Sajber bezbednost

Vodič za korisnike

Tematskog zahteva

Topical requirement

Prevedeno od strane:

The Institute of Internal Auditors

Udruženje internih revizora Srbije

Sadržaj

Pregled Tematskih zahteva 1

Primenljivost, rizik i profesionalna procena 1

Razmatranja 4

Dodatak A. Primeri praktične primene 9

Dodatak B. Mapiranje sa drugim okvirima.....11

Dodatak C. Opcioni alat za dokumentaciju.....15

Pregled Tematskih zahteva

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. Institut internih revizora zahteva da se Tematski zahtevi koriste zajedno sa Globalnim standardima interne revizije, koji obezbeđuju merodavnu osnovu zahtevane prakse. Reference na Standarde se pojavljuju u ovom Vodiču kao izvor detaljnijih informacija.

Tematski zahtevi formalizuju način na koji se interni revizori bave preovlađujućim područjima rizika kako bi promovisali kvalitet i doslednost u profesiji. Tematski zahtevi uspostavljaju osnovu i obezbeđuju relevantne kriterijume za pružanje usluga uveravanja u vezi sa predmetom Tematskog zahteva (Standard 13.4 Kriterijumi za vrednovanje). Usklađenost sa Tematskim zahtevima je obavezna za usluge uveravanja i preporučuje se za procenu tokom savetodavnih usluga. Tematski zahtevi nemaju za cilj da pokriju sve potencijalne aspekte koje treba uzeti u obzir prilikom sprovođenja angažmana uveravanja; umesto toga, oni imaju za cilj da obezbede minimalni skup zahteva koji omogućavaju doslednu, pouzdanu procenu teme.

Tematski zahtevi su jasno povezani sa Modelom tri linije IIA i Globalnim standardima interne revizije. Upravljanje organizacijom, upravljanje rizicima i kontrolni procesi su glavne komponente Tematskih zahteva usklađenih sa Standardom 9.1 Razumevanje upravljanja organizacijom, upravljanja rizicima i kontrolnih procesa. U odnosu na Model tri linije, upravljanje organizacijom je povezano sa odborom / upravljačkim telom, upravljanje rizicima sa drugom linijom, a kontrole ili kontrolni procesi su povezani sa prvom linijom. Dok je rukovodstvo predstavljeno i u prvoj i u drugoj liniji, funkcija interne revizije je prikazana u trećoj liniji kao nezavisni i objektivni pružalac uveravanja, koji izveštava odbor / upravljačko telo (Princip 8 Nadzor koji sprovodi odbor).

Primenljivost, rizik i profesionalna procena

Tematski zahtevi se moraju poštovati kada funkcije interne revizije obavljaju angažmane uveravanja o temama za koje postoji Tematski zahtev ili kada se identifikuju aspekti Tematskog zahteva u okviru drugih angažmana uveravanja.

Kao što je opisano u Standardima, procena rizika je važan deo planiranja izvršnog rukovodioca revizije. Određivanje angažmana uveravanja koje treba uključiti u plan interne revizije zahteva procenu strategija, ciljeva i rizika organizacije najmanje jednom godišnje (Standard 9.4 Plan interne revizije). Prilikom planiranja pojedinačnih angažmana uveravanja, interni revizori moraju proceniti rizike relevantne za angažman (Standard 13.2 Procena rizika angažmana).

Kada se predmet Tematskog zahteva identifikuje tokom procesa planiranja interne revizije zasnovanog na riziku i bude uključen u plan revizije, onda se za procenu teme u okviru primenljivih angažmana moraju koristiti zahtevi navedeni u Tematskom zahtevu. Pored toga, kada interni revizori sprovode angažman (bilo da je uključen ili nije uključen u plan) i kada se pojave elementi Tematskog zahteva, mora se proceniti da li je Tematski zahtev primenljiv kao deo angažmana. Na kraju, ako zahtevani angažman nije prvobitno bio u planu, a uključuje temu, mora se proceniti da li je Tematski zahtev primenljiv.

