Kibernetska varnost

Topical Requirement

Tematska zahteva

Uporabniški priročnik

The Institute of
Internal Auditors

Vsebina

Pregled tematskih zahtev

Tematske zahteve so obvezna sestavina Mednarodnega okvira strokovnega ravnanja (International Professional Practices Framework®), skupaj z Globalnimi standardi notranjega revidiranja (Global Internal Audit Standards™) in Globalnimi smernicami. Inštitut notranjih revizorjev zahteva, da se Tematske zahteve uporabljajo skupaj z Globalnimi standardi notranjega revidiranja, ki so avtoritativna podlaga za zahtevane prakse. Sklicevanja na Standarde se pojavljajo v tem priročniku kot vir podrobnejših informacij.

Tematske zahteve formalizirajo, kako notranji revizorji obravnavajo prevladujoča področja tveganj, da bi spodbudili kakovost in doslednost v stroki. Tematske zahteve določajo izhodišče in zagotavljajo primerna sodila za izvajanje storitev dajanja zagotovil, povezanih s predmetom tematske zahteve (Standard 13.4 Sodila za ocenjevanje). Skladnost s Tematskimi zahtevami je obvezna za storitve dajanja zagotovil in priporočljiva za vrednotenje pri svetovalnih storitvah. Namen Tematskih zahtev ni zajeti vseh možnih vidikov, ki jih je treba upoštevati pri izvajanju storitev dajanja zagotovil; njihov namen je zagotoviti najmanjši nabor zahtev, ki omogočajo dosledno in zanesljivo ocenjevanje teme.

Tematske zahteve so jasno povezane z Modelom treh linij IIA in Globalnimi standardi notranjega revidiranja. Procesi upravljanja, obvladovanja tveganj in kontrolnih procesov so glavne sestavine tematskih zahtev, ki so usklajene s Standardom 9.1 Razumevanje procesov upravljanja organizacije, obvladovanja tveganj in kontrolnih procesov. Glede na Model treh linij je upravljanje povezano z organom nadzora, obvladovanje tveganj z drugo linijo, kontrole ali kontrolni procesi pa s prvo linijo. Medtem ko je poslovodstvo zastopano v prvi in drugi liniji, je funkcija notranje revizije prikazana v tretji liniji kot neodvisen in nepristranski dajalec zagotovil, ki poroča organu nadzora (Načelo 8 Nadzor organa nadzora).

Uporabnost, tveganje in strokovna presoja

Tematske zahteve je treba upoštevati, kadar notranja revizija izvaja posle dajanja zagotovil o predmetih, za katere obstaja tematska zahteva, ali kadar so vidiki Tematske zahteve pripoznani v drugih poslih dajanja zagotovil.

Kot je opisano v Standardih, je ocenjevanje tveganja pomemben del načrtovanja vodje notranje revizije. Določanje poslov dajanja zagotovil, ki jih je treba vključiti v načrt notranje revizije, zahteva ocenjevanje strategij, ciljev in tveganj organizacije vsaj enkrat letno (Standard 9.4 Načrt notranje revizije). Pri načrtovanju posameznih poslov dajanja zagotovil morajo notranji revizorji oceniti tveganja, primerna za posel (Standard 13.2 Ocena tveganj posla).

Kadar je predmet Tematske zahteve pripoznan med procesom načrtovanja notranje revizije, ki temelji na tveganju, in je vključena v revizijski načrt, je treba zahteve, opisane v tematski zahtevi, uporabiti za ocenjevanje teme v okviru primernih poslov. Poleg tega, ko notranji revizorji opravijo posel (bodisi vključen bodisi ne vključen v načrt) in se pojavijo gradniki Tematske zahteve, je treba Tematsko zahtevo oceniti glede njene uporabnosti v okviru posla. Nazadnje, če se zahteva posel, ki prvotno ni bil v načrtu in vključuje temo, je treba oceniti, ali je aktualna zahteva uporabna.

Strokovna presoja ima ključno vlogo pri uporabi Tematske zahteve. Ocene tveganj spodbujajo odločitve vodij notranjih revizij o tem, katere posle vključiti v načrt notranje revizije (Standard 9.4 Notranjerevizijski načrt). Poleg tega notranji revizorji uporabljajo strokovno presojo, da določijo, kateri vidiki bodo zajeti v vsakem poslu (standardi 13.3 Cilji in obseg posla, 13.4 Sodila za ocenjevanje in 13.6 Delovni program). Dodatek A "Primeri praktične uporabe" opisuje, kako notranji revizorji ugotavljajo, ali se tematska zahteva uporablja.

Ohraniti je treba dokazila, da je bila vsaka zahteva v Tematski zahtevi ocenjena z vidika uporabnosti, vključno z utemeljitvijo, ki pojasnjuje izključitev katere koli zahteve. Skladnost s tematsko zahtevo je treba dokumentirati z uporabo revizorjeve strokovne presoje, kot je opisano v Standardu 14.6 Dokumentacija o poslu.

