Kibernetička sigurnost

Topical Requirement

Tematski zahtjev

Korisnički vodič

The Institute of
Internal Auditors

Sadržaj

Pregled tematskih zahtjeva

Tematski zahtjevi obvezna su komponenta Međunarodnog okvira profesionalnog djelovanja (International Professional Practices Framework®), zajedno s Globalnim standardima interne revizije (Global Internal Audit Standards™) i Globalnim smjernicama. Institut internih revizora zahtijeva da se tematski zahtjevi koriste u kombinaciji s Globalnim standardima interne revizije, koji pružaju mjerodavnu razinu potrebnih praksi. Reference na Standarde pojavljuju se u ovom vodiču kao izvor detaljnijih informacija.

Tematski zahtjevi formaliziraju način na koji interni revizori pristupaju najčešćim područjima rizika kako bi promicali kvalitetu i dosljednost unutar profesije. Tematski zahtjevi uspostavljaju osnovu i daju mjerodavne kriterije za obavljanje usluga angažmana s izražavanjem uvjerenja koje se odnose na predmet tematskog zahtjeva (Standard 13.4 Kriteriji ocjenjivanja). Usklađenost s tematskim zahtjevima obavezna je za usluge izražavanja uvjerenja i preporučuje se za evaluaciju tijekom savjetodavnih usluga. Tematski zahtjevi nisu namijenjeni pokrivanju svih potencijalnih aspekata koje treba uzeti u obzir prilikom obavljanja angažmana s izražavanjem uvjerenja; naprotiv, namijenjeni su pružanju minimalnog skupa zahtjeva kako bi se omogućila dosljedna, pouzdana procjena teme.

Tematski zahtjevi jasno su povezani s trolinijskim modelom IIA-e i Globalnim standardima interne revizije. Korporativno upravljanje, upravljanje rizicima i kontrolni procesi glavne su komponente tematskih zahtjeva usklađenih sa Standardom 9.1 Razumijevanje procesa korporativnog upravljanja, upravljanja rizikom i kontrolnih procesa. U odnosu na model, korporativno upravljanje je povezano s odborom/upravnim tijelom, upravljanje rizicima povezano je s drugom linijom, a kontrole ili kontrolni procesi povezani su s prvom linijom. Dok je rukovodstvo zastupljeno u prvoj i u drugoj liniji, funkcija interne revizije je prikazana u trećoj liniji kao neovisni i objektivni pružatelj uvjerenja (eng. „*assurance provider*“), koji izvještava odbor (Načelo 8. Pod nadzorom Odbora).

Primjenjivost, rizik i profesionalna prosudba

Tematski zahtjevi moraju se poštivati kad funkcije interne revizije obavljaju angažmane s izražavanjem uvjerenja o predmetima za koje postoji tematski zahtjev ili kad su aspekti tematskog zahtjeva prepoznati unutar drugih angažmana s izražavanjem uvjerenja.

Kao što je opisano u Standardima, procjena rizika važan je dio planiranja rukovoditelja interne revizije. Kako bi se odredili angažmani s izražavanjem uvjerenja koje treba uključiti u plan interne revizije potrebno je izvršiti procjenu strategije organizacije, ciljeva i rizika najmanje jednom godišnje (Standard 9.4 Plan interne revizije). Prilikom planiranja pojedinačnih angažmana s izražavanjem uvjerenja, interni revizori moraju procijeniti rizike koji su bitni za angažman (Standard 13.2 Procjena rizika angažmana).

Kad je predmet tematskog zahtjeva prepoznat tijekom procesa planiranja interne revizije temeljenog na riziku i uključen je u plan revizije, tad se zahtjevi navedeni u tematskom zahtjevu moraju koristiti za procjenu teme unutar primjenjivih angažmana. Nadalje, kad interni revizori obave angažman (bilo uključen ili neuključen u plan) i pojave se elementi tematskog zahtjeva, mora biti ocjenjena njegova primjenjivost kao dio angažmana. Na kraju, ako se traži angažman koji izvorno nije bio u planu, a uključuje temu, mora se ocijeniti primjenjivost Tematskog zahtjeva.

Stručna prosudba igra ključnu ulogu u primjeni tematskog zahtjeva. Procjene rizika pokreću odluke rukovoditelja interne revizije o tome koje angažmane uključiti u plan interne revizije (Standard 9.4 Plan interne revizije). Dodatno, interni revizori koriste profesionalnu prosudbu kako bi odredili koji će aspekti biti pokriveni unutar svakog angažmana (Standardi 13.3 Ciljevi i opseg angažmana, 13.4 Kriteriji ocjenjivanja i 13.6 Program rada angažmana). Dodatak A “Primjeri praktične primjene” opisuje kako interni revizori određuju je li tematski zahtjev primjenjiv.

Dokaz da je primjenjivost svakog zahtjeva u tematskom zahtjevu procijenjena mora biti sačuvan, uključujući obrazloženje koje objašnjava isključenje bilo kojeg zahtjeva. Sukladnost s Tematskim zahtjevom mora se dokumentirati korištenjem profesionalne prosudbe revizora kako je opisano u Standardu 14.6 Dokumentacija angažmana.