Profesionalno rasuđivanje igra ključnu ulogu u primeni Tematskog zahteva. Procene rizika utiču na donošenje odluka izvršnih rukovodilaca revizije o tome koje angažmane treba uključiti u plan interne revizije (Standard 9.4 Plan interne revizije). Pored toga, interni revizori koriste profesionalnu procenu kako bi odredili koji će aspekti biti obuhvaćeni u okviru svakog angažmana (standardi 13.3 Ciljevi i obuhvat angažmana, 13.4 Kriterijumi za vrednovanje i 13.6 Program rada). Dodatak A „Primeri praktične primene“ opisuje kako interni revizori određuju da li se primenjuje Tematski zahtev.

Dokazi da je svaki zahtev iz Tematskog zahteva procenjen u smislu primenljivosti, moraju biti sačuvani, uključujući i obrazloženje koje objašnjava isključenje bilo kog zahteva. Usklađenost sa Tematskim zahtevom mora biti dokumentovana korišćenjem profesionalnog rasuđivanja revizora, kao što je opisano u Standardu 14.6 Dokumentacija angažmana.

Dok Tematski zahtev za sajber bezbednost pruža osnovu za razmatranje kontrolnih procesa, organizacije koje procenjuju sajber rizike kao veoma visoke, možda će morati da procene dodatne aspekte.

Ako izvršni rukovodilac revizije utvrdi da funkcija interne revizije nema potrebno znanje za obavljanje revizijskih angažmana o predmetu Tematskih zahteva, sprovođenje angažmana se može poveriti spoljnom pružaocu usluga (standardi 3.1 Kompetentnost, 7.2 Kvalifikacije izvršnog rukovodioca revizije, 10.2 Upravljanje ljudskim resursima). Čak i tada, poveravanje ne oslobađa funkciju interne revizije njene odgovornosti za usklađivanje sa aktuelnim zahtevima. Izvršni rukovodilac revizije zadržava konačnu odgovornost za obezbeđenje usklađenosti. Pored toga, ako izvršni rukovodilac revizije utvrdi da su resursi interne revizije nedovoljni, on mora da obavesti odbor o uticaju nedovoljnih resursa i o tome kako će se rešiti bilo kakvi nedostaci resursa (Standard 8.2 Resursi).

Učinak, dokumentacija i izveštavanje

Kada primenjuju Tematske zahteve, interni revizori, takođe, moraju poštovati Standarde i obavljati posao u skladu sa domenom V: Pružanje usluga interne revizije. Standardi u domenu V opisuju planiranje angažmana (Princip 13 Planirajte angažmane efektivno), sprovođenje angažmana (Princip 14 Sprovedite angažman) i saopštavanje rezultata angažmana (Princip 15 Saopštite rezultate angažmana i nadzirite planove aktivnosti).

Pokrivenost Tematskih zahteva može biti dokumentovana ili u planu interne revizije ili u radnim papirima angažmana na osnovu profesionalnog rasuđivanja revizora. Jedan ili više angažmana interne revizije može pokriti zahteve. Pored toga, možda nisu primenljivi svi zahtevi. Dokazi da je procenjena primenljivost Tematskog zahteva moraju se sačuvati, uključujući obrazloženje koje objašnjava sva izuzeća.

Opcioni alat u Dodatku C može se koristiti kao referenca i za dokumentovanje rada koji sprovode interni revizori.

Obezbeđenje kvaliteta

Standardi zahtevaju od izvršnog rukovodioca revizije da razvije, implementira i održava program obezbeđenja i unapređenja kvaliteta koji pokriva sve aspekte funkcije interne revizije (Standard 8.3 Kvalitet). Rezultati moraju biti saopšteni odboru i najvišem rukovodstvu. Komunikacijom se mora izvestiti o usklađenosti funkcije interne revizije sa Standardima i postizanju ciljeva učinka.

Usklađenost sa Tematskim zahtevima biće ocenjena u procenama kvaliteta. Da bi se pripremili za procenu kvaliteta, interni revizori mogu koristiti alat koji je dat u Dodatku C.