Medtem ko tematska zahteva o kibernetski varnosti zagotavlja izhodišče kontrolnih procesov, ki jih je treba upoštevati, bodo organizacije, ki ocenjujejo kibernetsko tveganje kot zelo visoko, morda morale oceniti dodatne vidike.

Če vodja notranja revizije ugotovi, da služba notranje revizije nima zahtevanega znanja za izvajanje revizijskih poslov o predmetu Tematskih zahtev, se lahko posel odda v zunanje izvajanje (Standardi 3.1 Usposobljenost, 7.2 Kvalifikacije vodje notranje revizije, 10.2 Ravnanje s človeškimi viri). Tudi v tem primeru zunanje izvajanje ne odvezuje funkcije notranje revizije odgovornosti za skladnost s Temeljnimi zahtevami. Vodja notranje revizije ohrani končno odgovornost za zagotavljanje skladnosti. Poleg tega mora vodja notranje revizije, če ugotovi, da so viri notranje revizije nezadostni , obvestiti organ nadzora o vplivu nezadostnih virov in o tem, kako bo odpravil morebitni primanjkljaj virov (Standard 8.2 Viri).

Izvajanje, dokumentiranje in poročanje

Pri uporabi Tematskih zahtev morajo notranji revizorji ravnati v skladu s Standardi in svoje delo opravljati v skladu s Področjem V: Izvajanje notranjerevizijskih storitev. Standardi na Področju V opisujejo načrtovanje poslov (Načelo 13 Uspešno načrtujte posle), izvajanje poslov (Načelo 14 Izvedite posel) in sporočanje izidov poslov (Načelo 15 Sporočajte izide posla in spremljajte načrte ukrepanja).

Pokritje Tematske zahteve se lahko dokumentira v načrtu notranje revizije ali v delovnem gradivu posla na podlagi revizorjeve strokovne presoje. En ali več notranjerevizijskih poslov lahko pokriva zahteve. Poleg tega morda vse zahteve niso uporabne. Ohraniti je treba dokazila, da je bila ocenjena uporabnost tematske zahteve, vključno z utemeljitvijo, ki pojasnjuje morebitne izključitve.

Neobvezno orodje v Dodatku C se lahko uporablja kot referenca in za dokumentiranje dela, ki ga izvajajo notranji revizorji.

Zagotavljanje kakovosti

Standardi zahtevajo, da vodja notranje revizije razvije, izvaja in vzdržuje program zagotavljanja in izboljševanja kakovosti, ki zajema vse vidike notranje revizije (Standard 8.3 Kakovost). O izidih je treba obveščati organ nadzora in poslovodstvo. Sporočila morajo poročati o skladnosti funkcije notranje revizije s Standardi in doseganju ciljev poslovanja.

Skladnost s Tematskimi zahtevami se bo vrednotila pri ocenjevanju kakovosti. Za pripravo na presojo kakovosti lahko notranji revizorji uporabijo orodje iz Dodatka C.

Kibernetska varnost

Kibernetska varnost je široka tema, povezana z večino tehnoloških vidikov vsake organizacije. Poleg informacijske tehnologije je kibernetska varnost pogosto del poslovnih procesov, zaradi česar morajo notranji revizorji pri načrtovanju, določanju obsega in izvajanju storitev dajanja zagotovil oceniti tveganja, povezana s kibernetsko varnostjo.

Nacionalni inštitut za standarde in tehnologijo (NIST), ki je del ameriškega ministrstva za trgovino, kibernetsko varnost opredeljuje preprosto kot "sposobnost zaščititi ali obraniti uporabo kibernetskega prostora pred kibernetskimi napadi". Tematska zahteva o kibernetski varnosti se osredotoča na zunanji obod (parameter), ki ga organizacije zavarujejo, da bi zmanjšale tveganja pred nepooblaščenimi uporabniki in zlonamernimi kibernetskimi grožnjami. 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".

Zahteve tematske zahteve za kibernetsko varnost vključujejo:

- Upravljanje - jasno opredeljeni osnovni cilji in strategije kibernetske varnosti, ki podpirajo organizacijske cilje, politike in postopke.
- Obvladovanje tveganj - procesi za prepoznavanje, analiziranje, obvladovanje in spremljanje kibernetskih groženj, vključno s procesom za takojšnjo stopnjevanje kibernetskih tveganj.
- Kontrolni procesi - s strani vodstva vzpostavljeni in redno vrednoteni kontrolni procesi za zmanjšanje kibernetskega tveganja.

Preudarki

Notranji revizorji si lahko pri ocenjevanju zahtev iz tematske zahteve o kibernetski varnosti pomagajo z naslednjimi preudarki. Ti preudarki, ki se sklicujejo na zahteve, so revizorjem lahko v pomoč, vendar niso obvezni. Notranji revizorji se morajo pri odločanju, kaj naj vključijo v svoje vrednotenje, zanašati na strokovno presojo.

