

Ämnesrelaterat krav

Vägledning för tillämpning



The Institute of
Internal Auditors

Ämnesrelaterat krav Vägledning för tillämpning

Innehåll

1. Betydelsen av professionellt omdöme
2. Ett riskbaserat angreppssätt för att bestämma tillämpning
3. Obligatoriska krav vid identifiering av ämnen
4. Att tillämpa ämnesrelaterade krav inom revisionens livscykel
5. Begränsningar och undantag i omfattning
6. Hantering av område med hög risk där mognadsgraden är låg
7. Resursbegränsningar
8. Regulatorisk anpassning och användning av andra ramverk
9. Att tillämpa flera ämnesrelaterade krav

Vägledningen för tillämpning av ämnesrelaterade krav

International Professional Practices Framework® består av globala standarder för internrevision (Global Internal Audit Standards™), ämnesrelaterade krav och global vägledning. Ämnesrelaterade krav är obligatoriska för säkringsuppdrag och rekommenderade för rådgivningsuppdrag inom specifika riskområden. De måste användas tillsammans med Standarderna, som utgör normativ grund för obligatoriska metoder.

Ämnesrelaterade krav utgör lägsta nivå för att täcka specifika riskområden. Internrevisorer måste tillämpa kompletterande metoder om organisatoriska risker, regler eller sammanhang kräver större djup.

1. Betydelsen av professionellt omdöme

Tillämpningen av professionell bedömning är avgörande för att effektivt använda ämnesrelaterat krav och krävs uttryckligen av standarderna. Professionellt omdöme tillåter internrevisorer att **anpassa tillämpningen av ämnesrelaterade krav till organisationens unika sammanhang, riskprofil och strategiska prioriteringar, för att säkerställa att revisionen utformas relevant och proportionerligt.**

Professionellt omdöme tillämpas i olika skeden av revisionens livscykel. Detta spelar en roll under internrevisionens **planeringsprocess**, som beskrivs i standard 9.4 Plan för internrevision, där beslut fattas om vilka risker som är tillräckligt väsentliga avseende ämnesrelaterade krav för att omfattas. Det används också för **att definiera uppdragets omfattning och mål** enligt standard 13.3 Uppdragets mål och omfattning, särskilt för att avgöra om det ämnesrelaterade kravet ska tillämpas i sin helhet eller endast delvis.

Vidare ska omdöme tillämpas vid **utvärdering och dokumentation av användning och undantag**, vid val av utvärderingskriterier (standard 13.4 Utvärderingskriterier) och steg i arbetsprogram (standard 13.6 Arbetsprogram) samt vid **beslut om revisionsbevis från externa granskare**, t.ex. lagstadgade revisioner, uppfyller kraven.

Även om följsamhet till ämnesrelaterade krav förväntas, kan det finnas exceptionella omständigheter, såsom begränsade resurser eller sektorspecifika överväganden, som medför att en fullständig överensstämmelse inte är möjlig att nå. I sådant fall bör

internrevisionschefen vidta alternativa åtgärder för att uppfylla syftet med kravet samt dokumentera och kommunicera orsaken till avvikelser. Denna **"följ eller förklara"-strategi** är i linje med de principer som ingår i standarderna.

Enligt standardernas Princip I, Påvisa integritet, måste internrevisorer visa integritet i sitt arbete och beteende genom att använda professionella bedömningar. Standard 4.1 Överensstämmelse med Globala standarder för internrevision kräver att sådana bedömningar görs med lämplig yrkesomsorg. Detta innebär att beslut måste vara logiska och evidensbaserade, inte godtyckliga eller intuitiva. Dessa bör följa internrevisionens metod och vara anpassade till organisationens riskaptit. **Alla omdömesbaserade beslut ska vara tydligt dokumenterade** i planeringen av uppdrag, arbetspapper eller i underlag för hur ämnesrelaterat krav tillämpats. Dessa **måste vara transparenta och möjliga att försvara vid intern kvalitetssäkring eller externa kvalitetsutvärderingen**. Dokumentationen speglar vikten av ett välgrundat och genomtänkt förhållningssätt: Det blir enklare att visa följsamhet när den underliggande logiken är tydligt dokumenterad.

