# Organisatorisk motståndskraft

## Ämnesrelaterade krav

## Topical Requirement

The Institute of Internal Auditors

# Ämnesrelaterade krav för organisatorisk motståndskraft

International Professional Practices Framework® består av globala internrevisionsstandarder™ (Global Internal Audit Standards™), ämnesrelaterade krav och global vägledning. Ämnesrelaterade krav är obligatoriska och ska användas tillsammans med standarderna och utgör yrkesmässig praxis.

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

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

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:

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

Alla delar av ett ämnesrelaterat krav behöver inte vara tillämpliga i varje uppdrag och vissa kan uppfyllas genom andra tillvägagångssätt. Om delar av området utesluts ska detta motiveras, dokumenteras och bevaras.  Följsamhet med ämnesrelaterade krav kommer att utvärderas under kvalitetsutvärderingen.

Mer information finns i the Organizational Resilience Topical Requirement User Guide för det ämnesrelaterade kravet om organisatorisk motståndskraft.

## Organisatorisk motståndskraft

Organisatorisk motståndskraft definieras av International Organization for Standardization som förmåga att absorbera och anpassa sig i en föränderlig miljö för att kunna fortsätta uppnå sina mål, överleva och utvecklas(ISO 22316:2017). Även om denna definition sätter en tydlig ambitionsnivå varierar det i praktiken mycket mellan olika organisationer hur de förutser, reagerar på, anpassar sig till och återhämtar sig från förändring och störning. Eftersom organisatorisk motståndskraft omfattar strategiska, operativa, tekniska, mänskliga, sociala och finansiella dimensioner kan vissa organisationer absorbera förändringar effektivt, medan andra kämpar för att göra det eller väljer andra tillvägagångssätt när de ställs inför osäkerhet.

Organisatorisk motståndskraft är ett samlingsbegrepp som omfattar risker som på ett betydande sätt kan störa eller försämra en organisations förmåga att leverera sina kärnprodukter och -tjänster, upprätthålla intressenters förtroende eller nå sina strategiska mål. Dessa risker kan uppstå till följd av plötsliga händelser (t.ex. naturkatastrofer, cyberattacker och geopolitiska konflikter), långvariga miljörelaterade påfrestningar (t.ex. resursbrist och folkhälsokriser) eller förändringar i omvärlden (t.ex. tekniska störningar, regeländringar och försämrat anseende).

Dessa risker kan också vara stegvisa förändringar eller långsamt växande påfrestningar som med tiden äventyrar organisationens stabilitet och anpassningsförmåga. Stegvis ökande risker som dessa kan rutinmässigt förbises. Motståndskraftiga organisationer förutser och anpassar sig till både plötsliga och subtila risker för att bli framgångsrika.

Inneboende riskfaktorer som ökar hot mot motståndskraft inkluderar mycket komplexa verksamheter, globaliserade leveranskedjor, centraliserad infrastruktur eller datasystem, begränsad tillgång till arbetskraft, volatila marknadsförhållanden och starkt beroende av kritiska tredje parter eller geografiska platser. Organisationer som verkar i sektorer med hög förtroende eller som är föremål för ingående granskning av myndigheter kan också möta risker som i sig är högre på grund av påverkan på allmänheten och regelefterlevnadskrav.

Organisatorisk motståndskraft fokuserar på att hantera risker före, under och efter en störning. Internrevisorer utvärderar ofta processer och kontroller inom informationsteknik (IT) när det gäller kontinuitetshantering och återgång till ordinarie verksamhet. En kontinuitetsplan beskriver de åtgärder som en organisation vidtar för att upprätthålla kritiska funktioner och återgå till normalläge när en kris inträffar. En krisplan beskriver hur organisationer ska återställa sina IT-system, kritiska data och verksamhet efter en störande händelse för att återuppta normal verksamhet.

Organisatorisk motståndskraft, som omfattar båda dessa planer, kräver strategisk planering, riskhantering, effektivt ledarskap och kultur samt organisationsövergripande processer för intern styrning och kontroll. Att ha starka styr- och kontrollprocesser för organisatorisk motståndskraft gör det inte bara möjligt för organisationer att kontinuerligt förutse, förbereda sig för, svara på och anpassa sig till förändringar, utan gör det också möjligt för dem att överleva och frodas.

# Utvärdering och bedömning av organisationens motståndskraft Styrning, riskhantering, ledning och kontrollprocesser

Detta krav ger en konsekvent och heltäckande metod för att bedöma utformningen och implementeringen av styrningen av organisationens motståndskraft, riskhantering och kontrollprocesser. Kraven utgör en miniminivå för bedömning av organisationens motståndskraft.

## Styrning och ledning

### Krav

Internrevisorer måste bedöma följande aspekter av styrning och ledning av organisationens motståndskraft:

A. En formell organisationsstrategi som tar hänsyn till åtgärder som stärker motståndskraft fastställs av ledningen, antas och övervakas av styrelsen och omfattar de operativa, tekniska och finansiella delar som krävs för att hantera förändringar och upprätthålla verksamheten. Målen för motståndskraft ligger i linje med organisationens övergripande strategi för riskhantering.

B. Om det förekommer regelbunden kommunikation till styrelsen kring hur målen för de åtgärder som stärker motståndskraften uppnås. Detta säkerställer att motståndskraft är inkluderat i strategisk tillsyn, långsiktiga planeringsprocesser, successionsplanering och organisationens kultur, samt de resurs- och budgetöverväganden som krävs för att stödja kritiska affärsaktiviteter har gjorts.

C. Policies och rutiner för kritiska operativa, tekniska och finansiella processer upprättas och granskas, testas och uppdateras regelbundet vid behov för att stärka kontrollmiljön.

