Företagsekonomiska institutionen

Stockholms universitet

Akademin för ekonomistyrning i staten
Rapport 2025:1

COSOs ramverk för intern kontroll och IIA:s trelinjemodell: controllerrollens expansion mot internrevisorsrollen?

Gunilla Eklöv Alander

COSOs ramverk för intern kontroll och IIA:s trelinjemodell: controllerrollens expansion mot internrevisorsrollen?

Gunilla Eklöv Alander, docent

Företagsekonomiska institutionen vid Stockholms universitet samt

Akademin för ekonomistyrning i staten

Innehållsförteckning

Förord

Att skriva något som ensamförfattare är ju sällan ett arbete som bygger enbart på de egna erfarenheterna. Jag vill därför tacka dem som haft särskild betydelse för rapportens innehåll och framställning. Mikael Holmgren Caicedo, docent vid Företagsekonomiska institutionen, Stockholms universitet, har bistått med orientering i forskningslitteraturen om controllerrollen i ekonomistyrningsfältet. Olof Arwinge, Ekon. Dr. och rådgivare vid KMPG, Magnus Gunnarsson, internrevisor vid Försvarets materielverk, och Johan Rippe, partner vid PwC, har bistått med diskussioner om trelinjemodellen, COSO och internrevisorns och controllerns funktioner inom dem. Charlotta Löfstrand Hjelm, internrevisor på Länsförsäkringar och Stina Nilsson Kristiansson, generalsekreterare och VD vid IIA Sweden, har förmedlat insikter särskilt om internrevisorsrollen i den interna styrningen. Karin Jonnergård, professor emerita, Ekonomihögskolan vid Lunds universitet, har bistått med kunskaper inom bolagsstyrning generellt och i Sverige i synnerhet. Det är så fint att få bolla tankar och idéer med er.

Fredrik Svärdsten Nymans, docent vid Företagsekonomiska institutionen, Stockholms universitet, har genom sitt redaktörskap fått rapporten att uppnå de krav som AES rapportserie bygger på, och har tillsammans med Mikael Holmgren Caicedo bidragit med sakkunnig granskning av manuskriptet. Akademin för ekonomistyrning i staten, AES, och dess medlemmar inom myndigheter och lärosäten har givit värdefull input på tidigare tankar och idéer, och jag ser fram emot fortsatta diskussioner. Jag är givetvis ansvarig för rapporten i dess helhet inklusive eventuella kvarvarande fel. Tack också till kollegorna, i synnerhet redovisningssektionen vid Företagsekonomiska institutionen, Stockholms universitet, för den härliga arbetsmiljö som vi odlar varje dag och som vi alla får dela.

Den här rapporten utgör en delrapport i den studie som benämns *Hybrid forms of auditing and comfort in digital transformations of corporate governance* (anslagsnummer P22-0015), finansierad av Handelsbankens forskningsstiftelser; Jan Wallanders och Tom Hedelius stiftelse, Tore Browaldhs stiftelse. Jag riktar ett varmt tack för denna finansiering, som möjliggjort framställningen av rapporten.

Stockholm i juli 2025,

Gunilla Eklöv Alander

1. Inledning

Den här skriften handlar om hur COSO och trelinjemodellen om intern kontroll och riskhantering hänger samman med avseende på controllerrollens inflytande över säkerheten i den finansiella rapporteringen som styrelsen ytterst ansvarar för. Det här området är intressant dels därför att traditionellt sett har internrevisorn betraktats som den som ger denna säkerhet till styrelsen (Rezaee, 1995), dels för att en utredning vi genomfört visar att internrevisorer saknas i drygt hälften av Stockholmsbörsens large cap-bolag och att i flertalet av dessa företag uppges controllers istället utföra sådant arbete som motsvarar internrevisorns funktion.[1]