Sajber bezbednost

Sajber bezbednost je široka tema koja se odnosi na većinu tehnoloških aspekata bilo koje organizacije. Pored informacione tehnologije, sajber bezbednost obično je deo poslovnih procesa, što zahteva da interni revizori procenjuju sajber rizike prilikom planiranja, utvrđivanja obuhvata i sprovođenja angažmana uveravanja.

Nacionalni institut za standarde i tehnologiju (*National Institute of Standards and Technology* - NIST), deo Ministarstva trgovine SAD, definiše sajber bezbednost jednostavno kao „Sposobnost zaštite ili odbrane upotrebe sajber prostora od sajber napada“. Tematski zahtev za Sajber bezbednost se fokusira na spoljašnju granicu koju organizacije obezbeđuju da bi ublažile rizike od neovlašćenih korisnika i zlonamernih sajber pretnji. 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 obezbedila poverljivost, integritet i dostupnost.“

Zahtevi Tematskog zahteva za Sajber bezbednost uključuju:

- Upravljanje sajber bezbednošću – jasno definisani osnovni ciljevi i strategije sajber bezbednosti koje podržavaju ciljeve, politike i procedure organizacije.
- Upravljanje rizicima – procesi za identifikaciju, analizu, upravljanje i praćenje sajber pretnji, uključujući proces za brzo eskaliranje sajber rizika.
- Kontrole – uspostavljeni od strane rukovodstva, periodično ocenjeni kontrolni procesi za ublažavanje sajber rizika.

Razmatranja

Interni revizori mogu koristiti sledeća razmatranja da pomognu u proceni zahteva iz Tematskog zahteva za Sajber bezbednost. Ova razmatranja, koja upućuju na zahteve, su ilustrativna, ali nisu obavezna. Interni revizori treba da se oslone na profesionalnu procenu kada određuju šta da uključe u svoje procene.

Razmatranje upravljanja

Da bi procenili kako se procesi upravljanja primenjuju na ciljeve sajber bezbednosti, interni revizori mogu da pregledaju:

A. Zvanični, dokumentovani strateški plan i ciljeve sajber bezbednosti, uključujući dokaze da odbor periodično (uglavnom kvartalno) pregleda informacije o sajber bezbednosti koje pruža rukovodilac funkcije za bezbednost informacija (npr. *Chief Information Security Officer* - CISO). Dokazi mogu uključivati izveštavanje o:
   - Praćenju postizanja strateških ciljeva.
   - Budžetskim potrebama za podršku ciljeva i zadataka sajber bezbednosti.
   - Fokusu na rizike i interne kontrole, uključujući napredak u otklanjanju nedostataka.
   - Ključnim indikatorima učinka (*Key Performance Indicators* - KPI) za merenje uspeha.
   - Ljudskim resursima potrebnim za zapošljavanje, obuku i razvoj osoblja za sajber bezbednost.

B. Politike, procedure i druga relevantna dokumentacija koja se koristi za upravljanje procesima sajber bezbednosti, uključujući:
   - Politike koje se pregledaju i ažuriraju najmanje jednom godišnje. Novi sajber rizici mogu zahtevati da se pregledi i ažuriranja sprovode češće.
   - Procese kojima se utvrđuje da li su politike i procedure dovoljne za podršku operacijama sajber bezbednosti.
   - Opšte prihvaćene okvire (NIST, COBIT i drugi) za jačanje procesa sajber bezbednosti i internih kontrola.

C. Uloge i odgovornosti koje podržavaju postizanje ciljeva sajber bezbednosti, uključujući strukturu koja obezbeđuje da funkcija sajber bezbednosti izveštava nivo u organizaciji koji ima dovoljnu vidljivost za postizanje organizacione podrške.
   - Proces za periodičnu procenu znanja, veština i sposobnosti osoblja koje obavlja uloge u sajber bezbednosti.

D. Dokazi o angažovanju sa relevantnim zainteresovanim stranama (na primer, najviše rukovodstvo, operacije, upravljanje rizicima, ljudski resursi, pravni poslovi, usklađenost poslovanja, strateški dobavljači i drugi), uključujući komunikaciju o postojećim i rastućim sajber rizicima i poznatim potencijalnim ranjivostima. Dokazi o komunikaciji mogu uključivati zapisnike sa sastanaka, izveštaje ili imejlove.