D. En insatsledningsstruktur upprättas och används för att övervaka och stödja organisationens mål för motståndskraft. Den omfattar beslutshierarkier, kommunikations- och eskaleringsprotokoll samt ledarskapets och verksamhetens roller och ansvarsområden.

E. En process etableras för att periodiskt validera de kompetenser som krävs för att lyckas med att upprätta motståndskraft samt ompröva kompetensen hos de personer som fyller kritiska roller i processer för att upprätthålla motståndskraft.

F. En process etableras för att säkerställa att alla relevanta interna och externa intressenter identifieras, prioriteras och engageras i att upprätta informations- och rapporteringsstrukturer för att uppnå organisationens mål för motståndskraft. Intressenter kan vara högsta ledningen, verksamheten, riskhantering, IT, leveranskedja/upphandling, anläggningar, personal, ekonomi, juridik, interna och externa leverantörer av säkringstjänster (inklusive internrevision), regelefterlevnad, PR, kritiska leverantörer, kunder, tillsynsmyndigheter och övriga.

## Riskhantering

### Krav

Internrevisorer måste bedöma följande aspekter av riskhanteringen avseende organisationens motståndskraft:

A. Risker relaterade till organisationens motståndskraft identifieras, bedöms och hanteras regelbundet inom hela organisationen. Riskerna kartläggs i förhållande till organisationens strategiska mål. Processen för hantering av risker avseende motståndskraft innefattar utvärdering av väsentliga processer.

B. Ansvarsfördelning och ansvar för riskhantering avseende organisatorisk motståndskraft är tydligt definierade. En utpekad person eller ett team har i uppdrag att regelbundet övervaka och rapportera om hur motståndskraftsrisker hanteras i organisationen, inklusive de resurser som krävs för riskreducering och identifiering av nya hot mot organisationens motståndskraft.

C. En process är etablerad för att övervaka risknivåer för organisationens motståndskraft (nya eller tidigare identifierade) och snabbt eskalera de som når en nivå som anses oacceptabel enligt organisationens etablerade riktlinjer för riskhantering och risktolerans eller tillämpliga lagar och förordningar. Effekterna av organisatorisk motståndskraftsrisk beaktas.

D. Ledningen har implementerat och testar regelbundet en process för att agera på och återhämta sig från krishändelser, störningar och nödsituationer. Processen för incidenthantering och återhämtning omfattar upptäckt, prioritering, begränsning, återhämtning och analys efter incidenten. Incidenthanteringsstrategin omfattar scenarioanalyser och periodiska stresstester mot potentiella händelser.

## Kontrollprocesser

### Krav

Internrevisorer måste bedöma följande aspekter av kontrollprocesserna relaterade till organisationens motståndskraft:

A. En process finns på plats för att identifiera kritiska tredjepartsleverantörer (även återförsäljare) och fastställa de lägsta lagernivåer som krävs för att upprätthålla väsentliga verksamheter. Processen omfattar även att upprätthålla en uppdaterad förteckning över alternativa leverantörer.

B. Data som är kritisk för verksamheten identifieras och klassificeras. Dataklassificering omfattar identifiering av var data finns, vilka som ska ha åtkomst, hur åtkomst sker samt om den säkerhetskopieras och kan återställas i en nödsituation.

C. Kritiska IT-kontroller och kontinuerlig övervakning har införts för att minska informationssäkerhetsriskerna (inklusive cyberrelaterade risker) och säkerställa att känslig data skyddas under kriser, störningar och nödsituationer. Kontrollerna och den kontinuerliga övervakningen omfattar hotinformation i realtid och begränsning av åtkomst till endast behöriga användare.

D. Kritiska IT-tillgångar är inventerade. Tillgångarna omfattar hårdvara, mjukvara och tjänster som krävs för att stödja verksamheten under kriser, störningar och nödsituationer.

E. Planer för kontinuitet och återställning har upprättats och innehåller definierade roller för utsedd personal och grupper. Planerna testas regelbundet (t.ex. en skrivbordsövning) och resultaten, inklusive förbättringsmöjligheter, rapporteras till styrelsen och den verkställande ledningen.

F. En process har etablerats för att anpassa arbetsmiljön under kriser, störningar och nödsituationer.

G. En process har etablerats för att kontinuerligt övervaka och rapportera framväxande hot och sårbarheter som kan påverka organisationens motståndskraft. Processen används för att identifiera, prioritera och implementera möjligheter att stärka organisationens motståndskraft, inklusive system för visselblåsning eller insamling av riskinformation.

H. En process har etablerats för att utbilda och träna personalen i organisatorisk motståndskraft för att säkerställa att policyer och rutiner är kända och efterlevs samt att åtgärder vidtas när kriser, störningar och nödsituationer inträffar. Processen omfattar övningar där störningsscenarier simuleras.

I. En process har etablerats för att säkerställa att nödvändiga operativa, mänskliga, tekniska och finansiella resurser budgeteras och finns tillgängliga under kriser, störningar och nödsituationer. De finansiella resurser som krävs för att stödja organisationens motståndskraft analyseras regelbundet och kommuniceras till styrelsen.

J. En process har etablerats för att utvärdera kriser, störningar och nödsituationer. I processen ingår att analysera utvärderingar efter incidenter genom att dra lärdomar och integrera dessa i organisationens kris- och kontinuitetsplanering.

## 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 av Certified Internal Auditor® (CIA®) över hela världen. IIA grundades 1941 och är erkänt över hela världen som internrevisionsprofessionens ledare inom standarder, certifieringar, utbildning, forskning och teknisk vägledning. Gå till theiia.org för mer information.

## Upphovsrätt



April 2026

The Institute of Internal Auditors

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