Av forskningslitteraturen framgår att controllerns uppgifter har förändrats från att insamla och bearbeta information om företags ställning och resultat, om vad som varit, till att arbeta med framtidsinriktade redovisningsfrågor genom analyser och prognoser för beslutsfattande med strategisk bäring som aktiv deltagare i ledningsgrupper. Utvecklingen beskrivs i tidigare forskning dels som en breddning av controllerrollen (Friedman och Lyne, 1997; Burns och Baldvinsdottir, 2005; Byrne och Pierce, 2007), dels som en breddning av andra expertgruppers roller som ibland övertar funktioner som controllers traditionellt ansvarat för (Kurunmäki, 2004). I båda fallen beskrivs utvecklingen ibland som en fråga om hybridisering, där roller vidgas till att inkludera och ibland rentav överta delar av andras roller (Karlsson, Hersinger och Kurkkio, 2019), eller som en reduktion av inflytande över redovisningen i egenskap av business partner till en pedagogisk kapacitet, på rådgivningsbasis (Holmgren Caicedo, Mårtensson och Tamm Hallström, 2018). Dessa studier utgår emellertid från att controllerrollen och dess hybridisering befinner sig inom ekonomistyrning, eller att andra roller övertar uppgifter och ansvar från controllers, inom ekonomistyrning. Däremot framställs inte controllerrollen i denna litteratur som en granskningsfunktion. Om relationen mellan controllers och internrevisorer konstaterar också Nilsson och Olve (2018, sid. 76) följande: ”Även om ett nära samspel är önskvärt bör rollernas olika ansvar särskiljas tydligt”. Vår iakttagelse från utredningen, att controllern också är verksam inom det interna granskningsarbetet, saknas det alltså vetenskaplig kunskap

[1] Utredningen är framlagd i ett konferenspapper vid European Accounting Association Congress i Bukarest, maj 2024 (Eklöv Alander och Holmgren Caicedo, 2024). Enligt svensk bolagsstyrningskod måste företag som vill följa koden upplysa om vad de gör istället när de avstår från att ha en internrevisionsfunktion.

om. Mihret och Grant (2017) gör ett konstaterande om hur den vetenskapliga litteraturen framställer rapportering, styrning och revision som olika organisatoriska lager, där finansiell rapportering skapar möjligheter att styra aktiviteter genom att göra dem synliga och därmed mätbara, ekonomistyrning erbjuder verktyg och en begreppsapparat som möjliggör för ledningen att planera och styra organisationen, och revisorer ger ett betydelsefullt extra styrningslager genom att underkasta redovisningen en oberoende granskning. Det vi intresserar oss för är om en uppluckring av dessa lager är på gång och i så fall hur controllerns och internrevisorns roller förändras. Internrevisorer betraktas traditionellt som verksamma inom en profession eftersom de tillämpar professionella standarder för granskning och rapportering, vilket ska säkerställa en oberoende och högkvalitativ granskning för befattningshavare som behöver beslutsunderlag de kan lita på. I den här skriften undersöks möjligheterna till en rollöverskridande utvidgning, nämligen controllerrollens expansion in i internrevisorernas klassiska domäner att ge främst styrelsen säkerhet om den interna kontrollen och riskhanteringen över finansiell rapportering.

Utgångspunkten för studien är litteratur, både praktiskt orienterad och vetenskapligt framlagd, kring två vägledningar, dels det inflytelserika ramverk som beskriver systemet för intern kontroll och riskhantering, COSO, dels internrevisorernas modell för styrning av intern kontroll, riskhantering och revision, den så kallade trelinjemodellen. COSO beskrivs i den professionella litteraturen i termer av ett ramverk, medan trelinjemodellen beskrivs som en modell. COSO är ett ramverk för det interna kontroll- och riskhanteringssystemet för främst stora organisationer. Trelinjemodellen är en formalisering av de roller som arbetar med intern kontroll och riskhantering, och internrevision, och beskriver hur deras olika ansvarsområden ser ut, uppdelad i tre särskilda linjer för organisationers interna kontrollsystem. De båda vägledningarna kan alltså sägas hantera i princip samma sak, fast på olika sätt.

Av litteraturen kan noteras att kopplingarna mellan modellerna är oklara och i många fall tvetydiga. Dessutom, vid kontakter med befattningshavare med ansvar inom intern kontroll, riskhantering och också inom såväl intern som extern revision, blir det uppenbart att det föreligger väsentliga skillnader i uppfattningar om vad ramverket respektive modellen innebär. Vad mera är, de är ibland också okända, även om de tycks ha perkolerat in i praxis. Sådan kunskap är viktig eftersom intern kontroll, riskhantering och revisionen över dem är betydelsefulla för att organisationer ska kunna skaffa sig säkerhet över sin finansiella rapportering och i förlängningen för allmänhetens förtroende för de finansiella marknaderna. Då är det viktigt att meningen om deras innehåll och kopplingarna dem emellan är tydlig så

att de vägledningar och ramverk som är till för att stötta stora organisationers arbete med den interna kontrollen och riskhanteringen förstås på det sätt som upphovsmakarna avsett.

