



IIA'S DE TRE LINJERNAS MODELL

En uppdatering av de tre ansvarslinjerna

Innehållsförteckning

Inledning	1
Princip 1: Styrning och ledning	2
Princip 2: Styrelsens roll	2
Princip 3: Ledningens, första och andra linjens roller	3
Princip 4: Tredje linjens roller	3
Princip 5: Tredje linjens oberoende	3
Princip 6: Skapa och skydda värde	3
Nyckelroller i modellen	5
Styrelsen	5
Ledningen	5
Internrevisionen	6
Externa leverantörer av säkringstjänster	6
Relationer mellan de olika nyckelrollerna	7
Mellan styrelsen och ledningen (både första och andra linjen)	7
Mellan ledningen (både första och andra linjen) och internrevision	7
Mellan internrevisionen och styrelsen	8
Mellan samtliga roller	8
Att använda modellen	9
Struktur, roller och ansvar	9
Tillsyn och försäkrans	9
Samordning och anpassning	10

INLEDNING

Organisationer består av människor som samverkar mot ett gemensamt mål och som verkar i en alltmer osäker, komplex, sammankopplad och föränderlig värld. Det finns ofta flera intressenter med olika, föränderliga och ibland konkurrerande intressen. Intressenterna överlåter organisatorisk tillsyn till ett styrande organ, styrelsen, som i sin tur delegerar resurser och befogenheter till organisationens ledning för att vidta lämpliga åtgärder, inklusive riskhantering.

Detta innebär att organisationer behöver effektiva strukturer och processer för att göra det möjligt att nå uppsatta mål, samtidigt som de stödjer en stark styrning, ledning och riskhantering. Då styrelsen får rapporter från ledningen gällande aktiviteter, resultat och prognoser är både styrelsen och ledningen beroende av att det finns en internrevision som tillhandahåller oberoende och objektiv försäkran samt ger råd för att främja och underlätta organisationens utveckling och förbättring. Styrelsen är ytterst ansvarig för organisationens styrning och ledning, något som möjliggörs genom såväl styrelsens agerande som ledningens och internrevisionens handlingar och beteende.

De tre linjernas modell hjälper organisationer att identifiera de strukturer och processer som bäst hjälper organisationen att nå sina mål och främjar en stark styrning och riskhantering. Modellen gäller alla organisationer och är optimerad genom att:

- Anta ett principbaserat tillvägagångssätt och anpassa modellen för att passa organisatoriska mål och förutsättningar.
- Fokusera på det bidrag som riskhanteringen innebär för att uppnå mål och skapa värde, samt säkra och skydda tillgångar.
- Tydliggöra de roller och ansvar som representeras i modellen och relationerna mellan dem.
- Säkerställa att aktiviteter och mål är anpassade till intressenternas prioriterade intressen.

Nyckelbegrepp

Organisation – En organiserad grupp av aktiviteter, resurser och människor som arbetar mot gemensamma mål.

Intressenter – Grupper och individer vars intressen betjänas eller påverkas av organisationen.

Styrelsen – Det organ som har ansvar för organisationens framgång gentemot dess intressenter.¹

Ledning – Individer, arbetslag, och stabsfunktioner som tilldelats ett ansvar för att tillhandahålla produkter eller tjänster till organisationens kunder.

Internrevision – Funktion som arbetar oberoende från ledningen för att tillhandahålla försäkran och insikt om lämplighet och effektivitet av organisationens ledningsprocess, riskhantering samt styrning och kontroll.

De tre linjernas modell – Modellen är tidigare känd som de tre försvarslinjerna.

Intern styrning och kontrol – Processer utformade för att ge rimlig försäkran i arbetet med att nå uppsatta mål.

¹ Notera att i en enrådgivningsmyndighet finns ingen styrelse utan denna roll innehas av generaldirektören, som också är högsta ledning för verksamheten.