Professionellt omdöme ersätter inte struktur men det gör det möjligt för internrevisorer att **anpassa strukturerade krav, som ämnesrelaterade krav, till en komplex verklighet**. Professionellt omdöme säkerställer att standarderna inte bara följs utan också anpassas till organisationens behov, vilket ger en försäkrasom både är trovärdig och relevant.

2. Ett riskbaserat tillvägagångssätt för att avgöra tillämplighet

Internrevision har ett riskbaserat arbetssätt för att säkerställa att resurser fokuseras på de områden som är mest väsentliga. Identifiering av revisionsområden och beslut om omfattning bör bygga på en grundlig och väldokumenterad riskbedömning. Ett ämnesrelaterat krav ska följas när området **identifieras under riskbedömningen och där risken överskrider en för organisationen betydande risknivå**.

För att **bedöma väsentligheten av en risk som är relaterad till ett ämnesrelaterat krav** bör internrevisionen utgå från organisationens strategiska mål, kända exponeringar, tidigare incidenter eller förändringar i omvärlden. Därefter ska den inneboende risken bedömas genom att skatta dess påverkan och sannolikhet. Denna risknivå kan sedan jämföras med organisationens definierade riskaptit för att se om den överskrider en kritisk nivå.¹

¹ Internrevisorer kan överväga att använda ett känt riskvärderingsverktyg, till exempel IIA:s vägledning Enterprise and Business Process Risks Tool. [Enterprise and Business Process Risks Risker| IIA](#)



Definitionen av kritisk nivå ska ansluta till organisationens riskaptit, som utformas av styrelsen och ledningen. Här ingår ekonomisk, juridisk, reglerings- och efterlevnadsmässig påverkan samt kvalitativa konsekvenser, till exempel skadat anseende eller misslyckande med att nå strategiska eller etiska förväntningar.

Ledningen står för tydliga riktlinjer för vilka risktyper som endast accepteras i begränsad omfattning eller inte tillåts, även vid lägre sannolikhet. Tydliga förväntningar från styrelse och ledning och en överenskommen förståelse för gradering, är avgörande för att säkerställa konsekvent och riskanpassad bedömning av risker.

När en risk har identifierats som betydande ska den kopplas till **relevant ämnesrelaterat krav och komponenter för ledning, riskhantering, styrning och kontroll** för att fastställa vilka krav som ska tillämpas. Alla krav bör ses över för att säkerställa att de är relevanta. Om specifika krav inte bedöms vara tillämpliga på grund av riskens art, sammanhang eller grundorsak, måste bedömningen tydligt dokumenteras, inklusive motiveringen till varför kraven inte är tillämpliga. Om risken t.ex. uppstår på grund av en brist i utförandet av kontrollen snarare än i styrningen, kan det vara så att endast de kontrollrelaterade komponenterna är relevanta. Detta säkerställer att revisionen är både riskbaserad och har lämplig omfattning.

Slutligen måste **professionellt omdöme** tillämpas för att styrka beslutets lämplighet. Beslutet och grunden ska dokumenteras på lämpligt sätt.

3. Obligatoriska krav relaterade till ämnesrelaterade krav

Ämnesrelaterade krav är obligatoriska för säkringsuppdrag när risken har identifierats under riskbedömningen och överstiger ett kritiskt tröskelvärde (se 2. Ett riskbaserat tillvägagångssätt för att fastställa tillämplighet). Detta kan gälla den periodiska riskbedömningen som används för att ta fram internrevisionsplanen eller den specifika riskbedömningen som genomförs för att bestämma omfattningen av ett revisionsuppdrag. Tillämpningen av ämnesrelaterade krav rekommenderas för rådgivningsuppdrag om kravet är relaterat till uppdragets mål.

Ämnesrelaterade krav är tillämpliga när området uttryckligen ingår i internrevisionsplanen i form av ett säkringsuppdrag. Tillämpningen kan ske genom en omfattande temagranskning som helt inriktas på området eller så kan

kraven behandlas i flera uppdrag, eventuellt fördelade över flera år. I sådana fall måste internrevisorer säkerställa att alla relevanta krav slutligen omfattas och att uppdragsdokumentationen tydligt visar hur och när varje del behandlas.