Skriften tar sin början i litteratur om de vägledningar som nämnt ovan, för att förstå deras innehåll och syften. Utifrån denna bakgrund diskuteras sedan hur COSO-ramverket och trelinjemodellen skiljer sig åt med avseende på de uppgifter som ska utföras och de krav som ställs på utförare, för att kunna jämföra controllerns och internrevisorns roller. Skriften avslutas med att diskutera COSO och trelinjemodellen med bäring på controllerollens expansion in mot sådan granskning som internrevisorer traditionellt sett utför.

2. COSO-ramverket för intern kontroll och riskhantering

Intern kontroll handlar om att skapa system som underlättar kontrollen över en verksamhet, så att organisationer har stöd att uppnå sina strategiska och finansiella mål. Intern kontroll väl utförd är ett system som hjälper organisationer att identifiera, analysera och adressera risker som skulle kunna äventyra måluppfyllelsen för de olika områden som organisationen satt upp för driften av sin verksamhet. Intern kontroll har vuxit i betydelse sedan cirka fyra decennier, i en omfattning som har föreslagits handla om en revisionsimplosion (Power, 2000), eller rent av en internrevisionsexplosion (Maijoor, 2000).

Den här redogörelsen kommer att handla om COSOs ramverk för intern kontroll, men ramverket är blott ett av flera. I Storbritannien används the UK Corporate Governance Code, tidigare benämnt ’the Combined Code’, eller helt enkelt the Turnbull Report’, efter ordföranden i den kommitté som utvecklade koden. Den har ett principbaserat sätt att vägleda kring intern kontroll i företag. Denna kod har nyligen uppdaterats och för att underlätta implementeringen träder dess delar just kring intern kontroll i kraft först 2026. I en tidig vägledning om hur koden kan användas av styrelseledamöter i företag står följande ord (ICAEW, 1999, sid 5, författarens översättning).

> Ett företags mål, dess interna organisation och den miljö i vilken den verkar, utvecklas kontinuerligt, och som ett resultat därav förändras också ständigt de risker det möter. Ett sunt system för intern kontroll beror därför på en uttömmande och regelbunden utvärdering av karaktären på och omfattningen av riskerna som företaget exponeras för. Eftersom vinster delvis är belöningen för framgångsrikt risktagande, är syftet med intern kontroll att hjälpa till med att styra och kontrollera riskerna på ett lämpligt sätt istället för att helt eliminera dem.

Samma anda av principbaserad och ändamålsenlig vägledning genomsyrar ännu den brittiska koden. McCrae och Balthazor (2000) kallar detta för framtvingad självreglering (eng. enforced self-regulation), vilken trots utmaningar tycks bestå i brittisk normgivning. I denna kod sker en fokusering på framförallt fyra delar i intern kontroll, riskhantering, kontrollmiljön och kontrollaktiviteter, information och kommunikation och slutligen övervakning. Här nämns också ett antal exempel på övervakningsaktiviteter, såsom självutvärdering av kontroller, rutiner för bekräftelse från personal om deras efterlevnad av riktlinjer och code of conduct, samt granskning genom intern revision eller ledningens granskning (se ICAEW, 1999, bilaga). Det finns alltså stora likheter mellan den brittiska koden och COSO.

COSO publicerades år 1992 av *the Committee of Sponsoring Organizations of the Treadway Commission (COSO)*. Dess ramverk *Internal Control—Integrated Framework* har kommit att