Dok Tematski zahtjev za kibernetičku sigurnost pruža osnovu kontrolnih procesa koje treba razmotriti, organizacije koje kibernetički rizik procjenjuju kao vrlo visok možda će morati procijeniti i dodatne aspekte.

Ako rukovoditelj interne revizije utvrdi da funkcija interne revizije nema potrebno znanje za obavljanje revizijskih angažmana u skladu sa tematskim zahtjevom, rad na angažmanu može se prepustiti vanjskim izvođačima (Standardi 3.1 Kompetentnost, 7.2 Kvalifikacije rukovoditelja interne revizije, 10.2 Upravljanje ljudskim resursima). Čak ni tada, eksternalizacija ne oslobađa funkciju interne revizije od odgovornosti usklađivanja s tematskim zahtjevima. Rukovoditelj interne revizije zadržava krajnju odgovornost za osiguravanje sukladnosti. Nadalje, ako rukovoditelj interne revizije utvrdi da su resursi interne revizije nedostatni, mora obavijestiti odbor o učinku nedostatnih resursa i o tome kako će se svaki nedostatak resursa riješiti (Standard 8.2 Resursi).

Izvedba, dokumentacija i izvješćivanje

Prilikom primjene tematskih zahtjeva, interni revizori također se moraju pridržavati Standarda, obavljajući svoj rad u skladu s Domenom V: Obavljanje usluga interne revizije. Standardi u Domeni V opisuju planiranje angažmana (Načelo 13 Učinkovito planirajte angažmane), provođenje angažmana (Načelo 14 Provedite angažman) i komuniciranje rezultata angažmana (Načelo 15 Priopćite rezultate angažmana i pratite akcijske planove).

Pokrivenost tematskog zahtjeva može se dokumentirati ili u planu interne revizije ili u radnim dokumentima angažmana na temelju profesionalne prosudbe revizora. Jedan ili više angažmana interne revizije mogu pokriti zahtjeve. Osim toga, možda neće biti primjenjivi svi zahtjevi. Moraju se sačuvati dokazi da je primjenjivost tematskog zahtjeva procijenjena , uključujući obrazloženje koje objašnjava sve iznimke.

Izborni alat u Dodatku C može se koristiti kao referenca i za dokumentiranje posla koji obavljaju interni revizori.

Osiguranje kvalitete

Standardi zahtijevaju od rukovoditelja interne revizije da razvije, provede i održava program osiguranja kvalitete i poboljšanja koji pokriva sve aspekte funkcije interne revizije (Standard 8.3 Kvaliteta). Rezultati se moraju priopćiti odboru i višem menadžmentu. Komunikacije moraju izvještavati o usklađenosti funkcije interne revizije sa Standardima i postizanju ciljeva izvedbe.

Sukladnost s tematskim zahtjevima ocjenjivat će se u procjenama kvalitete. Interni revizori mogu koristiti alat koji se nalazi u Dodatku C kako bi se pripremili za pregled kvalitete.

Kibernetička sigurnost

Kibernetička sigurnost je široka tema povezana s najviše tehnoloških aspekata svake organizacije. Uz informacijsku tehnologiju, kibernetička sigurnost obično je dio poslovnih procesa, što zahtijeva da interni revizori procijene kibernetičke rizike prilikom planiranja, određivanja opsega i izvođenja angažmana s izražavanjem uvjerenja.

Nacionalni institut za standarde i tehnologiju (NIST), dio američkog Ministarstva trgovine, kibernetičku sigurnost definira jednostavno kao "Sposobnost zaštite ili obrane korištenja kibernetičkog prostora od kibernetičkih napada". Tematski zahtjev za kibernetičku sigurnost usredotočen je na vanjski perimetar koji organizacije osiguravaju kako bi ublažile rizike od neovlaštenih korisnika i zlonamjernih kibernetičkih prijetnji. Kibernetička sigurnost je podskup sveobuhvatne informacijske sigurnosti, koju NIST definira kao "Zaštitu informacija i informacijskih sustava od neovlaštenog pristupa, korištenja, otkrivanja, ometanja, izmjena ili uništenja, kako bi se osigurala povjerljivost, integritet i dostupnost".

Zahtjevi Tematskog zahtjeva za kibernetičku sigurnost uključuju:

- Korporativno upravljanje – jasno definirani osnovni ciljevi i strategije kibernetičke sigurnosti koji podržavaju organizacijske ciljeve, politike i procedure.
- Upravljanje rizicima – procesi za identifikaciju, analizu, upravljanje i praćenje kibernetičkih prijetnji, uključujući proces za brzu eskalaciju kibernetičkih rizika.
- Kontrole – kontrolni procesi koje je uspostavio menadžment, koji se periodički procjenjuju kako bi ublažili učinci kibernetičkih rizika.

Razmatranja

Interni revizori mogu koristiti sljedeća razmatranja kao pomoć pri procjeni zahtjeva u Tematskom zahtjevu kibernetičke sigurnosti. Ova razmatranja, koja su referencirana na zahtjeve, su ilustrativna, ali nisu obvezna. Interni revizori bi se trebali oslanjati na profesionalnu prosudbu kad određuju što će uključiti u svoje procjene.

