Cybersäkerhet

Topical Requirement

Användarvägledning

The Institute of
Internal Auditors

Innehåll

Översikt över ämnesrelaterat krav

Ämnesrelaterade krav (topical requirements) är en obligatorisk del av Internationella Standarder för yrkesmässigt utförande av internrevision (International Professional Practices Framework®) tillsammans med Globala standarder för internrevision (Global Internal Audit Standards™) och global vägledning. Institute of Internal Auditors kräver att de ämnesrelaterade kraven används tillsammans med Globala standarderna, som utgör yrkesmässig praxis. I denna vägledning finns hänvisningar till standarderna som en källa för mer detaljerad information.

Ämnesrelaterade krav formaliserar hur internrevisorer hanterar vanliga riskområden för att säkerställa kvalitet och likformighet inom yrket. Ämnesrelaterade krav lägger fast en grund och ger relevanta kriterier för genomförandet av säkringsuppdrag inom området för ett ämnesrelaterat krav (standard 13.4 Utvärderingskriterier). Ämnesrelaterade krav är obligatoriska för säkringsuppdrag och rekommenderas för utvärdering i samband med rådgivningsuppdrag. Ämnesrelaterade krav är inte avsedda att täcka alla möjliga aspekter som bör beaktas vid utförandet av säkringsuppdrag; de är snarare tillämpliga för att ge en minimiuppsättning av krav för att möjliggöra en konsekvent och tillförlitlig bedömning av området.

De ämnesrelaterade kraven har en tydlig koppling till IIA:s Trelinjemodell och de Globala standarderna för internrevision. Ledning, riskhantering samt styrning och kontroll är huvudkomponenterna i Ämnesrelaterade krav som följer Standard 9.1 Förstå processerna för ledning, riskhantering samt styrning och kontroll. Med hänvisning till Trelinjemodellen utövar styrelsen/ det styrande organet ledning, riskhantering utövas av den andra linjen samt styrning och kontroll utövas av den första linjen. Ledning utövas både i första och andra linjen. Internrevision utövas i tredje linjen som en oberoende och objektiv leverantör av säkringstjänster och rapporterar till styrelsen/det styrande organet (princip 8 Tillsyn av styrelsen).

Relevans, risk och yrkesmässig bedömning

Ämnesrelaterade krav måste följas när internrevisionen utför säkringsuppdrag inom områden där det finns ett ämnesrelaterat krav eller när aspekter av det ämnesrelaterade kravet identifieras i andra säkringsuppdrag.

I standarderna poängteras betydelsen av riskbedömning som en viktig del av revisionschefens planering. För att fastställa vilka säkringsuppdrag som ska ingå i intern-revisionsplanen krävs att organisationens strategier, mål och risker bedöms minst en gång varje år (Standard 9.4 Internrevisionsplan). Vid planeringen av enskilda säkringsuppdrag

måste internrevisorn bedöma de risker som är relevanta för uppdraget (Standard 13.2 Riskbedömning).

När området för ett ämnesrelaterat krav identifieras under internrevisionens riskbaserade planeringsprocess och ingår i internrevisionsplanen måste de krav som anges i det ämnesrelaterade kravet användas för att bedöma området inom de tillämpliga uppdragen. Dessutom, när internrevisorer utför ett uppdrag (antingen ingående i planen eller inte ingående i planen) och delar av ett ämnesrelaterat krav identifieras, måste en bedömning göras om det ämnesrelaterade kravet ska utgöra en del av uppdraget. Slutligen, om ett uppdrag genomförs som inte har varit en del av revisionsplanen och som omfattar ett område där det finns ett ämnesrelaterat krav, måste en bedömning göras om det ämnesrelaterade kravet ska tillämpas. Yrkesmässigt omdöme spelar en nyckelroll när ett ämnesrelaterat krav ska användas. Internrevisionschefens beslut om vilka uppdrag som ska ingå i revisionsplanen ska baseras på riskbedömningar (Standard 9.4 Internrevisionsplan). Dessutom använder internrevisorer yrkesmässigt omdöme för att avgöra vilka aspekter som ska tillämpas inom respektive uppdrag (Standarderna 13.3 Uppdragets mål och omfattning; 13.4 Utvärderingskriterier; 13.6 Arbetsprogram). Bilaga A ”Praktiska exempel” beskriver hur internrevisorn avgör om det ämnesrelaterade kravet ska användas.