bli synonymt med intern kontroll och används av företag över hela världen genom global spridning och anses vara det ledande ramverket för intern styrning och kontroll. Ramverket har sitt ursprung i ett arbete som leddes av James C. Treadway runt år 1985, i samarbete med fem olika organisationer inom den privata sektorn i USA.[2] Dessa organisationer sponsrade tillsammans en kommission benämnd The National Commission on Fraudulent Financial Reporting. Ramverket var ett självregleringsinitiativ från näringslivets sida och stod klart 1992. Det har uppdaterats under 2013 och 2018. Genom Sarbanes-Oxley Act i USA blev COSOs ramverk en 'golden standard' bland övriga liknande ramverk för att hantera effektiviteten i intern kontroll över finansiell rapportering (Gupta, Sami, Zhang och Zhou, 2025). Ramverket ger en definition av intern kontroll och beskriver principerna för effektiv intern kontroll och vilka beståndsdelar som då ingår. Ramverkets syfte är att hjälpa företag dels att utforma, dels att underhålla system för intern styrning, kontroll och riskhantering. Där ingår också att ramverket ska kunna ge stöd till företag att anpassa sig till omvärldsförändringar, begränsa risker till en rimlig nivå och stödja beslutsfattande och styrning (COSO, 2013). Internrevisorernas förening (IIA Sweden) har tillsammans med PwC tagit fram en översättning av COSO:s ramverk (COSO, 2009), och den är godkänd av COSO för överensstämmelse med det ursprungliga ramverket. Intern kontroll har definierats på följande sätt av COSO och tar avstamp i styrelsens ansvar (COSO, 2009, sid. 4).

> Intern styrning och kontroll är en process, utförd av en organisations styrelse, ledning och annan personal, utformad för att ge rimlig försäkran om att målen uppfylls inom följande kategorier: effektivitet och produktivitet i verksamheten, tillförlitlig finansiell rapportering och efterlevnad av tillämpliga lagar och regler.

Processen syftar också till att stötta bolagets styrelse att uppfylla sitt ansvar, i Sverige enligt ABL och andra relevanta lagar, att se till att kraven på kontroll över bolagets bokföring, medelsförvaltning och bolagets övriga ekonomiska förhållanden efterlevs. Definitionen omfattar tre delområden, för att stötta företags arbete med att uppfylla sina mål. Först gäller det verksamhetens effektivitet och produktivitet, där resultat- och vinstmål samt skydd av företagets tillgångar ingår. Sedan gäller det tillförlitlighet i den finansiella rapporteringen, vilket sker i en process som leder till rimlig säkerhet vid produktion av finansiella rapporter, både för interna och externa syften. Det tredje området omfattar efterlevnad av de lagar och

[2] Där ingick the American Institute of Certified Public Accountants (AICPA), the American Accounting Association (AAA), Financial Executives International (FEI), the Institute of Internal Auditors (IIA), och the Institute of Management Accountants (IMA).

regler som ska tillämpas på företagets verksamhet. Dessa tre områden beskrivs också i termer av målsättningar (eng. objectives) och består helt kort av att skaffa säkerhet över verksamheten, rapporteringen och regelefterlevnaden. (COSO, 2013)

Fördelningen av ansvaret för den interna kontrollen mellan verkställande direktören och styrelsen sker så att den verkställande direktören har det operativa ansvaret medan styrelsen har en övervakande roll. Även om förhoppningarna på varje systems fördelar kan vara höga betonas i COSO:s ramverk att ett väl fungerande system för riskhantering och intern styrning och kontroll inte per automatik säkerställer företagets framgång eller överlevnad. Systemet, förutsatt att det fungerar väl, anses ge en rimlig försäkran om huruvida målen uppfylls och också ge information om både framsteg och brister i företagets styrning och kontroll (COSO, 2013).

Här i del 2 görs en genomgång av litteratur om COSO för att bedöma vilka uppgifter som enligt COSO-ramverket ska utföras, särskilt inom kontrollaktiviteter och övervakningsaktiviteter, och vilka krav som ställs på utförarens egenskaper. I avsnitt 2.4 sker en koppling till revisions- och granskningsuppgifter genom att jämföra vilka förutsättningar dessa båda roller har att utföra uppgifterna utifrån de krav som ställs på utförarens egenskaper. Där sammanfattas också resultatet av denna analys i tabell 1.

2.1 COSO-ramverkets fem grundläggande komponenter

COSO består av fem grundläggande komponenter; kontrollmiljön, riskhantering, kontrollaktiviteter, information och kommunikation, och övervakningsaktiviteter. *Kontrollmiljön* är central när det gäller att sätta tonen för hela organisationen. Dess utformning påverkar hur företagets anställda uppfattar företagets interna styrning och kontroll. Här skapas ordning och struktur och den utgör grunden för de övriga komponenterna inom den interna kontrollen. Genom denna kan ledningen sätta tonen för sin organisationsfilosofi och ledarstil (”the tone at the top”). Den här komponenten rymmer företagets etiska värderingar, synsätt på integritet och kompetens, kompetensutveckling och fördelningen av ansvar och befogenheter. (COSO, 2013) Den här komponenten kan också beskrivas som systemets själ (Eklöv Alander, 2019).