Ämnesrelaterade krav måste också tillämpas **om det identifieras under ett uppdrag**, vilket innebär att det har nått en prioriterad nivå över den kritiska tröskeln, baserat på organisationens riskaptit. Denna bör hanteras som en betydande risk som kräver hantering, i linje med uppdragets mål och riskbedömning. Det är viktigt att beakta att alla delar av det ämnesrelaterade kravet inte behöver tillämpas om den identifierade risken endast avser en del av ledning, riskhantering samt styrning och kontroll (t.ex. endast kontroller eller ledning). Tillämpningsområdet måste överensstämma med den identifierade riskens beskaffenhet och avgränsningar samt med revisionens mål. Professionellt omdöme bör användas för att avgöra vilka krav som är relevanta och avpassade i förhållande till risknivå och risktyp.

Ett ämnesrelaterat krav är också **tillämpligt när det blir en del av ett uppdrag som läggs till på begäran**, även om det inte ursprungligen ingick i revisionsplanen. I dessa fall måste tillämpningen av det ämnesrelaterade kravet fortfarande följa ett riskbaserat tillvägagångssätt. Internrevisorer kan antingen tillämpa alla krav eller endast en delmängd av kraven beroende på riskens väsentlighet och dess anpassning till organisationens risknivå.

4. Tillämpning av ämnesrelaterade krav i revisionens livscykel

När en risk har bedömts som betydande genom riskbedömningen och ett ämnesrelaterat krav är tillämpligt, bör internrevisorer tillämpa det ämnesrelaterade kravet konsekvent under hela revisionens livscykel.

På planeringsnivå

Vid framtagandet av internrevisionsplanen, i enlighet med standard 9.4 Internrevisionsplan, bör identifierade betydande risker relaterade till ett ämnesrelaterat krav återspeglas på lämpligt sätt genom att inkluderas i en **fristående granskning eller att integrera kraven i flera uppdrag, potentiellt spridda över revisionscykler eller år**. I båda fallen är det viktigt att tydligt hänvisa till det tillämpliga ämnesrelaterade kravet i beskrivning av revisionsuniversum, riskbedömningsdokumentationen och planeringsdokumentationen för att säkerställa transparens och anpassning till både organisationens prioriteringar och professionella standarder.

Vid utförandet av uppdrag

Internrevisorer bör använda professionellt omdöme för att anpassa tillämpningen av det ämnesrelaterade kravet till riskens specifika egenskaper. Standard 13.3 Uppdragets mål och omfattning beaktar den underliggande orsaken till risken och identifierar vilka delar av ledning, riskhanteringen eller styrning och kontroll som är mest relevanta för riskens realisering och konsekvens. Baserat på denna analys **behöver endast de krav som direkt hänförs till uppdragets definierade omfattning och mål tillämpas**. Följaktligen kan vissa delar av det ämnesrelaterade kravet efter bedömning uteslutas när de faller utanför tillämpningsområdet för den identifierade risken och uppdragsmålen. Dessa avgränsningar ska återspegla ett riskbaserat och anpassat tillvägagångssätt och måste vara tydligt dokumenterat i uppdragets arbetspapper, inklusive en motivering som visar att det är i linje med uppdragets inriktning.

Internrevisorer bör sedan utföra **arbete** för att stödja slutsatserna om de tillämpliga kraven för att säkerställa en meningsfull och målinriktad granskningsinsats.

5. Avgränsningar avseende tillämpning

Sker det avgränsningar i tillämpningen av det ämnesrelaterade kravet, krävs det att detta dokumenteras i de fall där området **har identifierats som en väsentlig eller prioriterad risk**. Dessa beslut kan dokumenteras i olika skeden av **revisionsprocessen**. Om det ämnesrelaterade kravet ingår i revisionsplanen kan det dokumenteras i planen eller fördelas över flera uppdrag över tid. Alternativt kan det dokumenteras på uppdragsnivå när identifiering har gjorts under planeringen eller utförandet av ett uppdrag, eller när styrelse eller ledning begär så.

God dokumentationssed innebär att en tydlig och försvarbar logik tillämpas när omfattningen av det ämnesrelaterade kravet fastställs och dokumenteras. Detta innefattar att bedöma **relevansen av de tillämpliga kraven genom att utvärdera dessa** med hänsyn till den kontext som gäller för organisationen samt identifierade risker i verksamheten. Undantag eller delvis tillämpning bör understödjas av lämpliga referenser, såsom riskbedömning, begränsningar av omfattningen, tillämpad professionell bedömning samt motivering till den valda omfattningen. Relevant dokumentation stödjer revisorn i att motivera den valda omfattningen och minskar risken för att missa något väsentligt.