Dokumentation finns av att tillämpligheten för varje del i det ämnesrelaterade kravet har bedömts. Denna måste bevaras, inklusive en motivering till varför något krav har uteslutits. Överensstämmelse med det aktuella kravet måste dokumenteras med hjälp av internrevisorns yrkesmässiga omdöme enligt beskrivningen i standard 14.6 Uppdragsdokumentation.

Även om Ämnesrelaterat krav för Cyber-säkerhet ger en grund till vilka kontrollåtgärder som måste tas hänsyn till, kan organisationer som bedömer cyberrisken som mycket hög behöva bedöma ytterligare aspekter.

Om en internrevisionschef bedömer att intern-revisionsfunktionen inte har den kunskap som krävs för att utföra uppdrag inom ett område som omfattas av ett ämnesrelaterat krav, kan uppdragsarbetet läggas ut till en extern leverantör (standarderna 3.1 Kompetens, 7.2 Internrevisionschefens kvalifikationer, 10.2 Förvaltning av personalresurser). Även då innebär inte utkontraktering att internrevisionsfunktionen befrias från sitt ansvar för att uppfylla de ämnesrelaterade kraven. Internrevisionschefen behåller det yttersta ansvaret för att säkerställa överensstämmelse. Om internrevisionschefen bedömer att internrevisionens resurser är otillräckliga måste internrevisionschefen dessutom informera styrelsen om effekterna av otillräckliga resurser och hur eventuella resursbrister kommer att åtgärdas (standard 8.2 Resurser).

Genomföra, dokumentera och rapportera

När internrevisorer tillämpar de ämnes-relaterade kraven måste de också följa standarderna och utföra sitt arbete i enlighet med område V: Att utföra internrevisionstjänster. Standarderna inom område V beskriver planering av uppdrag (princip 13 Planera uppdraget effektivt), genomförande av uppdrag (princip 14 Utföra uppdraget) och kommunicera

resultatet av uppdraget (princip 15 Kommunicera resultaten från uppdraget och följa upp handlingsplanerna).

Omfattningen av det ämnesrelaterade kravet

kan dokumenteras antingen i revisionsplanen eller i uppdragets arbetsdokument baserat på revisorernas yrkesmässiga bedömning. Ett eller flera internrevisions-uppdrag kan täcka kraven. Dessutom är det inte säkert att alla krav är relevanta. Bevis för att det ämnesrelaterade kravet har bedömts vara tillämpligt måste dokumenteras och bevaras, inklusive en motivering som förklarar eventuella undantag.

Dokumentationsmallen i bilaga C kan användas som referens och för att dokumentera det arbete som internrevisorer utför.

När internrevisorerna tillämpar de aktuella kraven måste de också följa standarderna och utföra sitt arbete i enlighet med område V: Utföra internrevisionstjänster. Standarderna inom område V beskriver planering av uppdrag (princip 13 Planera uppdrag på ett effektivt sätt), genomförande av uppdrag (princip 14 Genomföra uppdragsarbete) och kommunikation av uppdragsresultat (princip 15 Kommunicera uppdragsresultat och övervaka handlingsplaner).

Omfattningen av det aktuella kravet kan dokumenteras antingen i internrevisionsplanen eller i uppdragets arbetsdokument baserat på revisorernas professionella bedömning. Ett eller flera revisionsuppdrag kan täcka kraven. Dessutom är det inte säkert att alla krav är tillämpliga. Bevis för att det aktuella kravet har bedömts vara tillämpligt måste bevaras, inklusive en motivering som förklarar eventuella undantag.

Den frivilliga mallen i bilaga C kan användas som referens och för att dokumentera det arbete som internrevisorerna utför.

Kvalitetssäkring

Standarderna kräver att internrevisionschefen utvecklar, implementerar och upprätthåller ett program för kvalitetssäkring och förbättring som omfattar alla aspekter av internrevisions-funktionen (Standard 8,3 Kvalitet). Resultaten måste kommuniceras till styrelsen och den verkställande ledningen. I kommunikationen ska internrevisionsfunktionens överens-stämmelse med standarderna och uppfyllelse av prestationsmål rapporteras.

Överensstämmelse med de ämnesrelaterade kraven kommer att utvärderas i kvalitets-bedömningar. För att förbereda sig för en kvalitetsgranskning kan internrevisorerna använda mallen som finns i bilaga C.