Razmatranja korporativnog upravljanja

Kako bi procijenili na koji se način procesi korporativnog upravljanja primjenjuju na ciljeve kibernetičke sigurnosti, interni revizori mogu pregledati:

A. Formalizirani, dokumentirani strateški plan i ciljevi kibernetičke sigurnosti, uključujući dokaze da odbor povremeno (obično tromjesečno) pregledava ažuriranja kibernetičke sigurnosti koje daje voditelj funkcije informacijske sigurnosti, kao što je glavni službenik za informacijsku sigurnost (CISO). Dokazi mogu uključivati izvještavanje o:
   - Praćenju ostvarivanja strateških ciljeva.
   - Proračunskim potrebama za podršku ciljevima kibernetičke sigurnosti.
   - Fokusu na rizike i interne kontrole, uključujući napretku rješavanja.
   - Ključnim pokazateljima uspješnosti (KPI) za mjerenje uspjeha.
   - Ljudskim resursima koje je potrebno zaposliti, obučiti i razviti vezano uz kibernetičku sigurnost.

B. Politike, procedure i drugu važnu dokumentaciju koja se koristi za upravljanje procesima kibernetičke sigurnosti, uključujući:
   - Politike koje se pregledavaju i ažuriraju najmanje jednom godišnje. Novi i nadolazeći kibernetički rizici mogu zahtijevati češće preglede i ažuriranja.
   - Proces kojim se utvrđuje jesu li politike i procedure dovoljni za podršku operacijama kibernetičke sigurnosti.
   - Široko prihvaćeni okviri (NIST, COBIT i drugi) za jačanje procesa kibernetičke sigurnosti i internih kontrola.

C. Uloge i odgovornosti koje podržavaju postizanje ciljeva kibernetičke sigurnosti, uključujući strukturu koja osigurava da funkcija kibernetičke sigurnosti izvještava razinu u organizaciji koja ima dovoljno vidljivosti za postizanje organizacijske podrške.
   - Proces redovite procjene znanja, vještina i sposobnosti osoblja koje imaju ulogu u kibernetičkoj sigurnost.

D. Dokazi o suradnji s relevantnim dionicima (na primjer, višim rukovodstvom, operacijama, upravljanjem rizicima, ljudskim resursima, pravnicima, odjelom usklađenosti, strateškim dobavljačima i drugima), uključujući komunikaciju o postojećim i nadolazećim kibernetičkim rizicima i poznatim potencijalnim slabostima . Dokazi o komunikaciji mogu uključivati zapisnike sa sastanaka, izvješća ili e-poštu.

Razmatranja upravljanja rizicima

Kako bi procijenili na koji se način procesi upravljanja rizikom primjenjuju na ciljeve kibernetičke sigurnosti, interni revizori mogu pregledati:

A. Kako organizacija procjenjuje i upravlja rizikom kibernetičke sigurnosti, uključujući kako su prijetnje i ranjivosti :
   - Prvobitno ustanovljene i prijavljene.
   - Analizirane kako bi se procijenio rizik za postizanje organizacijskih ciljeva.
   - Ublažene, uključujući akcijske planove za smanjenje rizika na prihvatljivu razinu.
   - Praćene, uključujući plan za stalno izvješćivanje dok se prijetnje u potpunosti ne riješe.

B. Kako organizacija dobiva periodične podatke o upravljanju rizikom kibernetičke sigurnosti iz funkcionalnih područja, kao što su informacijska tehnologija, upravljanje rizicima poduzeća, ljudski resursi, pravni poslovi, usklađenost, operacije, računovodstvo i financije. Za dobivanje informacija može se koristiti višefunkcionalni tim za kibernetičku sigurnost ili IT upravni odbor (eng. „*steering comittee*“).

C. Kako je organizacija dodijelila odgovornosti (eng. „*accountability and responsibility*“) za upravljanje rizicima kibernetičke sigurnosti pojedincu ili timu.
   - Odgovorna(e) osoba(e) treba(ju) u redovnim vremenskim razdobljima (tromjesečno, mjesečno ili prema potrebi) izvještavati o trenutnim ažuriranjima rizika kibernetičke sigurnosti u cijeloj organizaciji, a mogu također uključiti zahtjeve za resursima za strategije ublažavanja rizika.

D. Procese eskalacije za rizike kibernetičke sigurnosti, uključujući kako se razina prijetnje ili rizika procjenjuje, dodjeljuje i kako joj se daje prioritet. Pregled može uključivati utvrđivanje:
   - Definirane razine rizika organizacije – kao što su visoka, umjerena i niska – s detaljnim objašnjenjima svake razine rizika i postupcima eskalacije za svaku kategoriju rizika.
   - Popis trenutačno utvrđenih rizika kibernetičke sigurnosti i status ublažavanja svakog rizičnog događaja.
   - Primjenjivih pravnih, regulatornih zahtjeva i zahtjeva usklađenosti.
   - Financijske i nefinancijske utjecaje rizika (na primjer reputacija).