Preudarki o upravljanju

Da bi ocenili, kako se procesi upravljanja uporabljajo za cilje kibernetske varnosti, lahko notranji revizorji pregledajo:

A. Formaliziran, dokumentiran strateški načrt in cilji kibernetske varnosti, vključno z dokazili, da organ nadzora redno (običajno četrtletno) pregleduje posodobitve kibernetske varnosti, ki jih zagotovi vodja funkcije informacijske varnosti, kot npr. izvršni direktor za informacijsko varnost (CISO). Dokazila lahko vključujejo poročanje o:
   - spremljanju doseganja strateških ciljev.
   - proračunskih potrebah za podporo ciljem in dosežkom kibernetske varnosti.
   - Osredotočanju na tveganja in notranje kontrole, vključno z napredkom pri odpravljanju pomanjkljivosti.
   - Ključni kazalci uspešnosti (KPI) za merjenje uspeha.
   - Človeški viri, potrebni za zaposlovanje, usposabljanje in razvoj osebja za kibernetsko varnost.

B. Pravila, postopki in druga primerna dokumentacija, ki se uporablja za obvladovanje procesov kibernetske varnosti, vključno z:
   - politikami, ki se pregledajo in posodobijo vsaj enkrat na leto. Zaradi nastajajočih kibernetskih tveganj bo morda treba preglede in posodobitve izvajati pogosteje.
   - Postopek za ugotavljanje, ali so politike in postopki zadostni za podporo dejavnosti kibernetske varnosti.
   - Splošno sprejeti okviri (NIST, COBIT in drugi) za krepitev procesov kibernetske varnosti in notranjih kontrol.

C. Vloge in odgovornosti, ki podpirajo doseganje ciljev kibernetske varnosti, vključno s strukturo, ki zagotavlja, da funkcija kibernetske varnosti poroča na ravni v organizaciji, ki je dovolj vidna za doseganje organizacijske podpore.
   - Proces za obdobno ocenjevanje znanja, veščin in spretnosti osebja, ki opravlja naloge v zvezi s kibernetsko varnostjo.

D. Dokazila o sodelovanju s primernimi deležniki (na primer z vodstvom, poslovanje, obvladovanje tveganj, človeškimi viri, pravno službo, skladnostjo, strateškimi dobavitelji in drugimi), vključno s sporazumevanjem o obstoječih in nastajajočih kibernetskih tveganjih ter znanih morebitnih ranljivostih. Dokazila o sporazumevanju lahko vključujejo zapisnike sestankov, poročila ali elektronska sporočila.

Preudarki o obvladovanju tveganj

Da bi ocenili, kako se procesi obvladovanja tveganj uporabljajo za cilje kibernetske varnosti, lahko notranji revizorji pregledajo:

A. Kako organizacija ocenjuje in obvladuje tveganje kibernetske varnosti, vključno z načinom ocenjevanja groženj in ranljivosti, ki so bili:
   - Prvotno ugotovljeni in poročani.
   - Analizirani, da se oceni tveganje za doseganje ciljev organizacije.
   - Zmanjšani, vključno z načrti ukrepanja za zmanjšanje tveganja na sprejemljivo raven.
   - Spremljanji, vključno z načrtom za nenehno poročanje, dokler grožnje niso v celoti odpravljene.

B. Kako organizacija redno pridobiva podatke o obvladovanju tveganj kibernetske varnosti s funkcionalnih področij, kot so informacijska tehnologija, celovito obvladovanje tveganj, človeški viri, pravna služba, služba za zagotavljanje skladnosti, služba poslovanja, računovodstvo in finance. Za pridobivanje informacij se lahko uporablja medfunkcijska skupina za kibernetsko varnost ali usmerjevalni odbor za IT.

C. Kako je organizacija posamezniku ali skupini dodelila odgovornost za obvladovanje tveganj kibernetske varnosti.
   - Odgovorne osebe morajo redno (četrtletno, mesečno ali po potrebi) obveščati celotno organizacijo o nenehnih posodobitvah tveganj kibernetske varnosti in lahko vključujejo tudi zahteve po virih za strategije zmanjševanja tveganj.

D. Postopki stopnjevanja za tveganja kibernetske varnosti, vključno s tem, kako se vrednoti, dodeljuje in prednostno razvršča stopnja nevarnosti ali tveganja. Pregled lahko vključuje opredelitev:
   - Opredeljene ravni tveganja v organizaciji - kot so visoka, zmerna in nizka - s podrobnimi razlagami vsake ravni tveganja in postopki stopnjevanja za vsako kategorijo tveganja.
   - Seznam trenutno ugotovljenih tveganj za kibernetsko varnost in stanje blaženja vsakega dogodka tveganja.
   - Veljavne pravne in regulativne zahteve ter zahteve glede skladnosti.
   - Finančni in nefinančni (na primer ugled) vpliv tveganja.

E. Proces sporazumevanja vodstvu in zaposlenim o tveganjih kibernetske varnosti, ki vključuje:

- Obdobno (vsaj enkrat letno) usposabljanje zaposlenih o kibernetski varnosti, kot so nenapovedane igrane kampanje za lažno ribarjenje, s katerimi se preverja in spremlja organizacijska ozaveščenost.
- Posodobitve o odpravljanju obstoječih vprašanj s kibernetsko varnostjo s predvidenimi roki dokončanja.
- Spremljanje neskladnosti, ki vključuje posodobitve za organ nadzora in poslovodstvo.
- Ponovno ocenjevanje groženj, ko se spremenita nagnjenost organizacije k tveganju in toleranca do tveganja.