Cybersäkerhet

Cybersäkerhet är ett brett ämne som berör de flesta tekniska aspekter av en organisation. Förutom informationsteknik är cybersäkerhet ofta en del av organisationens affärs-processer, vilket kräver att internrevisorer bedömer cyberrelaterade risker när de planerar, avgränsar och utför säkrings-uppdrag.

National Institute of Standards and Technology (NIST), som är en del av USA:s handelsdepartement, definierar cyber-säkerhet som "förmågan att skydda eller försvara

cyberrymden från cyberattacker". Ämnesrelaterat krav för Cybersäkerhet fokuserar på den externa skyddsmur som organisationer bygger upp för att minska riskerna från obehöriga användare och skadliga cyberhot. Cybersäkerhet är en delmängd av den övergripande informationssäkerheten, som NIST definierar som "Skyddet av information och informations-system från obehörig åtkomst, användning, avslöjande, störning, modifiering eller förstörelse för att skapa konfidentialitet, integritet och tillgänglighet".

Det ämnesrelaterade kravet för cybersäkerhet inkluderar:

A. Ledning – tydligt definierade grundläggande mål och strategier för cyber-säkerhet som stödjer organisationens mål, policyer och rutiner.

B. Riskhantering – processer för att identifiera, värdera, hantera och övervaka cyberhot, inklusive en process för att snabbt eskalera cyberrisker.

C. Styrning och kontroll – av ledningen etablerade och regelbundet utvärderade åtgärder för att minska cyberrisken.

Överväganden

Internrevisorer kan använda följande överväganden för att underlätta sin bedömning av delar i det ämnesrelaterade kravet för cybersäkerhet. Dessa överväganden, som refererar till kraven, är förklarande och inte obligatoriska. Internrevisorer bör lita på sitt professionella omdöme vid bedömningar.

Överväganden om styrning och ledning

För att bedöma hur styr- och ledningsprocesserna tillämpas på cybersäkerhet kan internrevisorerna granska:

A. Att det finns en formaliserad strategisk plan samt beslutade mål för cybersäkerhet, inklusive underlag för att styrelsen regelbundet (vanligtvis kvartalsvis) behandlar uppdateringar om cybersäkerhets från ansvarig för informationssäkerheten, till exempel chefen för informationssäkerhet (CISO). Underlag kan utgöras av rapportering om:

- Uppföljning av att de strategiska målen uppnås.
- Budgetbehov för att uppnå mål och syfte med cybersäkerhetsarbetet.
- Fokus på risker samt intern styrning och kontroll, inklusive framsteg i förbättringsarbetet.
- Nyckelindikatorer (KPI) för att mäta framgång.
- Resurser som behövs för att anställa, utbilda och utveckla cybersäkerhetspersonal.

B. Policyer, förfaranden och annan relevant dokumentation som används för att leda cybersäkerhetsprocesser, inklusive:

- Policyer som ses över och uppdateras minst en gång per år. Framväxande cyberrisker kan göra det nödvändigt att se över och uppdatera oftare.
- En process för att avgöra om policyer och rutiner är tillräckliga för att stödja cybersäkerhetsverksamheten.
- Allmänt vedertagna ramverk (NIST, COBIT etcetera) för att stärka cybersäkerhetsprocesser och intern styrning och kontroll.

C. Att det finns roller och ansvarsområden som stödjer cybersäkerhetsmålen, inklusive att ansvarig för cybersäkerhet rapporterar till en nivå i organisationen som har tillräcklig synlighet för att få organisatoriskt stöd.

- En process för att regelbundet bedöma kunskaper, färdigheter och förmågor hos personal som har cybersäkerhetsroller.

D. Dokumentation av samverkan med relevanta intressenter (t.ex. högsta ledningen, operativ verksamhet, riskhantering, HR, juridik, regelefterlevnad, strategiska leverantörer och övriga, inklusive kommunikation om befintliga och framväxande cyberrisker samt kända sårbarheter. Dokumentation av kommunikation kan inkludera mötesprotokoll, rapporter eller e-postmeddelanden.

Överväganden om riskhantering

För att bedöma hur riskhanteringsprocesser tillämpas på cybersäkerhetsmål kan internrevisorer granska:

A. Hur organisationen bedömer och hanterar cybersäkerhetsrisker, bland annat hur hot och sårbarheter har:

- Ursprungligen identifierats och rapporterats.
- Analyserats för att värdera risken för att organisationens mål inte nås.
- Begränsats, inklusive handlingsplaner för att minska risken till en acceptabel nivå.
- Övervakats, inklusive plan för löpande rapportering tills hot är fullt ut hanterade.