E. Proces komuniciranja o rizicima kibernetičke sigurnosti menadžmentu i zaposlenicima, koji uključuje:
   - Periodičnu (barem jednom godišnje) obuku zaposlenika o kibernetičkoj sigurnosti, kao što su nenajavljene, simulirane „phishing“ kampanje za testiranje i praćenje organizacijske osviještenosti.
   - Ažuriranja o rješavaju postojećih problema kibernetičke sigurnosti, s predviđenim datumima završetka.
   - Praćenje neusklađenosti koje uključuje informiranje odbora i višeg menadžmenta.

- Ponovna procjena prijetnji kad se promijeni sklonost organizacije za prihvaćanje rizika te tolerancije na rizik.

F. Procesi koje je organizacija uvela kao odgovor na incident i oporavak, koji uključuju:

- Dokumentirani plan koji se pregledava i ažurira kako se poslovanje organizacije mijenja tijekom vremena. Plan bi trebao uključivati:
  - način na koji se incidenti otkrivaju i prijavljuju,
  - način na koji se incidenti ograničavaju kako bi se spriječila daljnja šteta,
  - način na koji će se organizacija oporaviti i odgovoriti kako bi nastavila s poslovanjem,
  - način na koji će se incident analizirati kako bi se ustanovile naučene lekcije (eng. „*lessons learned*“) i kako bi se spriječili slični budući događaji.
- Periodično (barem jednom godišnje) testiranje (“stolna vježba“, eng. „*tabletop excersize*“) i izvješćivanje o rezultatima višem menadžmentu i bitnim dionicima. Kao rezultat testiranja mogu proizaći akcijski planovi.

Razmatranja kontrolnih procesa

Kako bi procijenili kako se kontrolni procesi primjenjuju na ciljeve kibernetičke sigurnosti, interni revizori mogu pregledati:

A. Pristup menadžmenta u izgradnji učinkovitog internog kontrolnog okruženja kibernetičke sigurnosti, uključujući:
- Procjenu i provedbu internih kontrola potrebnih za ublažavanje povećanih rizika i zaštitu osjetljivih, kritičnih, osobnih ili povjerljivih podataka, na temelju procesa procjene rizika organizacije.
- Određivanje zahtjeva za resursima za održavanje ključnih kontrola kibernetičke sigurnosti.
- Razmatranje kontrola temeljenih na dobavljačima kao dijela kontrolnog okruženja, što uključuje pregled izvješća dobavljača o kontrolama uslužnih organizacija (eng. „*service organization controls*“) prije započinjanja poslovnog odnosa i tijekom trajanja odnosa.
- Periodično testiranje kontrola kibernetičke sigurnosti kako bi se ustanovilo funkcioniraju li na način koji umanjuje rizike i podupire postizanje ciljeva kibernetičke sigurnosti.
- Proces za otklanjanje nedostataka internih kontrola ili rješavanje nalaza iz procjena koje provodi funkcija interne revizije ili drugi pružatelji uvjerenja (na primjer, prilikom penetracijskih testiranja).

B. Proces kojim organizacija upravlja talentima kroz novačenje i obuku stručnjaka za kibernetičku sigurnost, uključujući način na koji organizacija prepoznaje mogućnosti

za povećanje kompetencija stručnjaka za kibernetičku sigurnost kako bi održali tehničko znanje i poboljšaju svijest organizacije o novim i nadolazećim problemima.
    - Primjeri uključuju sudjelovanje u obuci, uključenost u grupe za razmjenu znanja i kontinuirano profesionalno obrazovanje koje uključuje stjecanje certifikata povezanih s kibernetičkom sigurnošću.

C. Proces identifikacije, određivanja prioriteta, praćenja i izvještavanja o novim i nadolazećim prijetnjama i ranjivostima vezanim uz kibernetičku sigurnost koji je usmjeren na svakodnevne operacije. Pregled može uključivati uspostavu procesa za procjenu prijetnji i ranjivosti povezanih s novim tehnologijama ili tehnologijama u nastajanju kao što je upotreba umjetne inteligencije.

D. Upravljački procesi i kontrole uspostavljeni za upravljanje i zaštitu IT imovine tijekom životnog ciklusa, uključujući odabir, korištenje, održavanje i prestanak korištenja hardvera, softvera i usluga dobavljača. Hardver uključuje poslužitelje, mrežnu opremu (kao što su usmjerivači ili vatrozidi), stolna računala, prijenosna računala, mobitele, tablete i periferne uređaje. Softver uključuje operativne sustave (kao što je Windows), softver za planiranje poslovnih resursa, aplikacije, antivirusne programe i druge. Razmatranja hardvera i softvera mogu uključivati:
    - Korištenje enkripcije, antivirusnog softvera, upravljanja mobilnim uređajima, korištenje složenih zaporki, virtualne privatne mreže (VPN)/mreže s nultim povjerenjem (eng. „*zero trust networking*“, ZTN) za provjeru autentičnosti i povremeno ažuriranje firmvera.
    - Proces upravljanja imovinom koji osigurava da hardver koji tvrtka izdaje ima odgovarajuću sigurnosnu konfiguraciju nakon izdavanja i pravilnog odlaganja kad se imovina povuče iz upotrebe.
    - Kontrole baze podataka koje uključuju ograničavanje korisničkog i administratorskog pristupa, osiguravanje korištenja enkripcije, izrade sigurnosnih kopija i testiranje baza podataka te prisutnost snažnih mrežnih sigurnosnih kontrola.
    - Način na koji se prijetnje ili ranjivosti kibernetičke sigurnosti razmatraju u životnom ciklusu razvoja sustava (SDLC).
    - Pristup koji koriste razvoj, sigurnost i operacije (DevSecOps) kako bi se osiguralo da proces razvoja softvera uključuje kibernetičku sigurnost za proaktivno prepoznavanje ranjivosti.