PRINCIPER FÖR DE TRE LINJERNAS MODELL

Princip 1: Styrning och ledning

Styrning och ledning av en organisation kräver lämpliga strukturer och processer som möjliggör:

- En styrelse som verkar med integritet, ledarskap och öppenhet och är **ansvarig** inför organisationens intressenter.
- En ledning som vidtar **åtgärder** (inklusive riskhantering) för att uppnå organisationens mål genom riskbaserat beslutsfattande och nyttjande av resurser.
- En oberoende internrevision som genom **försäkran och råd** skapar tydlighet och förtroende samt främjar och underlättar kontinuerliga förbättringar genom grundliga utredningar och värdeskapande kommunikation.

Princip 2: Styrelsens roll

Styrelsen säkerställer att:

- Lämpliga strukturer och processer finns för en effektiv styrning och ledning.
- Organisatoriska mål och aktiviteter anpassas till intressenternas prioriterade intressen.

Styrelsen:

- Delegerar ansvar och förser ledningen med de resurser som krävs för att uppnå målen för organisationen samtidigt som de säkerställer att lagar, regler och etiska förväntningar uppfylls.
- Upprättar och övervakar en oberoende, objektiv och kompetent internrevisionsfunktion, som genom försäkran och råd skapar tydlighet och förtroende i arbetet med att nå de uppsatta målen.

Nyckelord

Riskbaserat beslutsfattande - En välplanerad process som inkluderar analys, planering, åtgärder och uppföljning samt tar hänsyn till osäkerhetsfaktorer som skulle kunna påverka möjligheten att uppnå de uppsatta målen.

Försäkran - En objektiv analys av fakta i syfte att tillhandahålla en oberoende utvärdering av organisationens ledningsprocess, riskhantering samt styrning och kontrollprocesser.

Princip 3: Ledningens, första och andra linjens roller

I ledningens arbete med att uppnå organisationens mål ingår både första och andra linjens roller². Första linjen är främst kopplad till leveransen av produkter eller tjänster till organisationens kunder och inkluderar stödfunktioner.³ Andra linjens uppdrag är främst att stödja organisationen i arbetet med att hantera identifierade risker.

Första och andra linjens roller kan kombineras eller hållas åtskilda. Vissa av de roller som finns inom andra linjen kan innehas av olika specialister som tillhandahåller expertis, support och uppföljning samt ger stöd till de som arbetar i första linjen. Inom andra linjen kan fokus ligga på specifika mål för riskhantering såsom efterlevnad av lagar och regler och ett acceptabelt etiskt beteende, en god intern styrning och kontroll, informationssäkerhet och teknisk säkerhet, hållbarhet och kvalitetssäkring. Alternativt kan andra linjen omfatta ett bredare ansvar för riskhantering såsom organisationsövergripande riskhantering (ERM). Ansvaret för att hantera riskerna är dock en del av första linjens ansvar respektive ledningens ansvar.

Princip 4: Tredje linjens roller

Internrevisionen tillhandahåller en oberoende och objektiv försäkran och ger råd om ändamålsenlighet och effektivitet avseende styrning och ledning samt riskhantering⁴. Detta gör internrevisionen genom att tillämpa systematiska och strukturerade processer, sakkunskap, erfarenhet och kompetens. Internrevisionen rapporterar sina resultat till ledningen och styrelsen i syfte att främja och underlätta en kontinuerlig förbättring. I detta arbete, kan internrevisionen beakta resultatet av arbete med försäkran genomfört av andra interna och externa leverantörer av säkringstjänster.

Princip 5: Tredje linjens oberoende

Att internrevisionen är fri från ledningsansvar är avgörande för dess objektivitet, auktoritet, och trovärdighet. Oberoendet säkras genom att internrevisionen är ansvarig inför styrelsen, har obegränsad tillgång till de personer, resurser och data som internrevisionen behöver för att kunna utföra sitt arbete tillsammans med frihet från partiskhet eller inblandning i planeringen och leveransen av revisionstjänster.