F. Procesi, ki jih je organizacija uvedla v zvezi z odzivanjem na incidente in okrevanjem, ki vključujejo:

- Dokumentiran načrt, ki se pregleduje in posodablja, ko se poslovanje organizacije sčasoma spremeni. Načrt mora vključevati:
  - Kako se incidenti odkrivajo in poročajo.
  - Kako se incidenti preprečujejo, da bi se preprečila nadaljnja škoda.
  - Kako bo organizacija okrevala in se odzvala za nadaljevanje poslovanja.
  - Kako bo incident analiziran, da se prepoznajo pridobljene izkušnje in kako preprečiti podobne dogodke v prihodnosti.
- Obdobno (vsaj enkrat letno) testiranje (namizna vaja) in poročanje o izidih poslovodstvu in primernim deležnikom. Izidi testiranja so lahko načrti ukrepanja.

Preudarki kontrolnih procesov

Da bi ocenili, kako se kontrolni procesi uporabljajo za doseganje ciljev kibernetske varnosti, lahko notranji revizorji pregledajo:

A. Pristop višjega vodstva za vzpostavitev uspešnega okolja notranjega kontroliranja, vključno z:
- Ocenjevanje in vpeljava notranjih kontrol, potrebnih za zmanjševanje povečanih tveganj in zaščito občutljivih, kritičnih, osebnih ali zaupnih podatkov na podlagi procesa ocenjevanja organizacijskih tveganj.
- Določanje potreb po virih za vzdrževanje ključnih kontrol kibernetske varnosti.
- Upoštevanje kontrol, ki temeljijo na dobaviteljih, kot dela kontrolnega okolja, kar vključuje pregledovanje poročil o kontrolah organizacije storitev (SOC) dobaviteljev pred začetkom poslovnega odnosa in ves čas trajanja odnosa.
- Obdobno preverjanje, ali kontrole kibernetske varnosti delujejo na način, ki zmanjšuje tveganja in podpira doseganje ciljev kibernetske varnosti.
- Proces za odpravljanje pomanjkljivosti pri notranjem kontroliranju ali obravnavanje ugotovitev iz ocen, ki jih opravi notranja revizija ali drugi izvajalci storitev dajanja zagotovil (na primer penetracijsko testiranje).

B. Proces organizacije za obvladovanje talentov za zaposlovanje in usposabljanje strokovnjakov za kibernetsko varnost, vključno s tem, kako organizacija ugotavlja priložnosti za povečanje usposobljenosti strokovnjakov za kibernetsko varnost za podporo tehničnega znanja in izboljšanje organizacijskega zavedanja o nastajajočih vprašanjih.
   - Primeri vključujejo udeležbo na usposabljanjih, sodelovanje v skupinah za izmenjavo znanja in stalno strokovno izobraževanje, ki vključuje pridobitev strokovnih poverilnic, povezanih s kibernetskim področjem.

C. Proces vodstva za stalno (continutous) prepoznavanje, določanje prednostnih nalog, spremljanje in poročanje o nastajajočih grožnjah in ranljivostih kibernetske varnosti, ki je osredotočen na vsakodnevno poslovanje. Pregled lahko vključuje, da so vzpostavljeni procesi za ocenjevanje groženj in ranljivosti, povezanih z novimi ali nastajajočimi tehnologijami, kot je uporaba umetne inteligence.

D. Procesi in kontrole vodstva, vzpostavljeni za obvladovanje in zaščito sredstev IT v celotnem življenjskem ciklu, vključno z izbiro, uporabo, vzdrževanjem in razgradnjo strojne in programske opreme ter storitev dobaviteljev. Strojna oprema vključuje strežnike, omrežno opremo (kot so usmerjevalniki ali požarni zidovi), namizne in prenosne računalnike, mobilne telefone, tablične računalnike in obrobne (periferne) naprave. Programska oprema vključuje operacijske sisteme (na primer Windows), programsko opremo za načrtovanje virov organizacije, aplikacije, protivirusne programe in drugo. Strojna in programska oprema lahko vključuje naslednje vidike:
   - Uporaba šifriranja, protivirusne programske opreme, obvladovanja mobilnih naprav, zahtev po kompleksnih geslih, navideznega zasebnega omrežja (VPN)/omrežja brez zaupanja (ZTN) za preverjanje pristnosti in obdobnega posodabljanja programske opreme naprave (firmware).
   - Proces obvladovanja sredstev, ki zagotavlja, da ima strojna oprema, ki jo izda podjetje, ustrezno varnostno konfiguracijo ob izdaji in ustrezno odstranitev ob upokojitvi sredstev.
   - Kontrole, povezane s podatkovnimi bazami, ki vključujejo omejevanje dostopa uporabnikov in skrbnikov, zagotavljanje uporabe šifriranja, varnostno kopiranje in testiranje podatkovnih baz ter prisotnost močnih kontrol varnosti omrežja.
   - Kako se grožnje in ranljivosti kibernetske varnosti upoštevajo v življenjskem ciklu razvoja sistema (SDLC).
   - Pristop, ki ga uporabljajo razvoj, varnost in operacije (DevSecOps) za zagotavljanje, da proces razvoja programske opreme vključuje kibernetsko varnost za proaktivno prepoznavanje ranljivosti.