B. Hur organisationen får regelbunden information om hantering av cybersäkerhetsrisker från t.ex. IT, riskhantering, HR, juridik, regelefterlevnad, operativ verksamhet, redovisning och finans. Ett tvärfunktionellt cybersäkerhetsteam eller en IT-styrkommitté kan användas för att inhämta information.

C. Hur organisationen har tilldelat, en individ eller ett team, ansvar och mandat för hantering av cybersäkerhetsrisker.

- Den eller de ansvariga bör regelbundet (kvartalsvis, månadsvis eller vid behov) informera hela organisationen om utvecklingen av cybersäkerhetsrisker och kan även inkludera resursbehov för riskreducering.

D. Processer för eskalering av cybersäkerhetsrisker, bland annat hur hot- eller risknivån värderas, tilldelas och prioriteras. Granskningen kan omfatta identifiering av:

- Organisationens definierade risknivåer – så som hög, måttlig och låg - med detaljerade förklaringar av varje risknivå och eskaleringsförfaranden för varje riskkategori.
- Förteckning över de cybersäkerhetsrisker som identifierats och status för hantering av varje riskhändelse.
- Tillämpliga lagar, förordningar och krav på efterlevnad.
- Både finansiella riskkonsekvenser och icke-finansiella riskkonsekvenser (t.ex. ryktesrisker).

E. Processen för att kommunicera cybersäkerhetsrisker till ledning och medarbetare, vilket inkluderar:

- Regelbunden (minst en gång om året) utbildning i cybersäkerhet för medarbetare, t.ex. oannonserade, simulerade nätfiskekampanjer för att testa och följa upp medvetenheten.
- Uppdateringar om hantering av befintliga cybersäkerhetsproblem, med förväntade slutförandedatum.
- Övervakning av bristande regelefterlevnad inklusive uppdateringar till styrelse och ledning.
- Omvärdera hot när organisationens riskaptit och risktolerans förändras.

F. Processer som organisationen har implementerat avseende incidenthantering och återställning, vilket inkluderar:

- En dokumenterad plan som ses över och uppdateras i takt med att verksamheten förändras över tid. Planen bör omfatta följande:
  - Hur incidenter upptäcks och rapporteras.
  - Hur incidenter begränsas för att förhindra ytterligare skada.
  - Hur organisationen kommer att agera för att återuppta verksamheten.
  - Hur incidenter kommer att analyseras för att dra lärdom om hur liknande händelser i framtiden kan förhindras.
- Periodisk (minst årligen) testning (skrivbordsövning) och rapportering av resultatet till högsta ledningen och relevanta intressenter. Testningen kan resultera i handlingsplaner.

Styr- och kontrollprocesser - överväganden vid tillämpning

För att bedöma hur styr- och kontrollprocesser tillämpas på cybersäkerhetsmål kan internrevisorn granska:

A. Ledningens strategi för att bygga upp en effektiv intern styrning och kontrollmiljö för cybersäkerhet, bland annat:
    - Bedömning och implementering av intern styrning och kontroll som krävs för att både reducera risker och skydda känsliga, kritiska, personliga eller konfidentiella data, med beaktande av organisationens process för riskbedömning.
    - Resursbehov för att upprätthålla viktiga cybersäkerhetskontroller.
    - Beakta kontroller hos leverantörer som en del av styr- och kontrollmiljön, vilket inkluderar att granska SOC-rapporter (Service Organisation Controls) från leverantörer innan affärsrelationen inleds och under hela relationens löptid.
    - Periodisk testning av att kontrollerna fungerar på ett sätt som minskar riskerna och stödjer uppfyllelsen av cybersäkerhetsmålen.
    - Process för att åtgärda brister i intern styrning och kontroll och hantera gjorda iakttagelser från internrevisionsfunktionen eller andra säkringsleverantörer (till exempel penetrationstest).

B. Organisationens process för rekrytering och utbildning av cybersäkerhetspersonal, inklusive hur organisationen identifierar möjligheter att öka cybersäkerhetspersonalens förmåga att stödja teknisk kunskap och förbättra organisationens medvetenhet om nya risker.
    - Exempel på detta är deltagande i utbildning, i grupper för kunskapsutbyte och fortbildning som inkluderar cyberrelaterade certifieringar.