En väl genomförd riskbedömning genererar mycket av den dokumentation som krävs, vilket gör denna process till en integrerad del av revisionsplaneringen och inte till en extra administrativ börda. Vidare kommer denna dokumentation att användas vid **kvalitetsbedömningar** för att utvärdera om de ämnesrelaterade kraven har tillämpats på ett relevant och konsekvent sätt.

Verktyg som tillhandahålls i användarhandboken, t.ex. **tillämpningsmatris för ämnesrelaterade krav**, kan bidra till konsekvent hantering, tydlig spårbarhet och anpassning till professionella standarder.

6. Hantering av område med hög risk där mognadsgraden är låg

När ett ämne identifieras som ett område med hög risk men där organisationens ledning, riskhantering samt styrnings- och kontrollmognad är låg, måste internrevisionen adressera detta.

Enligt standard ska internrevisionen säkerställa att väsentliga risker kommer till **styrelsens och ledningens** kännedom. Det krävs klargörande samtal för att säkerställa att ledningen förstår att riskområdet innehåller betydande exponeringar som för närvarande inte täcks av befintliga strukturer eller processer.

I sådana fall kan det ämnesrelaterade kravet fungera som en rekommenderad vägledning inom ramen för ett rådgivningsuppdrag och utgöra ett värdefullt ramverk för att utvärdera brister, belysa exponeringar och skapa medvetenhet inom hela organisationen.

Även om fullständig försäkran inte kan ges, är internrevisionens roll att säkerställa öppenhet, främja medvetenhet och uppmuntra ledningen att ta ägarskap för frågan. Frågan bör även lyftas till styrelsen för att säkerställa medvetenhet och samsyn om lämplig hantering.

7. Begränsningar av resurser

Om internrevisionen saknar kapacitet, t.ex. tid, personal eller budget, eller nödvändig kompetens, såsom sakkunskap eller tekniska färdigheter, för att fullt ut tillämpa ett ämnesrelaterat krav, innebär detta inte att ansvaret för att bedöma

risken eller avgöra tillämpligheten fråntas. Enligt standard 8.2 Resurser **måste revisionschefen informera styrelsen om sådana resursbegränsningar och förklara hur dessa kommer att hanteras.**

Resursbegränsningar kan hanteras genom att internrevisionen **utvecklar** den interna förmågan genom riktad utbildning eller rekrytering. Alternativt kan uppdraget **outsourcas eller cosourcas** till kvalificerade externa specialister. I vissa fall kan revisionen få en **ändrad omfattning** men endast om beslutet stöds av en dokumenterad motivering och har överenskommits eller godkänts av styrelsen.

Internrevisionschefen är ansvarig för att säkerställa att ämnesrelaterat krav efterlevs och för att identifiera alternativ för att uppnå detta, till exempel outsourcing, samtidigt som det övergripande ansvaret bibehålls. Vid avvikelse ska internrevisionen se till att detta **redovisas öppet** tillsammans med de bakomliggande orsakerna, till exempel resursbegränsningar. Alla relaterade riskreducerande åtgärder måste dokumenteras tydligt i revisionsplanen och i uppdragshandlingarna, så att ansvar och spårbarhet upprätthålls under hela processen.

8. Anpassning av regelverk och användning av andra ramverk

Ämnesrelaterade krav är globalt tillämpliga och anger en miniminivå för internrevisionens täckning av specifika riskområden, oavsett organisationens storlek, sektor eller mognadsgrad. **Organisationer kan dock också omfattas av externa regleringskrav, standarder eller ramverk**, såsom NIST, ISO 27001, SOC-rapporter, lagar och förordningar eller branschspecifika skyldigheter, som överlappar eller går utöver omfattningen av ett visst ämnesrelaterat krav.

När detta inträffar förväntas internrevisorerna anta ett **riskbaserat och jämförande tillvägagångssätt**. Om ett lagstadgat krav eller ett externt ramverk innebär en **striktare eller mer omfattande skyldighet** än det ämnesrelaterade kravet, bör den striktare standarden styra revisionens omfattning. Faktum är att de flesta regelverk, särskilt inom högriskområden såsom cybersäkerhet, tredjepartshantering eller finansiella tjänster, tenderar att vara mer detaljerade och krävande än motsvarande ämnesrelaterade krav. I de fall där organisationer redan uppfyller dessa mer striktare standarder bör det i allmänhet inte krävas

några betydande ytterligare ansträngningar för att visa följsamhet till det ämnesrelaterade kravet, förutsatt att kopplingen dokumenteras och att täckningen bedöms vara tillräcklig.