Princip 6: Skapa och skydda värde

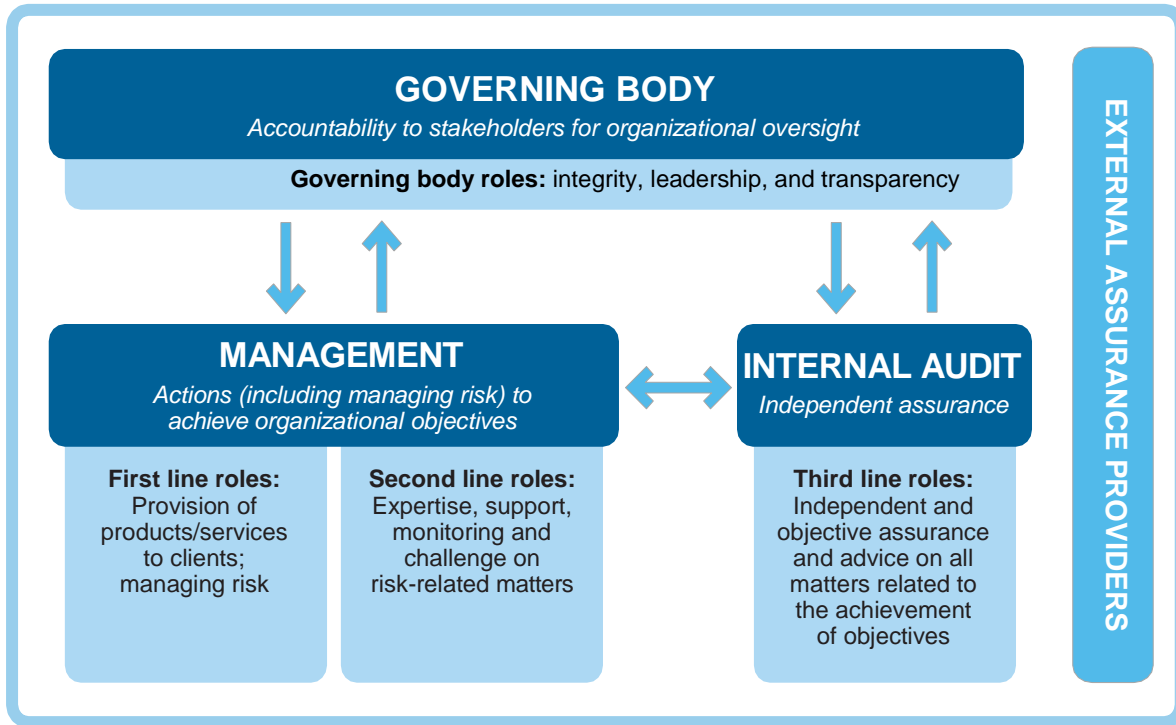
Genom att alla roller arbetar tillsammans bidrar de till att skapa och skydda organisationens värde i linje med intressenternas prioriterade intressen. Detta uppnås genom kommunikation, samarbete och samverkan, vilket säkerställer tillförlitligheten, samstämmigheten och transparensen i den information som behövs för ett riskbaserat beslutsfattande.

² Begreppen "första linjen", "andra linjen" och "tredje linjen" behålls från den ursprungliga modellen för igenkänningsfaktorns skull. Men begreppet "linje" är inte avsett att beteckna strukturella element utan används endast för att särskilja olika roller. Logiskt sett utgör styrelsen också en "linje" men denna benämning har inte införts för att undvika förvirring. Numreringen (första, andra, tredje) innebär inte att det är ett arbete som sker i sekvenser, utan alla uppgifter genomförs parallellt.

³ Vissa anser att stödfunktioner som exempelvis HR, administration och förvaltningstjänster är en del av andra linjen, men i de tre linjernas modell anses första linjen omfatta verksamhet både i "front office" och "back office" medan andra linjens roller avser de kompletterande aktiviteter som sker med fokus på riskrelaterade frågor.

⁴ I vissa organisationer identifieras också andra roller för tillsyn, inspektion, utredning, utvärdering och korrigerande. Dessa kan vara en del av internrevisionsfunktionen eller vara separata delar.

The IIA's Three Lines Model



KEY: ↑ Accountability, reporting ↓ Delegation, direction, resources, oversight ↔ Alignment, communication coordination, collaboration

NYCKELROLLER I MODELLEN

Hur ansvaret fördelas inom en organisation skiljer sig ofta åt, men i texten nedan beskrivs några övergripande roller i de tre linjernas modell och deras huvudsakliga ansvar.