Inom *riskbedömningen* stöttas hur organisationen kan svara på de risker som uppstår genom den verksamhet som företaget bedriver. Organisationer skapar ofta mervärde genom att ta

risker, som uppstår både internt och härrör från omvärlden. Dessa risker är dessutom snabbrörliga, på grund av snabba förändringar i branschen både nationellt och på globala marknader. Den här komponenten bidrar till att företaget organiserar processer och aktiviteter för att värdera de risker som sammanhänger med förändringarna. Förändringarna härrör från företagets ekonomiska villkor, branschförändringar, företagets egen verksamhet och de lagar och förordningar som företaget har att följa. (COSO, 2013) Eftersom den här komponenten kan sägas bidra till att risker som verksamheten möter kan identifieras, analyseras och hanteras kan den liknas vid systemets nervsystem (Eklöv Alander, 2019).

Kontrollaktiviteterna är stommen i den interna styrningen och kontrollen, då de rymmer riktlinjer och rutiner så att ledningens styrning mot uppsatta mål säkerställs. De bidrar till att de åtgärder som krävs för att målen ska uppnås faktiskt också genomförs, och handlar om aktiviteter kring godkännanden, attester och avstämningar. Kontrollaktiviteter utformas för att kunna förhindra, upptäcka och korrigera avvikelser och brister, och består av de aktiviteter som fastställs genom regler och rutiner i syfte att mildra risker. De kan vara både manuella och automatiserade till sin karaktär. De innefattar verifikationer, resultatgenomgångar, och att se till att företagets tillgångar skyddas. En viktig del av kontrollaktiviteterna rör avgränsningen av personalens roller och uppgifter genom befattningsbeskrivningar med behörigheter och attesträttigheter. (COSO, 2013) Kontrollaktiviteterna kan därför sägas utgöra ryggraden i företagets interna kontrollsystem (Eklöv Alander, 2019).

Informationen och kommunikationen i det interna systemet för styrning och kontroll handlar om att skapa en välfungerande informationsförmedling i organisationen, vilket är en förutsättning för att alla medarbetare ska veta och förstå sina respektive ansvarsområden. Genom information och kommunikation kan ledningen förmedla sin filosofi och ledarstil. En effektiv kommunikation bidrar till att personalen känner till sitt ansvar och befogenheter och hur deras egen roll påverkar andra i företaget. Kommunikationen flödar nedåt i organisationen, från styrelse och ledning till anställda genom beslut och direktiv, men även uppåt, så att ledningen för sitt beslutsfattande får information om hur företaget presterar. Genom informationssystemet genereras rapporter över verksamheten och även en struktur för rapportering för att kunna hantera finansiell information och de regler som gäller för företaget. (COSO, 2013) Information och kommunikation kan med anledning av sin utformning och betydelse betraktas som systemets blodomlopp eftersom det kanaliserar och återför information inom organisationen (Eklöv Alander, 2019).

För att systemet ska kunna upprätthålla en hög kvalitet över tiden krävs *övervakning, uppföljning och utvärdering*, Denna komponent innefattar löpande övervakningsaktiviteter, uppföljningar och separata utvärderingar i syfte att se till att alla komponenter i det interna kontrollsystemet finns på plats och fungerar på ett ändamålsenligt sätt. Hur omfattande dessa aktiviteter ska vara och hur ofta de bör ske beror på hur risker värderas och hur effektiva rutinerna för övervakning, uppföljning och utvärdering är. Inom den här komponenten verkar den interna revisionen, men den kan också kompletteras av andra åtgärder. (COSO, 2013) Den här komponenten fungerar som kontrollsystemets ögon och öron (Eklöv Alander, 2019).

I skriften sker en analys, så som beskrivits ovan, av vilka uppgifter som ska utföras inom det interna kontrollsystemet, eftersom en förståelse söks för controllerns roll i att utföra arbetet med att skapa rimlig försäkran om att det interna kontrollsystemet fungerar på ett ändamålsenligt sätt. I analysen blir kontrollaktiviteterna och aktiviteter för övervakningen (monitoring) centrala, och därför ägnas ytterligare fokus på hur COSO framställer de här två komponenterna.