E. Procesi, ki se uporabljajo za krepitev kibernetske varnosti, vključno z:
   - Konfiguracija varnostnih nastavitev za zmanjšanje tveganja kibernetske varnosti.
   - Administracija mobilne naprave (vključno z uporabo e-pošte in aplikacij) je konfigurirano tako, da zmanjšuje tveganja za kibernetsko varnost in se obvladuje na daljavo, če je uporabnikova naprava ogrožena.

- Uporaba šifriranja za podatke "v mirovanju", kot so podatki, shranjeni na trdem disku, ali podatke "v prenosu", kot je šifriranje e-pošte.
- Popravek (patch) strežnikov ali programske opreme (na primer operacijskega sistema) z najnovejšimi varnostnimi izdajami.
- Obvladovanje dostopa uporabnikov, kot je uporaba večfaktorske avtentikacije (MFA) in edinstvenih uporabniških identifikatorjev z zapletenimi gesli, ki obdobno potečejo.
- Vzpostavljene nadzorne kontrole za ugotavljanje, ali razpoložljivost in uporaba izraba virov ustrezno delujeta, kar omogoča pregled in analizo morebitnih vprašanj kibernetske varnosti, ki ogrožajo delovanje.
- Vključitev kibernetske varnosti v proces SDLC za prepoznavanje in odpravljanje ranljivosti kibernetske varnosti, preden se programska oprema prenese v živo (produkcijo).

F. Kontrole, povezane z omrežjem, ki varuje območje organizacije, vključno s tem, kako organizacija uporablja:
   - Segmentacijo omrežja.
   - Požarne zidove.
   - Nadzor dostopa uporabnika.
   - Omejitve za zunanje in notranje povezave.
   - Nadzor interneta stvari (IoT) za medsebojno povezana omrežja.
   - Sistemi za odkrivanje/preprečevanje vdorov za preprečevanje, odkrivanje in okrevanje po napadih na kibernetsko varnost.

G. Kontrole nad varnostnimi kontrolami končne komunikacijske točke, ki veljajo za storitve, kot so e-pošta, spletni brskalniki, videokonference, sporočanje (Zoom, MS Teams in drugi), družabni mediji, oblaki in protokoli za izmenjavo datotek. Kontrole lahko vključujejo omejevanje uporabe nekaterih razširitev datotek (kot so datoteke .exe) in večfaktorsko preverjanje pristnosti za izmenjavo datotek.

Dodatek A. Primeri praktične uporabe

Naslednji primeri opisujejo scenarije, v katerih bi se uporabljala Tematska zahteva o kibernetski varnosti:

Primer 1: Kibernetska varnost je opredeljena za notranjerevizijski posel, ki je vključen v notranjerevizijski načrt.

Ko notranja revizija zaključi proces načrtovanja na podlagi tveganj in vključi v notranjerevizijski načrt enega ali več poslov na področju kibernetske varnosti, je pri izvajanju takih poslov obvezno upoštevati tematsko zahtevo. Skladnost se lahko doseže z vključitvijo zahtev pri enem ali več poslih v notranjerevizijski načrt.

Kibernetska varnost je široka tema in vsaka zahteva v tematski zahtevi ne velja za vsak posel. Kadar notranji revizorji uporabijo strokovno presojo in ugotovijo, da ena ali več zahtev iz Tematske zahteve kibernetske varnosti niso uporabne in jih je zato treba izključiti iz posla, morajo notranji revizorji dokumentirati in hraniti utemeljitev za izključitev teh zahtev. Utemeljitev za izključitev nekaterih zahtev je lahko na primer ta, da služba notranje revizije izvaja različne posle kibernetske varnosti po načelu rotacije ali da je ugotovila, da je pomembnost tveganja v poslu majhna.

Primer 2: Tveganja kibernetske varnosti so ugotovljena med revizijskim poslom, ki ni osredotočen na kibernetsko varnost.

Notranji revizorji lahko ugotovijo tveganja kibernetske varnosti med ocenjevanjem procesa, ki ni neposredno povezan s kibernetsko varnostjo. Notranji revizorji lahko na primer ocenjujejo proces plačevanja računov pri poslovanju, ki ni osredotočen na kibernetsko varnost, in pri načrtovanju posla tveganj kibernetske varnosti ne opredelijo kot del obsega. Vendar po izvedbi začetnega sprehajalnega preizkusa notranji revizorji ugotovijo, da bi morala biti takšna tveganja v obsegu posla; na primer ugotovijo tveganja kibernetske varnosti, povezana s spletno oddajo začetnega zahtevka za naročilo (Standard 13.2 Ocena tveganj posla).

