Cybersäkerhet

Topical Requirement

The Institute of
Internal Auditors

Ämnesrelaterat krav för cyber-säkerhet

Internationella Standarder för yrkesmässigt utförande av internrevision (International Professional Practices Framework®) består av Globala standarder för internrevision (Global Internal Audit Standards™), Ämnesrelaterade krav (Topical Requirements) och Global Guidance. Ämnesrelaterade krav är obligatoriska och måste användas tillsammans med standarderna, som utgör den auktoritativa grunden för de metoder som krävs.

Ämnesrelaterade krav tillhandahåller tydlig vägledning för internrevisorer genom att etablera en miniminivå för revision av specifika riskområden. Organisationens riskprofil kan innebära att internrevisorer behöver beakta ytterligare aspekter.

Ämnesrelaterade krav kommer att öka likformigheten i hur internrevisionstjänster utförs samt förbättra kvaliteten och tillförlitligheten i genomförande och resultat.

Internrevisorer ska tillämpa ämnesrelaterade krav i enlighet med de globala standarderna. Ämnesrelaterade krav är obligatoriska för säkringsuppdrag och rekommenderas för rådgivningsuppdrag. Ämnesrelaterade krav är tillämpliga när något av följande föreligger:

A. Området är en del av revisionsplanen.
B. Området är identifierat i samband med utförandet av ett uppdrag.
C. Uppdrag som inte ingår i den ursprungliga revisionsplanen.

Alla delarna av ämnesrelaterade krav behöver inte vara tillämpliga i varje uppdrag; om delar av området har uteslutits ska detta motiveras, dokumenteras och bevaras. Följsamhet mot ämnesrelaterade krav kommer att utvärderas under kvalitetsutvärderingen.

Mer information finns i användarvägledningen för det ämnesrelaterade kravet.

Cybersäkerhet

National Institute of Standards and Technology (NIST) definierar cybersäkerhet som "förmågan att skydda eller försvara cyberrymden från cyberattacker". Cybersäkerhet är en delmängd av den övergripande informationssäkerheten, som NIST definierar som ”skyddet av information och informationssystem från obehörig åtkomst, användning, avslöjande, störning, modifiering eller förstörelse för att skapa konfidentialitet, integritet och tillgänglighet".

Cybersäkerhet minskar risken genom att stärka den övergripande kontrollmiljön och skydda en organisations informationstillgångar från obehörig åtkomst, störning, ändring eller förstörelse. Cyberattacker kan leda till direkta och indirekta effekter som ofta är betydande, eftersom datorer, nätverk, program, data och känslig information är kritiska komponenter i de flesta organisationer.

Utvärdering och bedömning av ledning, riskhantering samt styrning och kontroll för cybersäkerhet

Detta ämnesrelaterade krav ger en metod för att bedöma en miniminivå för utformning och implementering av processer för ledning riskhantering, styrning och kontroll av cybersäkerhet.

LEDNING: Utvärdering och bedömning av cybersäkerhet

Krav:

Internrevisorer ska bedöma följande i förhållande till organisationens styrning och ledning av cybersäkerhet:

- **A.** Strategi och mål för cybersäkerhet har fastställts och uppdateras regelbundet. Uppföljning av uppfyllandet av målen för cybersäkerhet har kommunicerats regelbundet och har följts upp av styrelsen, inklusive resurs- och budgetöverväganden för att genomföra strategin.
- **B.** Policyer och rutiner för cybersäkerhet finns och har uppdaterats regelbundet för att stärka styrning och kontroll.
- **C.** Roller och ansvarsområden som stödjer målen för cybersäkerhet har fastställts och det finns en process för att regelbundet bedöma kunskaper, färdigheter och förmågor hos de personer som tilldelats rollerna.
- **D.** Intressenter har engagerats för att diskutera och hantera sårbarheter och hot i cybersäkerhetsmiljön. Intressenterna omfattar bland annat högsta ledningen, operativ verksamhet, riskhantering, HR, juridik, regelefterlevnad, leverantörer och övriga.