E. Procesi koji se koriste za jačanje kibernetičke sigurnosti, uključujući:
    - Konfiguraciju sigurnosnih postavki za smanjivanje rizika kibernetičke sigurnosti.
    - Administraciju mobilnih uređaja (uključujući korištenje e-pošte i aplikacija) konfiguriranu za ublažavanje rizika kibernetičke sigurnosti i omogućavanje daljinskog upravljanja ako je uređaj korisnika ugrožen.
    - Korištenje enkripcije za podatke "u mirovanju", kao što su informacije pohranjene na tvrdom disku, ili podatke "u prijenosu", kao što je enkripcija e-pošte.

- Ažuriranje poslužitelja ili softvera (kao što je operativni sustav) s najnovijim sigurnosnim izdanjima i zakrpama.
- Upravljanje korisničkim pristupom kao što je korištenje višefaktorske autentifikacije (engl. „*MFA*“) i jedinstvenih korisničkih identiteta (engl. „*ID*“) sa složenim zaporkama koje je potrebno periodički promijeniti.
- Kontrole praćenja koje su uspostavljene kako bi se utvrdilo jesu li dostupnost i korištenje odgovarajući, omogućujući pregled i analizu potencijalnih problema kibernetičke sigurnosti koji ugrožavaju performanse sustava.
- Integracija kibernetičke sigurnosti u životni ciklus razvoja sustava (engl. „*SDLC*“) za prepoznavanje i rješavanje ranjivosti kibernetičke sigurnosti prije nego što se softver premjesti u produkciju.

F. Mrežne kontrole koje osiguravaju perimetar organizacije, uključujući kako organizacija koristi:
   - Segmentaciju mreže.
   - Vatrozide.
   - Kontrole korisničkog pristupa.
   - Ograničenja i vanjskih i unutarnjih veza.
   - Kontrole koje okružuju Internet stvari (IoT) za međusobno povezane mreže.
   - Sustave za otkrivanje/prevenciju upada za sprječavanje, otkrivanje i oporavak od kibernetičkih napada.

G. Kontrole koje okružuju sigurnosne kontrole komunikacije krajnjih točaka (eng. endpoint) primjenjive na usluge kao što su e-pošta, internetski preglednici, videokonferencije, slanje poruka (Zoom, MS Teams i drugi), društvene medije, oblak i protokole za dijeljenje datoteka. Kontrole mogu uključivati ograničavanje upotrebe određenih ekstenzija datoteka (kao što su .exe datoteke) i višefaktorsku provjeru autentičnosti za dijeljenje datoteka.

Dodatak A. Primjeri praktične primjene

Sljedeći primjeri opisuju scenarije u kojima bi bio primjenjiv Tematski zahtjev kibernetičke sigurnosti:

Primjer 1: Kibernetička sigurnost utvrđena je za angažman interne revizije

Tematski zahtjev je obvezan prilikom provođenja angažmana interne revizije, kad funkcija interne revizije dovrši svoj proces planiranja temeljen na riziku i uključi jedan ili više angažmana u vezi s kibernetičkom sigurnošću u plan interne revizije. Sukladnost se može postići uključivanjem zahtjeva u jedan ili više angažmana u planu interne revizije.

S obzirom da je kibernetička sigurnost široka tema ne mora svaki zahtjev u Tematskom zahtjevu biti primjenjiv na svaki angažman. Kad interni revizori primijene profesionalnu prosudbu i utvrde da jedan ili više zahtjeva iz Tematskog zahtjeva kibernetičke sigurnosti nisu primjenjivi i da ih stoga treba isključiti iz angažmana, interni revizori moraju dokumentirati i sačuvati obrazloženje za izuzimanje tih zahtjeva. Na primjer, obrazloženje za izuzimanje nekih zahtjeva moglo bi biti to što funkcija interne revizije obavlja različite angažmane u području kibernetičke sigurnosti na rotacijskoj osnovi ili je utvrdila da je značaj rizika u angažmanu nizak.

Primjer 2: Rizici kibernetičke sigurnosti utvrđeni su tijekom revizijskog angažmana koji nije usredotočen na kibernetičku sigurnost.