Ko so opredeljena primerna tveganja, morajo notranji revizorji pregledati Tematsko zahtevo o kibernetski varnosti in ugotoviti, katere zahteve se uporabljajo. V tem primeru lahko izključijo proces upravljanja kibernetske varnosti ali proces obvladovanja tveganj kibernetske varnosti. V delovnem gradivu posla morajo dokumentirati utemeljitev izključitve drugih zahtev iz Tematske zahteve o kibernetski varnosti in dokumentacijo hraniti.

Primer 3: Zahteva se posel kibernetske varnosti, ki prvotno ni bil vključen v načrt notranje revizije.

Deležniki, kot so organ nadzora, višje vodstvo ali regulator, lahko notranje revizorje zaprosijo, da izvedejo oceno kibernetske varnosti zunaj prvotnega revizijskega načrta. Na primer, ko so organizacije tarča kibernetskega napada, lahko organ nadzora zahteva izvedbo posla za oceno kontrol kibernetske varnosti. Tudi v tem primeru notranji revizorji uporabijo to Tematsko zahtevo in v njej opredeljene zahteve je treba oceniti, morebitne izključitve pa dokumentirati.

Dodatek B. Upoštevanje okvirov

Organizacija lahko na podlagi lastnih prizadevanj za kibernetsko varnost uporablja okvirje za obvladovanje tveganj in upravljanje organizacij, kot sta COBIT ali NIST. Notranji revizorji so morda že razvili revizijske programe in postopke preizkušanja na podlagi teh okvirov. Notranji revizorji naj uskladijo svoje načrtovano preizkušanje kontrol kibernetske varnosti s Tematsko zahtevo, da zagotovijo zadostno pokritost. V spodnji preglednici je Tematska zahteva o kibernetski varnosti prikazana s tremi pogosto uporabljenimi okviri: NIST Cybersecurity Framework 2.0, COBIT 2019 in NIST 800-53. Ta ogrodja so bila prikazana, ker so na voljo brez stroškov.

Zahteve za upravljanje	Okvirne reference		
	NIST CSF 2.0	NIST 800-53	COBIT 2019
A. Vzpostavljena je uradna strategija kibernetske varnosti in cilji, ki se obdobno posodabljajo. Posodobitve o doseganju ciljev kibernetske varnosti se redno sporočajo, organ nadzora pa jih pregleda, vključno z viri in proračunskimi vidiki za podporo strategiji kibernetske varnosti.	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. Politike in procesi, povezani s kibernetsko varnostjo, so vzpostavljeni in se obdobno posodabljajo ter krepijo kontrolno okolje.	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. Določene so vloge in odgovornosti, ki podpirajo cilje kibernetske varnosti, ter proces za obdobno ocenjevanje znanja, spretnosti in sposobnosti tistih, ki te vloge opravljajo.	GV.RR-02; GV.RR-04; GV.SC-02; GV.OC-02	PM-13; AT-2; AT-3	EDM02; APO01; APO07