RISKHANTERING: Utvärdering och bedömning av hantering av cybersäkerhetsrisker

Krav:

Internrevisorer ska bedöma följande avseende organisationens hantering av cybersäkerhetsrisker:

- **A.** Organisationens riskbedömnings- och riskhanteringsprocesser har omfattat identifiering, analys, hantering och övervakning av cybersäkerhetshot och dess effekt på uppfyllelsen av strategiska mål.
- **B.** Cybersäkerhetsrisker har hanterats inom hela organisationen (exempelvis IT, riskhantering, HR, juridik, regelefterlevnad, drift, leverantörskedja, redovisning, finans och övriga delar).

C. Roller och ansvar för hantering av cybersäkerhetsrisker har fastställts. En person eller ett team har utsetts för att regelbundet övervaka och rapportera hur cybersäkerhetsrisker hanteras, och att teamet har de resurser som krävs för att hantera riskerna och identifiera nya cybersäkerhetshot.

D. Det finns en process för att snabbt eskalera alla cybersäkerhetsrisker som är oacceptabla enligt organisationens riktlinjer eller tillämpliga lagar och förordningar. Finansiella och icke-finansiella konsekvenser av cybersäkerhetsrisker bör beaktas.

E. En process finns för att medvetandegöra cybersäkerhetsrisker hos ledning och anställda. Ledningen ska regelbundet granska problem, gap och brister. Dessa ska rapporteras och åtgärdas skyndsamt.

F. Organisationen har implementerat en process för hantering av cybersäkerhetsincidenter som omfattar upptäckt, hantering, återställning och analys efter en incident. Processen har testats regelbundet.

STYRNING OCH KONTROLL: Utvärdering och bedömning av styrning och kontroll för cybersäkerhet

Krav:

Internrevisorer ska bedöma följande avseende organisationens styrning och kontroll av cybersäkerhet:

A. En process har etablerats för att säkerställa att både organisationens och leverantörernas styrning och kontroll finns på plats för att skydda konfidentialitet, integritet och tillgänglighet av system och data. Utvärderingar har gjorts regelbundet för att avgöra om kontrollerna fungerar på ett sätt som främjar organisationens cybersäkerhetsmål.

B. En process har etablerats som inkluderar utbildning för att utveckla och upprätthålla teknisk kompetens för cybersäkerhet. Processen har utvärderats regelbundet.

C. En process finns för att kontinuerligt övervaka och rapportera nya hot och sårbarheter samt identifiera, prioritera och genomföra aktiviteter för att förbättra cybersäkerheten.

D. Cybersäkerhet ingår i livscykelhanteringen av alla IT-tillgångar, inklusive hårdvara, mjukvara och leverantörstjänster.

E. Processer finns för att stärka cybersäkerheten, inklusive konfiguration, slutanvändaradministration , kryptering, patchning, åtkomsthantering samt övervakning av tillgänglighet och prestanda. Cybersäkerhet ska beaktas vid mjukvaruutvecklingen (DevSecOps).

F. Nätverkskontroller finns, exempelvis segmentering av åtkomst, användning och placering av brandväggar, begräning av anslutningar från och till externa nätverk, virtuella privata nätverk (VPN)/zero trust network access (ZTNA), nätverkskontroller för IoT och system för upptäckt och förebyggande av intrång (IDS och IPS).

G. Säkerhetskontroller för verksamhetsnära kommunikationtjänster har upprättats för exempelvis e-post, webbläsare, videokonferenser, meddelanden, sociala medier, moln och fildelningsprotokoll.

Om Institutet för internrevisorer

Institute of Internal Auditors (IIA) är en internationell yrkesorganisation som har mer än 255.000 medlemmar globalt och har utfärdat mer än 200.000 certifieringar som Certified Internal Auditor® (CIA®) över hela världen. IIA grundades 1941 och är erkänt över hela världen som internrevisionsbranschens ledande aktör inom standarder, certifieringar, utbildning, forskning och teknisk vägledning. För mer information, besök www.theiia.org.

Upphovsrätt

Februari 2025

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