Interni revizori mogu prepoznati rizike kibernetičke sigurnosti dok procjenjuju proces koji nije izravno povezan s kibernetičkom sigurnošću. Na primjer, interni revizori mogu procjenjivati proces plaćanja računa u angažmanu koji nije usredotočen na kibernetičku sigurnost i ne prepoznaju rizike kibernetičke sigurnosti unutar opsega prilikom planiranja angažmana. Međutim, nakon izvođenja početnog pregleda, interni revizori utvrđuju da bi takvi rizici trebali biti obuhvaćeni; na primjer, utvrđuju rizike kibernetičke sigurnosti povezane s podnošenjem početnog zahtjeva za kupnju putem interneta (Standard 13.2 Procjena rizika angažmana).

Nakon što se utvrde bitni rizici, interni revizori moraju pregledati Tematski zahtjev kibernetičke sigurnosti i odrediti koji su zahtjevi primjenjivi. U ovom primjeru mogli bi isključiti proces upravljanja kibernetičkom sigurnošću ili proces upravljanja rizicima kibernetičke sigurnosti. U radnoj dokumentaciji angažmana moraju dokumentirati obrazloženje za isključivanje drugih zahtjeva Tematskog zahtjeva kibernetičke sigurnosti i sačuvati dokumentaciju.

Primjer 3: Zatražen je angažman u području kibernetičke sigurnosti koji izvorno nije bio uključen u plan interne revizije .

Dionici kao što su odbor, menadžment ili regulator mogu zatražiti od internih revizora da izvrše procjene kibernetičke sigurnosti izvan izvornog plana revizije. Na primjer, kad su organizacije meta kibernetičkog napada, odbor može zatražiti angažman interne revizije kako bi se procijenile kontrole kibernetičke sigurnosti. Tematski zahtjev je primjenjiv, zahtjevi moraju biti procijenjeni, a sva isključenja dokumentirana.

Dodatak B. Preslikavanje u okvire

Organizacija može imati vlastita djelovanja u području kibernetičke sigurnosti, koristeći okvire za upravljanje rizicima i korporativno upravljanje kao što su COBIT ili NIST. Interni revizori možda su već razvili revizijske programe i postupke testiranja temeljene na tim okvirima. Interni revizori trebali bi uskladiti svoje planirano testiranje kontrola kibernetičke sigurnosti s Tematskim zahtjevom kako bi osigurali odgovarajuću pokrivenost. Tablica u nastavku prikazuje Tematski zahtjev kibernetičke sigurnosti na tri često korištena okvira: NIST Cybersecurity Framework 2.0, COBIT 2019 i NIST 800-53. Ovi su okviri mapirani jer su lako dostupni i besplatni.

Zahtjevi korporativnog upravljanja	Reference u okvirima		
	NIST CSF 2.0	NIST 800-53	COBIT 2019
A. Uspostavljena je i povremeno ažurirana službena strategija i ciljevi kibernetičke sigurnosti. Ažuriranja o postizanju ciljeva kibernetičke sigurnosti redovito se priopćuju i pregledavaju od strane odbora, uključujući resurse i proračunska razmatranja za podršku strategiji kibernetičke sigurnosti.	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 i procedure povezane s kibernetičkom sigurnošću uspostavljaju se, povremeno ažuriraju te jačaju kontrolno okruženje.	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. Uspostavljene su uloge i odgovornosti koje podupiru ciljeve kibernetičke sigurnosti, a postoji i postupak za povremenu procjenu znanja, vještina i sposobnosti onih koji ispunjavaju te uloge.	GV.RR-02; GV.RR-04; GV.SC-02; GV.OC-02	PM-13; AT-2; AT-3	EDM02; APO01; APO07

D. Odgovarajući dionici uključeni su u raspravu i djelovanje u vezi s postojećim ranjivostima i prijetnjama koje nastaju u okruženju kibernetičke sigurnosti. Zainteresirane strane uključuju više rukovodstvo, operacije, upravljanje rizikom, ljudske resurse, pravne poslove, usklađenost, dobavljače i 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
Zahtjevi upravljanja rizicima	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A. Procesi procjene rizika i upravljanja rizicima u organizaciji uključuju prepoznavanje, analizu, ublažavanje i praćenje kibernetičkih prijetnji i njihovog učinka na postizanje strateških ciljeva.	GV.RM-01; GV.RM-03; GV.OC-01	AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
B. Upravljanje rizicima kibernetičke sigurnosti provodi se u cijeloj organizaciji, što može uključivati sljedeća područja: informacijsku tehnologiju, upravljanje rizikom poduzeća, ljudske resurse, pravne poslove, usklađenost, operacije, lanac opskrbe, računovodstvo, financije i 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. Uspostavljena je odgovornost za upravljanje rizicima kibernetičke sigurnosti i prepoznata je osoba ili tim koji će povremeno nadzirati i izvještavati o tome kako se upravlja rizicima kibernetičke sigurnosti, uključujući resurse potrebne za ublažavanje rizika i prepoznavanje novih prijetnji kibernetičkoj sigurnosti.	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. Uspostavljen je postupak za brzu eskalaciju bilo kojeg rizika kibernetičke sigurnosti (koji se pojavljuje ili je prethodno prepoznat) koji se penje na neprihvatljivu razinu na temelju uspostavljenih smjernica organizacije za upravljanje rizikom ili radi usklađivanja s primjenjivim zakonskim i regulatornim zahtjevima. Pri tom treba uzeti u obzir i financijske i nefinancijske učinke rizika kibernetičke sigurnosti.	GV.RM; ID.RA; RS.MA-04	CA-7; RA-3; RA-7	EDM03; APO01, APO10; APO12
E. Uspostavljen je proces za prenošenje svijesti o rizicima kibernetičke sigurnosti menadžmentu i zaposlenicima, te za periodični pregled problema, nedostataka, nedostataka ili propusta kontrola od strane menadžmenta uz izvješćivanje i njihovo otklanjanje.	PRAT; GV.RR.01; GV.RR-04; GV.PO	AT-2	APO01; APO02; EDM03; MEA03
F. Organizacija je uvela odgovor na incidente kibernetičke sigurnosti i proces oporavka koji uključuje otkrivanje, ograničavanje utjecaja, oporavak i analizu nakon incidenta. Odgovor na incident i proces oporavka se povremeno testiraju.	RS; RC	IR-4; IR-5; IR-6; IR-7; IR-8; IR-10; SA-15	DSS02; DSS03; DSS04; DSS05.07

