih omrežij in z njimi, navidezno zasebno omrežje (VPN)/dostop do omrežja brez zaupanja (ZTNA), kontrole omrežja interneta stvari (IoT) ter sistemi za odkrivanje/preprečevanje vdorov (IDS in IPS).

G. Varnostne kontrole končnih komunikacijskih točk so vzpostavljene za storitve, kot so e-pošta, spletni brskalniki, videokonference, sporočanje, družbeni mediji, oblak in protokoli za izmenjavo datotek.

O Inštitutu notranjih revizorjev

Inštitut notranjih revizorjev (The IIA) je mednarodno strokovno združenje, ki globalno združuje več kot 255.000 članov in je globalno podelilo več kot 200.000 strokovnih nazivov Certified Internal Auditor® (CIA®). Združenje IIA je bilo ustanovljeno leta 1941 in je globalno priznano kot vodilno združenje na področju standardov, certificiranja, izobraževanja, raziskav in tehničnega vodenja notranje revizije. Za več informacij obiščite www.theiia.org.

Avtorske pravice

Februar 2025

The Institute of Internal Auditors

Globalni sedež
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, ZDA
Telefon: +1-407-937-1111
Faks: +1-407-937-1101