Razmatranja upravljanja rizicima

Da bi procenili kako se procesi upravljanja rizicima primenjuju na ciljeve sajber bezbednosti, interni revizori mogu da pregledaju:

A. Kako organizacija procenjuje i upravlja rizikom sajber bezbednosti, uključujući kako se pretnje i ranjivosti:
   - Identifikuju i prijavljuju.
   - Analiziraju u cilju procene rizika za postizanje ciljeva organizacije.
   - Ublažavaju, uključujući planove aktivnosti za smanjenje rizika na prihvatljiv nivo.
   - Nadgledaju, uključujući plan za kontinuirano izveštavanje dok se pretnje u potpunosti ne reše.

B. Kako organizacija pribavlja periodične podatke u vezi sa upravljanjem rizikom sajber bezbednosti iz funkcionalnih oblasti, kao što su informaciona tehnologija, upravljanje rizicima na nivou organizacije, ljudski resursi, pravni poslovi, usklađenost poslovanja, operacije, računovodstvo i finansije. Za dobijanje informacija može se koristiti multifunkcionalni tim za sajber bezbednost ili odbor za nadzor IT.

C. Kako je organizacija dodelila nadležnosti i odgovornosti za upravljanje rizikom od sajber bezbednosti pojedincu ili timu.
   - Odgovorna lica treba da saopštavaju novosti o rizicima sajber bezbednosti u celoj organizaciji periodično (tromesečno, mesečno ili po potrebi) i mogu takođe uključiti zahteve za resursima potrebnim za strategije za ublažavanje rizika.

D. Procese eskalacije za rizike sajber bezbednosti, uključujući način na koji se nivo pretnje ili rizika procenjuje, dodeljuje i prioritizuje. Pregled može uključivati identifikaciju:
   - Definisanog nivoa rizika organizacije – kao što su visok, umeren i nizak – sa detaljnim objašnjenjima svakog nivoa rizika i procedurama eskalacije za svaku kategoriju rizika.
   - Liste trenutno identifikovanih rizika za sajber bezbednost i status ublažavanja svakog događaja rizika.
   - Primenljivih pravnih, regulatornih i zahteva usklađenosti.
   - Finansijskih i nefinansijskih (na primer, reputacija) uticaja rizika.

E. Proces za saopštavanje rizika sajber bezbednosti rukovodstvu i zaposlenima, koji uključuje:
   - Periodične (barem jednom godišnje) obuke zaposlenih o sajber bezbednosti, kao što su nenajavljene, simulirane fišing (*phishing*) kampanje za testiranje i praćenje svesti u organizaciji.
   - Novosti o otklanjanju postojećih problema sa sajber bezbednošću, sa predviđenim datumima završetka.

- Praćenje neusaklađenosti koje uključuje informisanje odbora i najvišeg rukovodstva.
- Ponovna procena pretnji u slučaju kada je organizacila promenila svoju sklonost i toleranciju rizika.

F. Procese koje je organizacija implementirala u vezi sa odgovorom na incidente i oporavkom, koji uključuju:

- Dokumentovani plan koji se pregleda i ažurira kako se poslovanje organizacije menja tokom vremena. Plan treba da sadrži sledeće:
  - Kako se incidenti otkrivaju i prijavljuju.
  - Kako se incidenti obuzdavaju da bi se sprečila dalja šteta.
  - Kako će organizacija odgovoriti i kako će se oporaviti za nastavak rada.
  - Kako će se incident analizirati radi utvrđivanja naučenih lekcija i kako će se sprečiti slični budući događaji.
- Periodično (najmanje jednom godišnje) testiranje (simulacija kroz diskusiju) i izveštavanje o rezultatima najvišem rukovodstvu i relevantnim zainteresovanim stranama. Planovi aktivnosti mogu biti rezultat testiranja.