2.1.1 Utformningen av aktiviteter för kontroll och övervakning

COSO bygger på 17 principer och av dessa handlar tre principer om kontrollaktiviteter och två principer om övervakningsaktiviteter (COSO, 2013). COSO framställs som en struktur, men där roller och ansvar inte primärt beskrivs utan i centrum står istället de uppgifter som ska utföras i systemet (COSO, 2015).

Kontrollaktiviteter

Kontrollaktiviteter kan vara utformade för att manuellt och/eller automatiskt upptäcka och hindra risker som skulle kunna äventyra uppfyllandet av företagsledningens mål. Deras syfte är att verksamheten ska kunna möta de krav som ställs på kvalitet och tillförlitlighet (Espinosa-Jaramillo, 2024). Ansvarsområden och funktioner ska också vara separerade, och om detta inte är praktiskt genomförbart bör alternativa kontrollaktiviteter sättas in (Rezaee, 1995; Uwadiae, 2015). Kontrollaktiviteterna kan omfatta aktiviteter kring tillstånd och godkännanden, verifieringar, avstämningar, samt prestationsgranskningar (eng. performance reviews) (Uwadiae, 2015). Av COSOs tre principer för kontrollaktiviteter handlar den första principen om att organisationen har till uppgift att välja ut och utveckla kontrollaktiviteter som syftar till att begränsa risker så att mål ska kunna uppnås. Den här principen hanterar

riskerna kring manuella processer som hanteras av människor (Rezaee, 1995; Uwadiae, 2015). Bland aktiviteter förekommer till exempel att använda matriser och workshops för att kartlägga vilka risker som föreligger för kontrollaktiviteter, att bedöma befintliga kontrollaktiviteter och om de behöver utvecklas eller kompletteras, och bedöma kontrollaktiviteter för att separera ansvarsområden (Uwadiae, 2015).

Den andra principen handlar om att välja ut och utveckla generella kontrollaktiviteter över teknologi, främst informationsteknologi, för att stödja måluppfyllelsen. Kontrollaktiviteterna här handlar bland annat om att använda matriser för risk och kontroll vid dokumentationen av teknikberoende, utvärdera slutanvändarberäkningar, konfigurera infrastrukturen för IT för att stötta begränsad åtkomst och åtskillnad av arbetsuppgifter, konfigurera, processa, administrera och tillämpa mjukvaror och -åtkomst inom IT-systemet (Rezaee, 1995; Uwadiae, 2015).

Den tredje principen handlar om att kontrollaktiviteter ska baseras på rutiner och riktlinjer, så att de kontrollaktiviteter som utvecklats också dokumenteras och implementeras. Dessa riktlinjer ska fastställa vad som förväntas inom organisationen och de tillvägagångssätt genom vilka riktlinjerna kan verkställas. Detta kan utgöras genom att till exempel utveckla och dokumentera rutiner och riktlinjer, sprida kontrollaktiviteterna genom affärsenheter och deras chefer, och utföra regelbundna eller tillfälliga analyser av kontrollaktiviteter (Rezaee, 1995; Uwadiae, 2015).

Övervakningsaktiviteter

När det interna kontrollsystemet löpande underhålls och övervakas säkerställer organisationens styrelse och högsta ledning att problem identifieras och aktiviteter för att åtgärda dessa kan utföras kontinuerligt (Espinosa-Jaramillo, 2024). Detta kräver att resurser tillhandahålls för övervakningen, och också tillsättning av särskilda chefer som ges i uppgift att utföra övervakningen och underhålla kontrollerna över tid (Espinosa-Jaramillo, 2024). En del av övervakningen kan också utföras med teknologi så att tidig upptäckt av eventuella problem sker automatiskt (Espinosa-Jaramillo, 2024).