Att jämföra det ämnesrelaterade kravet mot lagstadgade krav och andra erkända ramverk anses vara god praxis. Jämförelsen gör det möjligt för internrevisionen att visa hur kraven uppfylls – antingen direkt eller genom att förlita sig på befintliga revisionsbevis – samtidigt som det säkerställs att inga kritiska brister förbises. Om till exempel en cybersäkerhetsrevision redan har genomförts enligt NIST:s riktlinjer av en annan säkringsgivare, kan internrevisionen hänvisa till och utnyttja detta arbete för att bekräfta följsamheten till det ämnesrelaterade kravet för cybersäkerhet. Detta måste dock uttryckligen dokumenteras och bevisens tillräcklighet ska bedömas med hjälp av professionellt omdöme (se även Global Practice Guide: Coordination and Reliance: Working with Other Assurance Providers – [Samordning och att förlita sig på andras arbete: Samarbete med andra säkringsleverantörer](#)).

Tillämpningen av ämnesrelaterade krav i en reglerad miljö kräver **noggrann samordning**. Internrevisorer bör säkerställa att tillvägagångssättet återspeglar den mest rigorösa tillämpliga standarden, samtidigt som dubbelarbete undviks och befintliga kontroller, utvärderingar och externa revisioner utnyttjas där så är lämpligt. Detta främjar effektivitet och trovärdighet och säkerställer att internrevisionen fortsätter att uppfylla sitt ansvar enligt standarderna att tillhandahålla oberoende, riskbaserad försäkran som är både anpassad till sammanhanget och globalt konsekvent.

9. Tillämpning av flera ämnesrelaterade krav

Hur flera ämnesrelaterade krav ska tillämpas inom ett och samma revisionsuppdrag beror helt på vilka väsentliga risker som identifierats genom **organisationens riskbedömningsprocess**. Istället för att förutsätta att flera ämnesrelaterade krav ska tillämpas tillsammans, måste internrevisorer bedöma om riskens art och omfattning faktiskt innebär att mer än ett ämnesrelaterat krav behöver användas.

Om exempelvis en väsentlig risk identifieras inom området för tredje parts cybersäkerhet när en tredje part tillhandahåller cybersäkerhetstjänster, kan det vara lämpligt att tillämpa både det ämnesrelaterade kravet på cybersäkerhet och det ämnesrelaterade kravet avseende tredje partsrelationer. Men om risken endast avser tredje parts efterlevnad av avtal utan inverkan på



cybersäkerheten, är det endast det ämnesrelaterade kravet för tredje partsrelationer som gäller. Detta säkerställer att uppdragets omfattning förblir inriktad på prioriterade risker och undviker onödig utvidgning.

Internrevisorer bör tydligt definiera omfattningen utifrån de **väsentliga risker som har identifierats** för att undvika att uppdragets omfattning oavsiktligt kan utvidgas utöver de ursprungliga målen. Målen bör överensstämma med organisationens riskaptit, strategi, mål och prioriteringar. Skälen för att inkludera eller utesluta specifika ämnesrelaterade krav ska dokumenteras i uppdragsplaneringen. Detta tillvägagångssätt bidrar till att skydda revisionsprocessens integritet, säkerställer en effektiv resursanvändning och ger en fokuserad försäkran om organisationens mest angelägna risker.

Om Institutet för internrevisorer

Institute of Internal Auditors (IIA) är en internationell yrkesorganisation som har mer än 265.000 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 theiia.org.

Ansvarsfriskrivning

IIA publicerar detta dokument för informations- och utbildningsändamål. Detta material är inte avsett att ge definitiva svar på specifika individuella oms tändigheter och är därför endast avsett att användas som en vägledning. IIA rekommenderar att man söker oberoende expertrådgivning relaterad till en specifik situation. IIA tar inget ansvar för någon som enbart förlitar sig på detta material.

Upphovsrätt

© 2025 The Institute of Internal Auditors, Inc. Alla rättigheter förbehållna. För tillstånd att återge, vänligen kontakta Copyright@theiia.org.

Augusti 2025



The Institute of
Internal Auditors

Global Headquarters

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