Zahtjevi kontrolnih procesa	NIST CSF 2.0	NIST 800-53	COBIT 2019
A. Uspostavljen je proces koji osigurava da su interne kontrole i kontrole koje se temelje na dobavljačima uspostavljene kako bi se zaštitila povjerljivost, integritet i dostupnost sustava i podataka organizacije. Kontrole se ocjenjuju u redovitim vremenskim razdobljima kako bi se utvrdilo funkcioniraju li na način koji promiče postizanje organizacijskih ciljeva kibernetičke sigurnosti i pravovremeno rješavanje problema.	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. Uspostavlja se proces upravljanja talentima koji se pregledava u redovnim vremenskim razdobljima za operacije kibernetičke sigurnosti, a uključuje mogućnosti obuke za razvoj i održavanje tehničkih kompetencija.	PR.AT-01; PR.AT-02; GV.RR-03	AT-2; AT-3; IR-2; PM-14	APOO7; DSS04
C. Uspostavljen je proces za kontinuirano praćenje i izvješćivanje o nastajanju prijetnji i ranjivosti kibernetičke sigurnosti te za prepoznavanje, određivanje prioriteta i uvođenje prilika za poboljšanje operacija kibernetičke sigurnosti.	ID.RA-02; ID.RA-03, ID.RA-04	CA-7; PM-31; RA-5	DSS03.05
D. Kibernetička sigurnost je uključena u upravljanje životnim ciklusom (odabir, korištenje, održavanje i stavljanje izvan korištenja) sve IT imovine, uključujući hardver, softver i usluge dobavljača.	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. Uspostavljeni su procesi za promicanje kibernetičke sigurnosti uključujući konfiguraciju, administraciju uređaja krajnjih korisnika, enkripciju, krpanje (eng. „*patching*“), upravljanje korisničkim pristupom te praćenje dostupnosti i performansi. Razmatranja kibernetičke sigurnosti uključena su u razvoj softvera (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. Uspostavljene su mrežne kontrole, kao što su kontrole pristupa mreži i segmentacija; korištenje i postavljanje vatrozida, ograničene veze od i prema vanjskim mrežama; virtualna privatna mreža (VPN)/mrežni pristup s nultim povjerenjem (eng. zero trust network access, ZTNA), uključivanje mrežnih kontrola Interneta stvari (IoT) i sustava za otkrivanje/sprečavanje upada (IDS i IPS).	PR.IR; DE.CM-01	AC-6; AC-17; AC-18; AC-20; SC-7; SC-10; CA-8	DSS05.02
G. Sigurnosne kontrole krajnjih točaka (eng. „*endpoint*“) komunikacije su uspostavljene za usluge kao što su e-pošta, internetski preglednici, videokonferencije, slanje poruka, društveni mediji, oblak i protokoli za dijeljenje datoteka.	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

Dodatak C. Izborni alat za dokumentaciju

Od internih revizora se očekuje profesionalna prosudba pri određivanju primjenjivosti zahtjeva na temelju procjene rizika i odgovarajuće dokumentiranje isključenja određenih zahtjeva. Tematski zahtjev može se dokumentirati u planu interne revizije ili u radnoj dokumentaciji angažmana na temelju profesionalne prosudbe revizora. Jedan ili više angažmana interne revizije mogu pokriti zahtjeve. Osim toga, možda neće biti primjenjivi svi zahtjevi. Obrazac za ispis u nastavku pruža jednu opciju za dokumentiranje usklađenosti s Tematskim zahtjevom kibernetičke sigurnosti, ali njegova upotreba nije obvezna.