Razmatranja kontrolnih procesa

Da bi procenili kako se kontrolni procesi primenjuju na ciljeve sajber bezbednosti, interni revizori mogu da pregledaju:

A. Način na koji rukovodstvo pristupa izgradnji efektivnog okruženja unutrašnjih kontrola za sajber bezbednost, uključujući:
   - Procenu i primenu internih kontrola potrebnih za ublažavanje povišenih rizika i zaštitu osetljivih, kritičnih, ličnih ili poverljivih podataka, na osnovu informacija iz procesa procene rizika organizacije.
   - Utvrđivanje zahteva za resursima za održavanje ključnih kontrola sajber bezbednosti.
   - Razmatranje kontrola koje primenjuju pružaoci usluga, kao dela kontrolnog okruženja, koje uključuje pregled Izveštaja o kontrolama uslužne organizacije (*Service Organization Controls* – SOC) od pružalaca usluga / dobavljača pre početka poslovnog odnosa i tokom trajanja odnosa.
   - Periodično testiranje da li kontrole sajber bezbednosti funkcionišu na način koji ublažava rizike i podržava postizanje ciljeva sajber bezbednosti.
   - Proces za otklanjanje nedostataka interne kontrole ili rešavanja nalaza iz procena koje je izvršila funkcija interne revizije ili drugi pružaoci usluga uveravanja (na primer, penetraciono testiranje).

B. Proces upravljanja talentima organizacije za regrutovanje i obuku profesionalaca za sajber bezbednost, uključujući način na koji organizacija identifikuje mogućnosti za povećanje sposobnosti stručnjaka za sajber bezbednost da podrže tehničko znanje i unapredi svest organizacije o rastućim izazovima.

- Primeri uključuju učešće u obukama, uključenost u grupe za razmenu znanja i stalno profesionalno obrazovanje koje uključuje dobijanje sertifikata vezanih za sajber bezbednost.

C. Procesi rukovodstva za identifikaciju, određivanje prioriteta, praćenje i izveštavanje o rastućim pretnjama i ranjivostima u sajber bezbednosti na kontinuiranoj osnovi, koji su fokusirani na svakodnevne operacije. Pregled može uključiti i to da li su uspostavljeni procesi za procenu pretnji i ranjivosti u vezi sa novim tehnologijama i tehnologijama koje su u nastajanju, kao što je upotreba veštačke inteligencije.

D. Procese i kontrole rukovodstva uspostavljene za upravljanje i zaštitu IT imovine tokom životnog ciklusa, uključujući izbor, korišćenje, održavanje i rashodovanje hardvera, softvera i usluga pružalaca usluga / dobavljača. Hardver uključuje servere, mrežnu opremu (kao što su ruteri ili zaštitni zidovi), desktop računare, laptopove, mobilne telefone, tablete i periferne uređaje. Softver uključuje operativne sisteme (kao što je *Windows*), softver za planiranje resursa preduzeća (*Enterprise Resource Planning – ERP)*, aplikacije, antivirusne programe i druge. Razmatranja o hardveru i softveru mogu uključivati:
   - Korišćenje enkripcije i antivirusnog softvera u organizaciji, upravljanje mobilnim uređajima, korišćenje složenih zahteva za lozinke, virtuelne privatne mreže (Virtual Private Network – VPN) / mreže sa nultim poverenjem (*Zero Trust Networking* – ZTN) za autentifikaciju i periodično ažuriranje firmvera.
   - Proces upravljanja imovinom koji obezbeđuje da hardver koji je kompanija stavila u upotrebu ima odgovarajuću bezbednosnu konfiguraciju i da će biti pravilno odložen kada se povuče iz upotrebe.
   - Kontrole u vezi sa bazom podataka koje uključuju ograničavanje pristupa korisnika i administratora, obezbeđivanje korišćenja enkripcije, pravljenje rezervnih kopija i testiranje baza podataka i prisustvo jakih kontrola mrežne bezbednosti.
   - Kako se pretnje ili ranjivosti sajber bezbednosti razmatraju u životnom ciklusu razvoja sistema (*Software Development Life Cycle* - SDLC).
   - Korišćenje pristupa razvoja, bezbednosti i operacija (DevSecOps) da bi se obezbedilo da proces razvoja softvera uključuje sajber bezbednost za proaktivno identifikovanje ranjivosti.