Styrelsen

- Har ansvar för tillsyn över organisationen gentemot intressenter.
- Samarbetar med intressenter för att följa upp att deras intressen tillgodoses och kommunicerar öppet hur väl uppsatta mål nås.
- Arbetar för att inrätta en kultur i organisationen som främjar ett önskat etiskt beteende och ansvarstagande.
- Fastställer organisatorisk struktur för styrning och ledning, samt inrättar de stödjande kommittéer som bedöms behövas.
- Delegerar ansvaret för verksamheten och tillhandahåller resurser till ledningen i dess arbete med att uppnå organisationens mål
- Bestämmer vilken riskaptit organisationen ska ha och utövar tillsyn över den riskhantering som sker.
- Tillsier att verksamheten följer lagar och regler och verkar i enlighet med uppställda etiska normer.
- Inrättar och följer upp en oberoende, objektiv och kompetent internrevision.

Ledningen

Första linjens roller

- Leder och styr verksamheten inklusive riskhantering med tilldelade resurser i syfte att uppnå organisationens mål.
 - Upprätthåller en kontinuerlig dialog med styrelsen och rapporterar om planerat, faktiskt och förväntat resultat kopplat till målen för organisationen och planerat, faktiskt och förväntat resultat av riskhanteringen.
 - Etablerar och underhåller lämpliga strukturer för att leda och genomföra verksamheten och hantera identifierade risker.
 - Säkerställer efterlevnad av lagar, regler och etiska förväntningar.
-

Andra linjens roller

- Tillhandahåller sakkunskap, support, uppföljning och stöd i verksamhetens riskhantering. Arbetet inkluderar:
 - Utveckling, implementering och kontinuerlig förbättring av organisationens riskhanteringsarbete, inklusive intern kontroll, inom processer, system och på enhetsnivå.
 - Uppföljning av hur väl målen för riskhantering nås; såsom efterlevnad av lagar och regler, etiska normer, en god intern styrning och kontroll, informationssäkerhet, teknisk säkerhet, hållbarhet och kvalitetssäkring.

- Tillhandahåller analyser och rapporter om i vilken grad som organisationens riskhantering bedöms som tillräcklig och effektiv.

Internrevisionen

- Är ansvarig gentemot styrelsen och oberoende från organisationens ledning.
- Lämnar oberoende och objektiv försäkran och råd till ledning och styrelse avseende lämplighet och effektivitet i organisationens ledningsprocess, riskhantering samt styrning och kontrollprocesser, i syfte att stödja organisationen i arbetet med att nå sina mål och främja och underlätta en kontinuerlig förbättring av verksamheten.
- Vidtar de åtgärder som bedöms nödvändiga för att upprätthålla objektivitet och oberoende samt rapporterar eventuella hinder för att bibehålla sitt oberoende eller sin objektivitet till styrelsen.

Externa leverantörer av säkringstjänster

- En extern leverantör av säkringstjänster tillhandahåller en ytterligare försäkran genom att:
 - Genomföra de lagenliga och regelmässiga granskningar som förväntas och som finns för att skydda de externa intressenternas intressen.
 - Genomföra uppdrag på begäran från ledning och styrelse i syfte att komplettera de interna säkringstjänsterna.

RELATIONER MELLAN DE OLIKA NYCKELROLLERNA

Mellan styrelsen och ledningen (både första och andra linjen)

Styrelsen anger vanligtvis en organisations inriktning

genom att fastställa vision, uppdrag, värderingar och riskaptit. Styrelsen delegerar sedan, tillsammans med de nödvändiga resurserna, ansvaret för att uppnå organisationens mål till ledningen. Ledningen rapporterar i sin tur planerade, faktiska och förväntade resultat tillsammans med risk- och riskhanteringsrapporter till styrelsen.

Nyckelord

Verkställande direktör (VD) – Den högsta chefen i organisationen med ansvar för verksamheten. I en statlig myndighet motsvaras detta av generaldirektören (GD).