C. Ledningens process för att kontinuerligt identifiera, prioritera, övervaka och rapportera framväxande hot och sårbarheter inom cybersäkerhet med fokus på den dagliga verksamheten. Granskningen kan omfatta att processer har etablerats för att bedöma hot och sårbarheter relaterade till ny eller framväxande teknik, såsom användning av artificiell intelligens.

D. Ledningens processer och kontroller för att hantera och skydda IT-tillgångar under hela livscykeln, inklusive anskaffning, användning, underhåll och avveckling av hårdvara, mjukvara och leverantörstjänster. Hårdvara omfattar servrar, nätverksutrustning (t.ex. routrar eller brandväggar), stationära datorer, bärbara datorer, mobiltelefoner, surfplattor och kringutrustning. Programvara omfattar operativsystem (t.ex. Windows), programvara för resursplanering, applikationer, antivirusprogram och annat. Överväganden kan inkludera:
    - Organisationens användning av kryptering, antivirusprogram, hantering av mobila enheter, komplexa lösenordskrav, virtuella privata nätverk (VPN) / Zero Trust Networking (ZTN) för autentisering och periodisk uppdatering av firmware.
    - En process för att säkerställa att hårdvara som företaget har anskaffat har en lämplig säkerhetskonfiguration både vid implementering och vid utrangering.
    - Databasrelaterade kontroller som inkluderar begränsning av användar- och administratörsåtkomst, säkerställande av användning av kryptering,

säkerhetskopiering och testning av databaser samt förekomsten av starka nätverkssäkerhetskontroller.

- Hur hot mot eller sårbarheter beaktas i livscykeln för systemutveckling (SDLC).
- De metoder som används av utveckling, säkerhet och drift (DevSecOps) för att säkerställa att processen för programvaruutveckling inkluderar cybersäkerhet för att proaktivt identifiera sårbarheter.

E. Processer som används för att stärka cybersäkerheten, inklusive:

- Konfiguration av säkerhetsinställningar för att minimera cybersäkerhetsrisker.
- Administration av att mobila enheter (inklusive användning av e-post och applikationer) är konfigurerad för att minska riskerna och kan fjärrstyras om en användares enhet har tagits över.
- Användning av kryptering för data "i vila", t.ex. information som lagras på en hårddisk, eller data "i transit", t.ex. kryptering av e-postmeddelanden.
- Uppdatera servrar eller programvara (t.ex. ett operativsystem) med de senaste säkerhetsversionerna.
- Hantering av användaråtkomst, t.ex. användning av multifaktorautentisering (MFA) och unika användar-ID med komplexa lösenord som löper ut med jämna mellanrum.
- Kontroller är på plats för att avgöra om tillgänglighet och resursutnyttjande fungerar tillfredsställande, vilket möjliggör översyn och analys av potentiella cybersäkerhetsproblem som hotar prestandan.
- Integrering av cybersäkerhet i systemutveckling (SDLC) för att identifiera och åtgärda sårbarheter avseende cybersäkerhet innan programvaran tas i produktion.

F. Nätverksrelaterade kontroller som säkrar organisationens skalskydd, inklusive hur organisationen använder:

- Segmentering av nätverk.
- Brandväggar.
- Kontroll av användaråtkomst.
- Begränsningar för både externa och interna anslutningar.
- Kontroller kring sakernas internet (IoT) för sammankopplade nätverk.
- Intrångsdetekterings-/preventionssystem för att förhindra, upptäcka och återhämta sig från cybersäkerhetsattacker.

G. Säkerhetskontroller för tjänster som exempelvis e-post, webbläsare, videokonferenser, meddelanden (Zoom, MS Teams och andra), sociala medier, moln och fildelningsprotokoll. Kontrollerna kan omfatta begränsning av användningen av vissa filtillägg (t.ex. Excel-filer) och multifaktorautentisering för fildelning.

Bilaga A. Exempel på tillämpning

Följande exempel beskriver scenarier där det ämnesrelaterade kravet avseende cybersäkerhet kan vara tillämpligt:

Exempel 1: Cybersäkerhet identifieras för ett revisionsuppdrag som ingår i revisionsplanen.

När internrevisionsfunktionen slutför sin riskbaserade planeringsprocess och inkluderar ett eller flera uppdrag om cybersäkerhet i revisionsplanen, är det ämnesrelaterade kravet obligatoriskt vid genomförandet av sådana uppdrag. Överensstämmelse kan uppnås genom att inkludera kraven i ett eller flera uppdrag i revisionsplanen.