E. Procese koji se koriste za jačanje sajber bezbednosti, uključujući proveru:
   - Konfiguracije bezbednosnih postavki za minimiziranje rizika po sajber bezbednost.
   - Upravljanja mobilnim uređajima (uključujući korišćenje elektronske pošte i aplikacija) koja treba da bude konfigurisana tako da ublaži rizike sajber bezbednosti i da se uređajem korisnika može daljinski upravljati ako je uređaj kompromitovan.
   - Korišćenja enkripcije podataka „u mirovanju“, kao što su informacije uskladištene na čvrstom disku (*hard disk*), ili podaci „u tranzitu“, kao što je enkripcija elektronske pošte.

- Instaliranja zakrpa (*patching*) servera ili softvera (kao što je operativni sistem) najnovijim bezbednosnim izdanjima.
- Upravljanja pristupom korisnika kao što je upotreba višefaktorske autentifikacije (*multifactor authentication* – MFA) i jedinstvenih korisničkih ID-jeva sa složenim lozinkama koje periodično ističu.
- Praćenja postojećih kontrola kako bi se utvrdilo da li su dostupnost i korišćenje resursa adekvatni, omogućavajući pregled i analizu potencijalnih problema sajber bezbednosti koji ugrožavaju performanse.
- Integracije sajber bezbednosti u životnom ciklusu razvoja sistema (SDLC) da bi se identifikovale i rešile ranjivosti u sajber bezbednosti pre nego što se softver prebaci u produkciju.

F. Kontrole povezane sa mrežom koje obezbeđuju spoljašnju granicu organizacije, uključujući i način na koji organizacija koristi:
   - Segmentaciju mreže.
   - Zaštitne zidove *(firewalls*).
   - Kontrole korisničkog pristupa.
   - Ograničenja za spoljašnje i unutrašnje veze.
   - Kontrole oko Interneta stvari (*Internet of Things* – IoT) za međusobno povezane mreže.
   - Sisteme za otkrivanje / prevenciju upada za sprečavanje, otkrivanje i oporavak od sajber napada.

G. Bezbednosne kontrole za komunikaciju krajnjih tačaka koje se primenjuju na usluge kao što su elektronska pošta, Internet pretraživači, video konferencije, razmena poruka (Zoom, MS Teams i drugi), društvene mreže, klaud (*cloud*) i protokoli za deljenje datoteka. Kontrole mogu uključivati ograničavanje upotrebe određenih ekstenzija datoteka (kao što su .exe datoteke) i višefaktorsku autentifikaciju za deljenje datoteka.

Dodatak A. Primeri praktične primene

Sledeći primeri opisuju scenarija u kojima bi se primenio Tematski zahtev za Sajber bezbednost:

Primer 1: Sajber bezbednost je identifikovana za angažman interne revizije koji je uključen u plan interne revizije.

Kada funkcija interne revizije završi proces planiranja zasnovan na rizicima i uključi jedan ili više angažmana u vezi sa sajber bezbednošću u plan interne revizije, Tematski zahtev je obavezan pri sprovođenju takvih angažmana. Usklađenost se može postići ako su zahtevi uključeni kroz jedan ili više angažmana u planu interne revizije.

Sajber bezbednost je široka tema i ne može se svaki zahtev u Tematskim zahtevima primeniti na svaki angažman. Kada interni revizori primenjuju profesionalno rasuđivanje i utvrde da jedan ili više zahteva Tematskog zahteva za Sajber bezbednost nisu primenljivi i da ih stoga treba isključiti iz angažmana, interni revizori moraju dokumentovati i sačuvati obrazloženje za isključivanje tih zahteva. Na primer, razlog za isključivanje nekih zahteva može biti da funkcija interne revizije ciklično sprovodi različite angažmane vezane za sajber bezbednost ili da je utvrdila da je značaj rizika u angažmanu nizak.