D. Primerni deležniki so vključeni v razpravo o obstoječih ranljivostih in novih grožnjah v okolju kibernetske varnosti ter v ukrepanje v zvezi z njimi. Deležnike vključuje poslovodstvo, poslovanje, obvladovanje tveganj, človeške vire, pravno službo, skladnost s predpisi, dobavitelje in druge.	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
Zahteve za obvladovanje tveganj	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A. Procesi organizacije za ocenjevanje in obvladovanje tveganj vključujejo prepoznavanje, analizo, zmanjševanje in spremljanje groženj kibernetski varnosti ter njihovega učinka na doseganje strateških ciljev.	GV.RM-01; GV.RM-03; GV.OC-01	AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
B. Obvladovanje tveganja kibernetske varnosti se izvaja v celotni organizaciji, kar lahko vključuje naslednja področja: informacijsko tehnologijo, celovito obvladovanje tveganj, človeške vire, pravne zadeve, skladnost, poslovanje, dobavno verigo, računovodstvo, finance in druge.	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. Določena je odgovornost za obvladovanje tveganj kibernetske varnosti in posameznik ali skupina, ki obdobno spremlja in poroča, kako se obvladujejo tveganja kibernetske varnosti, vključno z viri, potrebnimi za zmanjšanje tveganja in prepoznavanje novih groženj kibernetske varnosti.	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. Vzpostavljen je proces za hitro stopnjevanje vseh tveganj kibernetske varnosti (nastajajočih ali predhodno ugotovljenih), ki se na podlagi vzpostavljenih smernic organizacije za obvladovanje tveganj ali zaradi skladnosti z veljavnimi zakonskimi in regulativnimi zahtevami dvignejo na nesprejemljivo raven. Upoštevati je treba tako finančne kot nefinančne vplive tveganja kibernetske varnosti.	GV.RM; ID.RA; RS.MA-04	CA-7; RA-3; RA-7	EDM03; APO01, APO10; APO12
E. Vzpostavljen je proces za ozaveščanje vodstva in zaposlenih o tveganju kibernetske varnosti ter za obdobni pregled vprašanj, vrzeli, pomanjkljivosti ali napak pri nadzoru s poročanjem in odpravljanjem pomanjkljivosti s strani vodstva.	PR.AT; GV.RR.01; GV.RR-04; GV.PO	AT-2	APO01; APO02; EDM03; MEA03
F. Organizacija je vpeljala proces odzivanja na incidente kibernetske varnosti in sanacije, ki vključuje odkrivanje, obvladovanje, sanacijo in analizo po incidentu. Proces odzivanja na incidente in okrevanja se obdobno preizkuša.	RS; RC	IR-4; IR-5; IR-6; IR-7; IR-8; IR-10; SA-15	DSS02; DSS03; DSS04; DSS05.07
Zahteve kontrolnih procesov	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A. Vzpostavljen je proces, ki zagotavlja, da so vzpostavljene notranje kontrole in kontrole s strani dobaviteljev za zaščito zaupnosti, celovitosti in razpoložljivosti sistemov in podatkov organizacije. Kontrole se obdobno ocenjujejo, da se ugotovi, ali delujejo na način, ki spodbuja doseganje organizacijskih ciljev kibernetske varnosti in pravočasno reševanje vprašanj.	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. Vzpostavljen in obdobno pregledovan je proces obvladovanja talentov za delovne korake kibernetske varnosti, ki vključuje možnosti usposabljanja za razvoj in ohranjanje tehničnih kompetenc.	PR.AT-01; PR.AT-02; GV.RR-03	AT-2; AT-3; IR-2; PM-14	APOO7; DSS04
C. Vzpostavljen je proces za nenehno spremljanje in poročanje o nastajajočih grožnjah in ranljivostih kibernetske varnosti ter za prepoznavanje, prednostno razvrščanje in izvajanje priložnosti za izboljšanje kibernetske varnosti.	ID.RA-02; ID.RA-03, ID.RA-04	CA-7; PM-31; RA-5	DSS03.05
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.	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. Vzpostavljeni so procesi za spodbujanje kibernetske varnosti, vključno s konfiguracijo, obvladovanjem naprav za končne uporabnike, šifriranjem, popravki, obvladovanjem dostopa uporabnikov ter spremljanjem razpoložljivosti in učinkovitosti. Kibernetska varnost je vključena v razvoj programske opreme (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. Vzpostavljene so kontrole, povezane z omrežjem, kot so kontrole dostopa do omrežja in segmentacija, uporaba in postavitev požarnih pregrad, omejene povezave iz zunanjih omrežij in z njimi, navidezno zasebno omrežje (VPN)/dostop do omrežja brez zaupanja (ZTNA), vključitev omrežnih kontrol interneta stvari (IoT) ter sistemov za odkrivanje/preprečevanje vdorov (IDS in IPS).	PR.IR; DE.CM-01	AC-6; AC-17; AC-18; AC-20; SC-7; SC-10; CA-8	DSS05.02

G. Vzpostavljen je varnostni nadzor sporazumevanja na končni točki v zvezi s storitvami, kot so e-pošta, spletni brskalniki, videokonference, sporočanje, družabni mediji, oblaki in protokoli za izmenjavo datotek.	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

Dodatek C. Izbirno orodje za dokumentacijo

Od notranjih revizorjev se pričakuje strokovna presoja pri določanju uporabnosti zahtev na podlagi ocene tveganj in primerno dokumentiranje izključitev nekaterih zahtev. Tematska zahteva se lahko dokumentira v načrtu notranje revizije ali v delovnem gradivu posla na podlagi revizorjeve strokovne presoje. Zahteve lahko zajema en ali več notranjerevizijskih poslov. Poleg tega morda ne bo mogoče uporabiti vseh zahtev. Spodnji obrazec za tiskanje zagotavlja eno od možnosti za dokumentiranje skladnosti s tematsko zahtevo kibernetske varnosti, vendar njegova uporaba ni obvezna.

Kibernetska varnost - upravljanje

Zahteva	Izvedeno kritje ali utemeljitev izključitve	Sklic na dokumentacijo
A. Vzpostavljena je uradna strategija kibernetske varnosti in cilji, ki se obdobno posodabljajo. Posodobitve o doseganju ciljev kibernetske varnosti se redno sporočajo, organ nadzora pa jih pregleda, vključno z viri in proračunskimi vidiki za podporo strategiji kibernetske varnosti.		
B. Politike in procesi, povezani s kibernetsko varnostjo, so vzpostavljeni in se obdobno posodabljajo ter krepijo kontrolno okolje.		
C. Določene so vloge in odgovornosti, ki podpirajo cilje kibernetske varnosti, ter proces za obdobno ocenjevanje znanja, spretnosti in sposobnosti tistih, ki te vloge opravljajo.		
D. Primerni deležniki so vključeni v razpravo o obstoječih ranljivostih in novih grožnjah v okolju kibernetske varnosti ter v ukrepanje v zvezi z njimi. Deležnike vključuje poslovodstvo, poslovanje, obvladovanje tveganj, človeške vire, pravno službo, skladnost s predpisi, dobavitelje in druge.		