I vilken grad styrelsens och ledningens roller överlappar varandra varierar mellan organisationer och innebär att en styrelse kan vara mer eller mindre involverad i strategiska och operativa frågor för verksamheten. Det kan vara styrelsen eller ledningen som tar fram verksamhetens strategi eller så sker det gemensamt. I vissa organisationer är VD (GD) medlem av styrelsen, ibland till och med dess ordförande. Oavsett vilken struktur som en organisation har måste det finnas en väl etablerad kommunikation mellan högsta ledningen och styrelsen. Det är vanligtvis VD (GD) som är den naturliga punkten för denna kommunikation, men även andra höga chefer kan ha en kontinuerlig kontakt med styrelsen. Det kan inom organisationen finnas en önskan om eller krav på att chefer inom andra linjen, såsom Chief Risk Officer (CRO) eller Chief Compliance Officer (CCO) ska ha en direkt rapporteringslinje till styrelsen. En sådan struktur är helt i linje med principerna för de tre linjernas modell.

Mellan ledningen (både första och andra linjen) och internrevision

Det är internrevisionens oberoende från ledningen som säkerställer att internrevisionen kan vara objektiv och opartisk i planering och genomförande av sitt uppdrag samt ges full och obehindrad tillgång till de personer, de resurser och den information som krävs. Internrevisionen är ansvarig inför styrelsen, men detta innebär inte att internrevisionen ska vara isolerad från verksamheten, utan det måste finnas en regelbunden samverkan mellan internrevisionen och organisationens ledning för att säkerställa att det internrevisionsarbete som sker är relevant och anpassat till organisationens strategiska och operativa behov. Genom sitt arbete bygger internrevisionen upp en kunskap och förståelse för organisationen, vilket bidrar till att de säkringstjänster som genomförs och de råd som internrevisionen lämnar är relevanta och sker i rollen som betrodd rådgivare och strategisk partner. Det krävs också en samverkan och en kommunikation mellan internrevisionen och såväl första som andra linjen för att säkerställa att onödigt dubbelarbete inte sker eller att luckor uppstår.

Mellan internrevisionen och styrelsen

Internrevisionen är ansvarig inför och beskrivs ibland som styrelsens "ögon och öron" i organisationen.

Styrelsen ansvarar i sin tur för tillsynen av internrevisionen, vilket kräver att styrelsen säkerställer att en oberoende internrevisionsfunktion inrättas, anställer och avskedar internrevisionschefen (CAE), fungerar som den primära kontakten för CAE⁵, beslutar om revisionsplanen och resurser för dess genomförande, att styrelsen är mottagare av rapporter från CAE och CAE har direkta tillgång till styrelsen, inklusive enskilda möten mellan styrelse och CAE utan närvaro från ledningen.

Nyckelord

**Chief Audit Executive (CAE) –
Internrevisionschef eller liknande titel.**

Mellan samtliga roller

Både styrelse, ledning och internrevision har sina tydligt utpekade ansvarsområden, men all verksamhet ska vara i linje med organisationens mål. Grunden för ett framgångsrikt arbete är regelbunden och effektiv samordning, samarbete och kommunikation.

⁵ I administrativa frågor kan CAE rapportera till en lämplig chefsnivå inom organisationen.

ATT ANVÄNDA MODELLEN

Struktur, roller och ansvar

De tre linjernas modell är mest effektiv när den är anpassad till den enskilda organisationens mål och förhållanden. Hur en organisation är strukturerad och hur roller tilldelas bestäms av ledningen och styrelsen. Styrelsen kan också inrätta kommittéer för ytterligare tillsyn över särskilda ansvarsområden, såsom revision, risk, ekonomi, planering och ersättningssystem. Inom ledningen finns det troligtvis funktionella och hierarkiska strukturer och sannolikt en ökad grad av specialisering i takt med att organisationen växer i storlek och komplexitet.