Primer 2: Rizici sajber bezbednosti su identifikovani tokom angažmana revizije koji nije fokusiran na sajber bezbednost.

Interni revizori mogu identifikovati rizike sajber bezbednosti dok procenjuju proces koji nije direktno povezan sa sajber bezbednošću. Na primer, interni revizori procenjuju proces plaćanja dobavljačima u angažmanu koji nije fokusiran na sajber bezbednost i prilikom planiranja angažmana ne identifikuju da su rizici sajber bezbednosti u obuhvatu angažmana. Međutim, nakon sprovođenja „hoda kroz proces", interni revizori utvrđuju da takvi rizici treba da budu u obuhvatu; na primer, oni identifikuju rizike sajber bezbednosti koji se odnose na podnošenje zahteva za inicijalnu narudžbinu putem Interneta (Standard 13.2 Procena rizika angažmana).

Kada se identifikuju relevantni rizici, interni revizori moraju da pregledaju Tematski zahtev za Sajber bezbednost i utvrde koji su zahtevi primenljivi. U ovom primeru, oni mogu isključiti proces upravljanja sajber bezbednošću ili proces upravljanja rizicima sajber bezbednosti. Oni moraju da dokumentuju u radnim papirima angažmana obrazloženje za isključivanje drugih zahteva iz Tematskog zahteva za Sajber bezbednost i da sačuvaju dokumentaciju.

Primer 3: Zahteva se angažman u oblasti sajber bezbednosti koji prvobitno nije bio uključen u plan interne revizije.

Zainteresovane strane kao što su odbor, rukovodstvo ili regulator mogu tražiti od internih revizora da izvrše procene sajber bezbednosti van prvobitnog plana revizije. Na primer, kada su organizacije meta sajber napada, odbor može zatražiti angažovanje interne revizije radi procene kontrola sajber bezbednosti. Tematski zahtev je primenljiv, zahtevi moraju biti procenjeni, a sva isključenja dokumentovana.

Dodatak B. Mapiranje sa drugim okvirima

Organizacija može imati sopstvene napore u oblasti sajber bezbednosti, koristeći okvire upravljanja rizicima i organizacijom kao što su COBIT ili NIST. Interni revizori su možda već razvili programe revizije i procedure testiranja zasnovane na ovim okvirima. Interni revizori treba da usklade testiranja kontrola sajber bezbednosti koja nameravaju da sprovedu sa Tematskim zahtevom da bi osigurali adekvatnu pokrivenost. Tabela u nastavku mapira Tematski zahtev za sajber bezbednost sa tri najčešće korišćena okvira: NIST Cybersecurity Framework 2.0, COBIT 2019 i NIST 800-53. Ovi okviri su mapirani jer su lako dostupni bez ikakvih troškova.

Zahtevi za Upravljanje	Reference okvira		
	NIST CSF 2.0	NIST 800-53	COBIT 2019
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.	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 koje se odnose na sajber bezbednost su uspostavljene i periodično se ažuriraju kako bi se ojačalo 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. Uloge i odgovornosti koje podržavaju ciljeve sajber bezbednosti su utvrđene a postoji i proces za periodičnu procenu znanja, veština i sposobnosti pojedinaca koji obavljaju te uloge.	GV.RR-02; GV.RR-04; GV.SC-02; GV.OC-02	PM-13; AT-2; AT-3	EDM02; APO01; APO07
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.	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

Zahtevi za Upravljanje rizicima	NIST CSF 2.0	NIST 800-53	COBIT 2019
A. Procena rizika organizacije i procesi upravljanja rizicima uključuju identifikaciju, analizu, ublažavanje i praćenje pretnji sajber bezbednosti i njihovog uticaja 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 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.	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. 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.	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 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.	GV.RM; ID.RA; RS.MA-04	CA-7; RA-3; RA-7	EDM03; APO01, APO10; APO12
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.	PR.AT; GV.RR.01; GV.RR-04; GV.PO	AT-2	APO01; APO02; EDM03; MEA03
F. Organizacija je primenila proces za odgovor na 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.	RS; RC	IR-4; IR-5; IR-6; IR-7; IR-8; IR-10; SA-15	DSS02; DSS03; DSS04; DSS05.07