Kibernetička sigurnost – korporativno upravljanje

Zahtjev	Izvršeno pokriće ili obrazloženje za isključenje	Referenca dokumentacije
A. Uspostavljena je i periodično ažurirana službena strategija i ciljevi kibernetičke sigurnosti. Ažuriranja o postizanju ciljeva kibernetičke sigurnosti periodično se priopćuju i pregledavaju od strane odbora, uključujući resurse i proračunska razmatranja za podršku strategiji kibernetičke sigurnosti.		
B. Politike i procedure vezane uz kibernetičku sigurnost uspostavljaju se, periodično ažuriraju i jačaju kontrolno okruženje.		
C. Uspostavljene su uloge i odgovornosti koje podržavaju ciljeve kibernetičke sigurnosti, a postoji i postupak za periodičku procjenu znanja, vještina i sposobnosti onih koji ispunjavaju te uloge.		
D. Bitni dionici uključeni su u raspravu i djelovanje u vezi s postojećim ranjivostima i prijetnjama koje nastaju i rastu u okruženju kibernetičke sigurnosti. Dionici uključuju više rukovodstvo, operacije, upravljanje rizikom, ljudske resurse, pravne poslove, usklađenost, dobavljače i druge.		

Kibernetička sigurnost – upravljanje rizicima

Zahtjev	Izvršeno pokriće ili obrazloženje za isključenje	Referenca dokumentacije
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 rizikom kibernetičke sigurnosti provodi se u cijeloj organizaciji i može uključivati sljedeća područja: informacijsku tehnologiju, upravljanje rizikom poduzeća, ljudske resurse, pravne poslove, usklađenost, operacije, lanac opskrbe, računovodstvo, financije i druga.		
C. Uspostavljena je odgovornost i odgovornost za upravljanje rizikom kibernetičke sigurnosti. Utvrđuje se osoba ili tim koji će periodično nadzirati i izvještavati o tome kako se upravlja rizicima kibernetičke sigurnosti, uključujući resurse potrebne za ublažavanje rizika i prepoznavanje novih prijetnji kibernetičkoj sigurnosti.		
D. Uspostavljen je postupak za brzu eskalaciju bilo kojeg rizika kibernetičke sigurnosti (koji se tek pojavljuje ili je prethodno utvrđen) 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.		

Zahtjev	Izvršeno pokriće ili obrazloženje za isključenje	Referenca dokumentacije
E. Uspostavljen je proces za prenošenje svijesti o riziku kibernetičke sigurnosti menadžmentu i zaposlenicima te za menadžment da povremeno pregleda probleme, nedostatke ili propuste u kontrolama uz pravovremeno izvješćivanje i rješavanje.		
F. Organizacija je uvela odgovor na incidente vezane uz kibernetičku sigurnost te proces oporavka, uključujući otkrivanje, obuzdavanje, oporavak i analizu nakon incidenta. Odgovor na incidente i proces oporavka periodično se testiraju.		

Kibernetička sigurnost – Kontrolni procesi

Zahtjev	Izvršeno pokriće ili obrazloženje za isključenje	Referenca dokumentacije
O. Uspostavljen je proces kako bi se osiguralo postojanje internih kontrola i kontrola dobavljača radi zaštite povjerljivosti, cjelovitosti i dostupnosti sustava i podataka organizacije. Procjene se provode periodično kako bi se utvrdilo funkcioniraju li kontrole na način koji promiče postizanje ciljeva kibernetičke sigurnosti organizacije i brzo rješavanje problema.		
B. Uspostavljen je proces upravljanja talentima koji uključuje obuku za razvoj i održavanje tehničkih kompetencija povezanih s operacijama kibernetičke sigurnosti. Proces se revidira u redovnim vremenskim razmacima.		

Zahtjev	Izvršeno pokriće ili obrazloženje za isključenje	Referenca dokumentacije
C. Uspostavljen je proces za kontinuirano praćenje i izvješćivanje o nastajanju prijetnji i ranjivosti kibernetičke sigurnosti te za prepoznavanje, određivanje prioriteta i uvođenje prilika za poboljšanje operacija kibernetičke sigurnosti.		
D. Kibernetička sigurnost je uključena u upravljanje životnim ciklusom (odabir, korištenje, održavanje i prestanak korištenja) sve IT imovine, uključujući hardver, softver i usluge dobavljača.		
E. Uspostavljeni su procesi za promicanje kibernetičke sigurnosti, uključujući konfiguraciju, administraciju uređaja krajnjih korisnika, enkripciju, krpanje (eng. „*patching*“), upravljanje korisničkim pristupom i praćenje dostupnosti i performansi. Razmatranja kibernetičke sigurnosti uključena su u razvoj softvera (DevSecOps).		
F . Uspostavljaju se mrežne kontrole , kao što su kontrole pristupa mreži i segmentacija; korištenje i postavljanje vatrozida; ograničene veze od i prema vanjskim mrežama; virtualna privatna mreža (VPN)/mrežni pristup s nultim povjerenjem (eng. „*zero trust network access*“, ZTNA), mrežne kontrole Interneta stvari (IoT) i sustavi za otkrivanje/sprečavanje upada (IDS i IPS).		
G. Sigurnosne kontrole krajnjih točaka (eng. endpoint) komunikacije 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 www.theiia.org.

Disclaimer

Copyright

February 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