Kibernetska varnost - obvladovanje tveganj

Zahteva	Izvedeno kritje ali utemeljitev izključitve	Sklic na dokumentacijo
A. Procesi organizacije za ocenjevanje in obvladovanje tveganj vključujejo prepoznavanje, analizo, zmanjševanje in spremljanje groženj kibernetski varnosti ter njihovega učinka na doseganje strateških ciljev.		
B. Obvladovanje tveganja kibernetske varnosti se izvaja v celotni organizaciji, kar lahko vključuje naslednja področja: informacijsko tehnologijo, celovito obvladovanje tveganj, človeške vire, pravne zadeve, skladnost, poslovanje, dobavno verigo, računovodstvo, finance in druge.		
C. Določena je odgovornost za obvladovanje tveganj kibernetske varnosti in posameznik ali skupina, ki obdobno spremlja in poroča, kako se obvladujejo tveganja kibernetske varnosti, vključno z viri, potrebnimi za zmanjšanje tveganja in prepoznavanje novih groženj kibernetske varnosti.		
D. Vzpostavljen je proces za hitro stopnjevanje vseh tveganj kibernetske varnosti (nastajajočih ali predhodno ugotovljenih), ki se na podlagi vzpostavljenih smernic organizacije za obvladovanje tveganj ali zaradi skladnosti z veljavnimi zakonskimi in regulativnimi zahtevami dvignejo na nesprejemljivo raven. Upoštevati je treba tako finančne kot nefinančne vplive tveganja kibernetske varnosti.		

Zahteva	Izvedeno kritje ali utemeljitev izključitve	Sklic na dokumentacijo
E. Vzpostavljen je proces za ozaveščanje vodstva in zaposlenih o tveganju kibernetske varnosti ter za obdobni pregled vprašanj, vrzeli, pomanjkljivosti ali napak pri nadzoru s poročanjem in odpravljanjem pomanjkljivosti s strani vodstva.		
F. Organizacija je vpeljala proces odzivanja na incidente kibernetske varnosti in sanacije, ki vključuje odkrivanje, obvladovanje, sanacijo in analizo po incidentu. Proces odzivanja na incidente in okrevanja se obdobno preizkuša.		

Kibernetska varnost - kontrolni procesi

Zahteva	Izvedeno kritje ali utemeljitev izključitve	Sklic na dokumentacijo
A. Vzpostavljen je proces, ki zagotavlja, da so vzpostavljene notranje kontrole in kontrole s strani dobaviteljev za zaščito zaupnosti, celovitosti in razpoložljivosti sistemov in podatkov organizacije. Kontrole se obdobno ocenjujejo, da se ugotovi, ali delujejo na način, ki spodbuja doseganje organizacijskih ciljev kibernetske varnosti in pravočasno reševanje vprašanj.		
B. Vzpostavljen in obdobno pregledovan je proces obvladovanja talentov za delovne korake kibernetske varnosti, ki vključuje možnosti usposabljanja za razvoj in ohranjanje tehničnih kompetenc.		

Zahteva	Izvedeno kritje ali utemeljitev izključitve	Sklic na dokumentacijo
C. Vzpostavljen je proces za nenehno spremljanje in poročanje o nastajajočih grožnjah in ranljivostih kibernetske varnosti ter za prepoznavanje, prednostno razvrščanje in izvajanje 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 spodbujanje kibernetske varnosti, vključno s konfiguracijo, obvladovanjem naprav za končne uporabnike, šifriranjem, popravki, obvladovanjem dostopa uporabnikov ter spremljanjem razpoložljivosti in učinkovitosti. Kibernetska varnost je vključena v razvoj programske opreme (DevSecOps).		
F. Vzpostavljene so kontrole, povezane z omrežjem, kot so kontrole dostopa do omrežja in segmentacija, uporaba in postavitev požarnih pregrad, omejene povezave iz zunanjih omrežij in z njimi, navidezno zasebno omrežje (VPN)/dostop do omrežja brez zaupanja (ZTNA), vključitev omrežnih kontrol interneta stvari (IoT) ter sistemov za odkrivanje/preprečevanje vdorov (IDS in IPS).		

Zahteva	Izvedeno kritje ali utemeljitev izključitve	Sklic na dokumentacijo
G. Vzpostavljen je varnostni nadzor sporazumevanja na končni točki v zvezi s storitvami, kot so e-pošta, spletni brskalniki, videokonference, sporočanje, družabni mediji, oblaki 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®). IIA je bilo ustanovljeno leta 1941 in je globalno priznano kot vodilno združenje na področju standardov, strokovnih nazivov, izobraževanja, raziskav in tehničnega vodenja notranje revizije. Za več informacij www.theiia.org.

Izjava o omejitvi odgovornosti

IIA objavlja ta dokument v informativne in izobraževalne namene. To gradivo ni namenjeno zagotavljanju dokončnih odgovorov na posebne posamezne okoliščine in se kot tako uporablja le kot priročnik. Organ IIA priporoča, da poiščete neodvisen strokovni nasvet, ki se neposredno nanaša na vsako posamezno okoliščino. Organ IIA ne prevzema nobene odgovornosti za nikogar, ki se zanaša izključno na to gradivo.

Avtorske pravice

Februar 2025

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