Cybersäkerhet är omfattande och det är inte säkert att alla delar är tillämpliga i alla uppdrag. När internrevisorn tillämpar yrkesmässig bedömning och fastställer att ett eller flera krav i det ämnesrelaterade kravet avseende cybersäkerhet inte är tillämpliga, måste internrevisorn dokumentera och bevara skälen till att dessa krav utesluts. Orsaken till att utesluta vissa krav kan t.ex. vara att internrevisionsfunktionen utför olika cybersäkerhetsgranskningar på rotationsbasis eller har fastställt att risken i uppdraget är låg.

Exempel 2: Cybersäkerhetsrisker identifieras under ett revisionsuppdrag som inte är direkt relaterad till cybersäkerhet.

Internrevisorn kan identifiera cybersäkerhetsrisker när den bedömer en process som inte är direkt relaterad till cybersäkerhet. Exempelvis kan internrevisorn bedöma leverantörsreskontraprocessen i ett uppdrag som inte är inriktat på cybersäkerhet och har inte identifierat cybersäkerhetsrisker som en del av uppdraget när de planerar. Efter att ha genomfört den inledande informationsinsamlingen bedömer dock internrevisorn att sådana risker bör ingå till exempel identifierar cybersäkerhetsrisker i samband med webbaserad inhämtning av offerter (standard 13.2 Riskbedömning av uppdrag).

När relevanta risker har identifierats måste internrevisorn beakta det ämnesrelaterade kravet avseende cybersäkerhet och avgöra vilka delar som är tillämpliga. I det här exemplet kan revisorn utesluta processen för styrning av cybersäkerhet eller hantering av cybersäkerhetsrisker. I uppdragets dokumentation måste orsaken till att krav har uteslutits framgå.

Exempel 3: Ett cybersäkerhetsuppdrag som inte ingick i den ursprungliga revisionsplanen.

Intressenter som styrelsen, ledningen eller en tillsynsmyndighet kan be internrevisorer att bedöma cybersäkerhetsrisker utanför den ursprungliga revisionsplanen. Till exempel när organisationer utsätts för en cyberattack kan styrelsen begära att internrevisionen ska bedöma cybersäkerhetskontroller. Det ämnesrelaterade kravet är då tillämpligt, kraven måste bedömas och eventuella undantag dokumenteras.

Bilaga B. Mappning till ramverk

Organisationen kan ha sitt eget cybersäkerhetsarbete med hjälp av ramverk för riskhantering och styrning, till exempel COBIT eller NIST. Internrevisorer kan redan ha utvecklat revisionsprogram och testprocedurer baserade på dessa ramverk. Internrevisorer bör stämma av sina planerade kontrolltester för cybersäkerhet mot det aktuella kravet för att säkerställa tillräcklig täckning. I diagrammet nedan kartläggs det ämnesrelaterade kravet för cybersäkerhet med tre vanligt förekommande ramverk: NIST Cybersecurity Framework 2.0, COBIT 2019 och NIST 800-53. Dessa ramverk har kartlagts eftersom de är lättillgängliga utan kostnad.

Krav för styrning	Referensramverk		
	NIST CSF 2.0	NIST 800-53	COBIT 2019
A. Strategi och mål för cybersäkerhet har fastställts och uppdateras regelbundet. Uppdateringar om uppfyllandet av målen för cybersäkerhet har kommunicerats regelbundet och följts upp av styrelsen, inklusive resurser och budgetöverväganden för att genomföra strategin.	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. Policyer och rutiner för cybersäkerhet finns och har uppdaterats regelbundet för att stärka styrning och kontroll.	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. 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.	GV.RR-02; GV.RR-04; GV.SC-02; GV.OC-02	PM-13; AT-2; AT-3	EDM02; APO01; APO07