Funktioner, grupper och till och med individer kan ha ansvar som hör till roller i såväl första som andra linjen. Styrning och uppföljning i andra linjen kan utformas så att oberoende från första linjen och från de högsta ledningsnivåerna säkerställs genom ett direkt ansvar inför och med direkt rapportering till styrelsen. De tre linjernas modell möjliggör att organisationen inrättar så många rapporteringslinjer mellan ledningen och styrelsen som behövs. I vissa organisationer, i synnerhet för särskilt reglerade finansinstitut, finns det lagkrav på att den här typen av rapporteringslinjer inrättas för att säkerställa ett tillräckligt oberoende. Även i dessa fall ligger ansvaret för att hantera risker i första linjen.

Andra linjens roller kan omfatta uppföljning, rådgivning, vägledning, testning, analys och rapportering i frågor som rör hantering av risker. I den mån dessa roller ger stöd, råd och rekommendationer till dem som har roller i första linjen och är integrerade i ledningens beslut och åtgärder blir andra linjen en del av ledningens ansvar och aldrig helt oberoende av ledningen, oavsett rapporteringslinjer och ansvarsområden.

Ett tydligt kännetecken för tredje linjen är dess oberoende från organisationens ledning. Principerna för de tre linjernas modell beskriver vikten och utformandet av internrevisionens oberoende som skiljer internrevisionen från andra funktioner och möjliggör det särskilda värdet av dess säkring och råd. Internrevisionens oberoende skyddas genom att den inte fattar beslut eller vidtar åtgärder som ingår i ledningens ansvarsområden inklusive hantering av risker och genom att inte utföra säkringstjänster för aktiviteter där internrevision har eller nyligen haft ansvar. I vissa organisationer kan CAE bli ombedd att ta ytterligare beslutsansvar över aktiviteter inom liknande kompetensområden, exempelvis inom regelefterlevnad eller ERM. Under sådana omständigheter blir internrevisionen i förhållandet till dessa verksamheter eller deras resultat inte oberoende. Då blir det nödvändigt för styrelsen att söka oberoende och objektiv försäkran från en kvalificerad extern part.

Tillsyn och försäkran

Styrelsen förlitar sig på rapporter från ledningen från första och andra linjen, internrevision och övriga, i sitt arbete med att utöva tillsyn och uppnå organisationens mål, för vilka de är ansvariga inför intressenterna. Ledningen ger värdefull försäkran (intyg) om planerade, faktiska och prognostiserade resultat samt om risk och riskhantering genom att dra nytta av direkt egen erfarenhet och andras expertis/sakkunskap. Andra linjen ger ytterligare försäkran avseende riskrelaterade frågor. Genom sitt oberoende från ledningen ger den försäkran som internrevisionen lämnar den högsta graden av objektivitet och förtroende utöver den som första

och andra linjen kan ge styrelsen oavsett rapporteringslinjer. Ytterligare försäkran kan också komma från externa leverantörer.

Samordning och anpassning

Effektiva ledningsprocesser kräver en ändamålsenlig ansvarsfördelning samt en väl utformad samordning och anpassning av aktiviteter genom samarbete, samverkan och kommunikation. Styrelsen efterfrågar, genom internrevisionens säkringstjänster, en bekräftelse på att ledningsstrukturer och processer är ändamålsenligt utformad och fungerar som avsetts.

OM IIA

The Institute of Internal Auditors (IIA) är den mest erkända företrädaren för internrevisorer samt leverantör av utbildningar, standarder, vägledning och certifieringar. IIA grundades 1941 och har idag mer än 200 000 medlemmar från mer än 170 länder och territorier. Föreningens globala huvudkontor ligger i Lake Mary, Florida, USA. För mer information besök, www.globaliia.org.

Ansvarsfriskrivning

IIA publicerar detta dokument i informations- och utbildningssyfte. Materialet är inte avsett att tillhandahålla definitiva svar på specifika förhållanden och endast avsett att fungera som vägledning. För specifika situationer rekommenderar IIA kontakt med expert på det specifika området. IIA tar inte ansvar för resultatet av att någon helt förlitat sig enbart på detta material.

Copyright

Copyright © 2020 Alla rättigheter förbehållna Institutet för Internrevisorer. För tillstånd att reproducera kontakta copyright@theiia.org.

July 2020



**The Institute of
Internal Auditors**

Global

Global Headquarters

The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 149
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101
www.globaliia.org