Den första av COSOs två principer om övervakningsaktiviteter handlar om att företagsledningen ansvarar för att organisationen väljer ut, utvecklar och löpande utvärderar om internkontrollkomponenterna är på plats och framförallt om de fungerar. Sådana utvärderingar kan ta formen av att vid bestämda tidpunkter granska sammansättningen av

övervakningsaktiviteter. Det kan också handla om att utforma och följa upp olika nyckeltal, ta fram en instrumentpanel (eng. dashboard) för olika visuella data, eller använda teknik för att stötta övervakningsaktiviteterna. Andra former av övervakningsaktiviteter kan utgöras av att utföra särskilda utvärderingar. Sådana utvärderingar eller granskningar kan också utföras av internrevisorer. (Deloitte, 2015)

Den andra principen om övervakningsaktiviteter handlar om att ta hand om de brister som upptäckts i arbetet med det interna kontrollsystemet, och fokuserar på organisationens utvärdering och kommunikation om brister i den interna kontrollen till dem som är ansvariga, inklusive högsta ledningen och styrelsen, för att inom rimlig tid genomföra rättelser av bristerna, efter vad som är lämpligt. Den här principen kan genomföras genom att bedöma och rapportera brister, att övervaka hur korrigeringar och rättelser görs, och att utforma vägledningar för hur brister ska rapporteras. (Deloitte, 2015)

COSO (2009) har också presenterat vägledningar om övervakning inom interna kontrollsystem, i syfte att övervakningen byggs in i systemen för att utföras löpande i stället för periodvis (årligen, tertial eller kvartal). Styrelsen har ett tillsynsansvar som kan utövas genom att skaffa en förståelse för de risker som föreligger om organisationens mål, vilka kontroller ledningen har för att mildra dessa risker, och hur ledningen övervakar att internkontrollsystemet löpande fungerar effektivt (COSO, 2009). Där framgår också hur styrelsen kan hantera de kontroller som ledningen inte kan övervaka på ett objektivt sätt. Exempel som ges är kontroller som chefer i ledningsgruppen utför själva eller som innefattar en risk för att dessa chefer kan kringgå dem. Övervakning av sådana kontroller kan styrelsen inrätta genom intern revision. Ramverket visar också på möjligheten att andra objektiva anställda i företagets ledning kan utföra dem (COSO, 2009). Det framgår inte i COSO-ramverket vilka de senare skulle kunna utgöras av, men om organisationen saknar en internrevisionsfunktion föreslås i vägledningen att styrelsen utökar sin övervakning, särskilt inom områden där ledningen kan sakna objektivitet (COSO, 2010). Detta kan ske genom sådana interaktioner som beskrivs härnäst.

2.2 Styrelsens olika källor för att bedöma övervakningssystemets effektivitet

Styrelsen kan använda olika källor för att bedöma om ledningen har inrättat ett effektivt övervakningssystem (COSO, 2010). Styrelsen kan ställa frågor till ledningen, ta del av internrevisionens arbete där sådan finns inrättad, anlita externa specialister, eller lyssna med de externa revisorerna. Övervakningsaktiviteterna kan också utföras av operativ personal inom organisationen. I vägledningen ges en princip för att bedöma vilka som kan komma ifråga och särskilt kompetens och objektivitet utgör då viktiga kriterier (COSO, 2009). Kompetens innebär att utföraren av övervakningsaktiviteterna behöver ha kunskap om internkontrollsystemet och dess processer, hur dessa är avsedda att fungera och hur det ser ut vid förekomst av en avvikelse i en viss kontroll. Objektivitet föreligger när utföraren av övervakningsaktiviteterna är fri från oro för personliga konsekvenser i samband med tester och annan övervakning, och också avsaknad av intresse för att på något sätt manipulera testerna för egen vinning. Objektiviteten kan bedömas utifrån utförarens kompensationsplan, rapporteringsskyldigheter och -vägar, hens personliga relationer, och hur utföraren på annat sätt kan påverkas av övervakningsaktiviteterna (COSO, 2010).

En kontrollövervakningsaktivitet kan vara att undersöka om metoder finns på plats för att utvärdera om internkontrollsystemet behöver förändras eller utvärderas på ett annat sätt pga ändrade risker (COSO 2009). Direkt information från en kontrollövervakningsaktivitet kan skaffas genom att observera kontroller som arbetar, att göra om dem (eng. reperform), eller på annat sätt direkt utvärdera deras funktion. Information för att kunna utöva övervakning kan också anskaffas indirekt, genom till exempel olika nyckeltal eller numeriska data, såsom intern statistik om verksamheten, indikatorer för nyckelrisker, nyckeltal (eng. KPI) och marknads- och branschdata (COSO 2009). Utförare av övervakning kan granska olika aspekter av interna kontroller genom att utföra tester genom sådana sedvanliga granskningsåtgärder som utvecklats inom revisionspraktiken såsom inspektion, observation, förfrågan, bekräftelse, göra om en beräkning, återupprepa en kontroll, eller genom analytiska procedurer.