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.	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
Krav för riskhantering	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A. Organisationens riskbedömnings- och riskhanteringsprocesser har omfattat identifiering, analys, hantering och övervakning av cybersäkerhetshot och dess effekt på uppfyllelsen av strategiska mål.	GV.RM-01; GV.RM-03; GV.OC-01	AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
B. Cybersäkerhetsrisker har hanterats inom hela organisationen (exempelvis IT, riskhantering, HR, juridik, regelefterlevnad, drift, leverantörskedja, redovisning, finans och övriga delar.	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. 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.	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. 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.	GV.RM; ID.RA; RS.MA-04	CA-7; RA-3; RA-7	EDM03; APO01, APO10; APO12
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.	PR.AT; GV.RR.01; GV.RR-04; GV.PO	AT-2	APO01; APO02; EDM03; MEA03
F. Organisationen har implementerat en process för hantering av cybersäkerhetsincidenter som omfattar upptäckt, hantering, återställning och analys efter en incident. Processen har testats regelbundet.	RS; RC	IR-4; IR-5; IR-6; IR-7; IR-8; IR-10; SA-15	DSS02; DSS03; DSS04; DSS05.07

Krav på styrnings- och kontrollprocesser	NIST CSF 2.0	NIST 800-53	COBIT 2019
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.	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. En process har etablerats som inkluderar utbildning för att utveckla och upprätthålla teknisk kompetens för cybersäkerhet. Processen har utvärderats regelbundet.	PR.AT-01; PR.AT-02; GV.RR-03	AT-2; AT-3; IR-2; PM-14	APOO7; DSS04
C. En process finns för att kontinuerligt övervaka och rapportera nya hot och sårbarheter samt identifiera, prioritera och genomföra aktiviteter för att förbättra cybersäkerheten.	ID.RA-02; ID.RA-03, ID.RA-04	CA-7; PM-31; RA-5	DSS03.05
D. Cybersäkerhet ingår i livscykelhanteringen av alla IT-tillgångar, inklusive hårdvara, mjukvara och leverantörstjänster.	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. Processer finns för att stärka cybersäkerhet, inklusive konfiguration, slutanvändaradministration, kryptering, patchning, åtkomsthantering samt övervakning av tillgänglighet och prestanda. Cybersäkerhet ska beaktas vid mjukvaruutvecklingen (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. Nätverkskontroller finns, exempelvis segmentering, användning och placering av brandväggar, begränsning 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).	PR.IR; DE.CM-01	AC-6; AC-17; AC-18; AC-20; SC-7; SC-10; CA-8	DSS05.02

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

Bilaga C. Dokumentationsmall

Internrevisorer förväntas göra en yrkesmässig bedömning när de avgör om kraven är tillämpliga utifrån riskbedömningen och på lämpligt sätt dokumentera undantag från vissa krav. Det ämnesrelaterade kravet kan dokumenteras i revisionsplanen eller i uppdragets arbetsdokumentation baserat på revisorns professionella bedömning. Ett eller flera revisionsuppdrag kan täcka kravet. Dessutom är det inte säkert att alla krav är tillämpliga. Den utskrivbara mallen nedan är ett alternativ för att dokumentera överensstämmelse med det ämnesrelaterade kravet för cybersäkerhet, men mallen är inte obligatoriskt att använda.

Cybersäkerhet - Styrning

Krav	Genomförd täckning eller motivering för uteslutning	Dokumentation Referens
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 resurser 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 kunskaperna, färdigheterna och förmågorna 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, verksamheten, riskhantering, HR, juridik, regelefterlevnad, leverantörer och övriga.		

Cybersäkerhet - Riskhantering

Krav	Genomförd täckning eller motivering för uteslutning	Dokumentation Referens
A. Organisationens riskbedömnings- och riskhanteringsprocesser omfattar identifiering, analys, begränsning 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, leveranskedja, redovisning, finans och övriga delar.		
C. Roller och ansvarsför 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 för riskhantering 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.		

Krav	Genomförd täckning eller motivering för uteslutning	Dokumentation Referens
F. Organisationen har implementerat en process för hantering av cybersäkerhetsincidenter som omfattar upptäckt, hantering, återställning och analys efter en incident. Processen har testats regelbundet.		

Cybersäkerhet – Styrning och kontroll

Krav	Genomförd täckning eller motivering för uteslutning	Dokumentation Referens
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.		
C. En process finns för att kontinuerligt övervaka och rapportera nya hot och sårbarheter samt identifiera, prioritera och genomföra aktiviteter för att förbättra cybersäkerheten.		

Krav	Genomförd täckning eller motivering för uteslutning	Dokumentation Referens
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, begränsning 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 kommunikationstjänster 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 ledare inom standarder, certifieringar, utbildning, forskning och teknisk vägledning. För mer information www.theiia.org.

Ansvarsfriskrivning

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

Upphovsrätt

Februari 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