Zahtevi Kontrolnih procesa	NIST CSF 2.0	NIST 800-53	COBIT 2019
A. Uspostavljen je proces kako bi se osiguralo da postoje i interne kontrole i kontrole na strani pružalaca usluga / dobavljača kako bi se zaštitila poverljivost, integritet i dostupnost sistema i podataka organizacije. Procene se vrše periodično kako bi se utvrdilo da li kontrole funkcionišu na način koji promoviše postizanje ciljeva sajber bezbednosti organizacije i brzo rešavanje 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. Uspostavljen je proces upravljanja talentima koji uključuje obuku za razvoj i održavanje tehničkih kompetencija u vezi sa operacijama sajber bezbednosti. Proces se periodično pregleda.	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 izveštavanje o rastućim pretnjama i ranjivostima u vezi sa sajber bezbednošću i za identifikaciju, određivanje prioriteta i primenu mogućnosti za poboljšanje operacija sajber bezbednosti.	ID.RA-02; ID.RA-03, ID.RA-04	CA-7; PM-31; RA-5	DSS03.05
D. Sajber bezbednost je uključena u upravljanje životnim ciklusom (izbor, korišćenje, održavanje i povlačenje iz upotrebe) sve IT imovine, uključujući hardver, softver i usluge pružalaca usluga / 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 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).	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 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).	PR.IR; DE.CM-01	AC-6; AC-17; AC-18; AC-20; SC-7; SC-10; CA-8	DSS05.02
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.	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. Opcioni alat za dokumentaciju

Od internih revizora se očekuje da primenjuju profesionalno rasuđivanje u određivanju primenljivosti zahteva na osnovu procene rizika i na odgovarajući način dokumentuju isključenja određenih zahteva. Tematski zahtev može biti dokumentovan u planu interne revizije ili u radnim papirima angažmana na osnovu profesionalne procene revizora. Jedan ili više angažmana interne revizije može pokriti zahteve. Pored toga, možda nisu primenljivi svi zahtevi. Obrazac za štampanje u nastavku pruža jednu opciju za dokumentovanje usaglašenosti sa aktuelnim zahtevima za sajber bezbednost, ali njegova upotreba nije obavezna.

Sajber bezbednost – Upravljanje

Zahtev	Sprovedeno pokrivanje ili obrazloženje za isključenje	Referenca za dokumentaciju
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. Uloge i odgovornosti koje podržavaju ciljeve sajber bezbednosti su utvrđene, 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.		

Sajber bezbednost – Upravljanje rizicima

Zahtev	Sprovedeno pokrivanje ili obrazloženje za isključenje	Referenca za dokumentaciju
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.		

Zahtev	Sprovedeno pokrivanje ili obrazloženje za isključenje	Referenca za dokumentaciju
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.		

Sajber bezbednost – Kontrolni procesi

Zahtev	Sprovedeno pokrivanje ili obrazloženje za isključenje	Referenca za dokumentaciju
A. Uspostavljen je proces kako bi se osiguralo da postoje i interne kontrole i kontrole na strani pružalaca usluga / dobavljača kako bi se zaštitila poverljivost, integritet i dostupnost sistema i podataka organizacije. Procene 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 implementaciju 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 pružalaca usluga / dobavljača.		

Zahtev	Sprovedeno pokrivanje ili obrazloženje za isključenje	Referenca za dokumentaciju
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.

Odricanje od odgovornosti

IIA objavljuje ovaj dokument u informativne i obrazovne svrhe. Ovaj materijal nije namenjen da pruži konačne odgovore na specifične pojedinačne okolnosti i kao takav je namenjen samo da se koristi kao vodič. IIA preporučuje traženje saveta nezavisnog stručnjaka koji se direktno odnosi na bilo koju specifičnu situaciju. IIA ne prihvata odgovornost za bilo koga ko se isključivo oslanja na ovaj materijal.

Autorska prava

Ferbuar 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