Enligt COSO (2009) kan övervakningen så som framfördes ovan ske både löpande och periodvis med betoning på löpande kontroller. Löpande kontroller innebär att de funktioner som är ansvariga för internkontrollsystemets effektivitet fortlöpande får information från verksamheten. Där ingår rutiner såsom regelbundna tillsynsaktiviteter från ledningen,

jämförelser kollegor emellan, avstämningar och trendanalyser baserade på interna och externa data. Även automatiserade kontroller kan användas på löpande basis för att övervaka att kontroller eller transaktioner utförs på rätt sätt.

Digitala tekniker för kontroll kan också användas för övervakning (COSO, 2009). Exempel är löpande tester som sker enligt viss rutin för att förbättra effektiviteten hos information och bidra till att den kommer i rätt tid (tex “continuous controls monitoring”). De kan utföras genom att testa transaktioner på viss basis, och av viss omfattning, för att bedöma förekomst av avvikelser såsom transaktioner som överskrider vissa tröskelvärden avseende väsentlighet, eller jämföra mot uppsatta kriterier såsom betalningar som sker två gånger, eller om arbetsuppgifter separeras samt attesträttigheter följs.

Manuella kontroller behöver mer övervakning eftersom de ofta har fler avvikelser och brister än automatiska kontroller. Övervakningens innehåll och omfattning beror på informationsbehovet, och utformas utifrån hur ofta de manuella kontrollerna används, personalomsättning, och vilken träning och erfarenhet som personalen som utför kontrollerna har (COSO, 2010). Automatiserade kontroller å andra sidan fungerar på enhetligt och konsekvent sätt i en kontrollmiljö. De kan därför övervakas genom återkommande bekräftelser (eng. reconfirmations) vid ett utvalt tillfälle för att bedöma hur kontrollen fungerar. Då kan övervakningsaktiviteterna också innefatta IT avseende kontrollen, såsom programtester och säkerhet (COSO, 2010).

2.3 Vilka utför övervakningen och vilka egenskaper behöver de ha?

I COSO benämns personer som utför övervakande funktioner för ’utvärderare’ (eng. evaluators) (COSO, 2010). De kan vara internrevisorer, men kan även så som noterades i föregående avsnitt utföras av andra roller. De ska ha särskild utbildning och eventuellt stå utanför företagets verksamhet, eller utföras av personal som befinner sig i verksamheten och som fått till särskild uppgift att bevaka processer eller övervaka hur vissa kontroller fungerar inom ramen för sitt arbete. För att intern kontroll ska kunna implementeras på ett korrekt sätt i organisationer måste det finnas dels en djup förståelse för organisationens processer och risker, dels en välgrundad uppfattning om organisationens kultur med avseende på etikfrågor och också om hur ansvar tas om hand och fördelas inom organisationen (Espinosa-Jaramillo, 2024). Av COSO framgår att utvärderare ska ha kompetens, auktoritet och resurser för att

kunna utforma och implementera övervakning och också en god förståelse för de risker som kontrollerna syftar till att hantera (COSO, 2010). Vägledningen (COSO, 2010) ger exempel på hur en utvärderare kan använda information för att utvärdera om kontroller fungerar effektivt; såsom att bedöma den information en affärsområdescontroller (eng. divisional controller) ger till en regionchef som denne använder vid sin övervakning. Av COSOs ramverk framgår alltså att 'utvärderare' inte nödvändigtvis tycks behöva vara internrevisorer, så länge de har rätt kompetens och objektivitet samt auktoritet och resurser för sin uppgift. Utvärderaren ska kunna identifiera avvikelser i kontroller och analysera orsaken till dessa, och därför ha kunskap om kontrollens uppgift och de risker den har utformats för att hantera (COSO, 2010).

Utvärderares objektivitet diskuteras i termer av avstånd från operativt arbete med och ansvar för kontrollerna, från minst till mest objektiv i fyra steg (COSO, 2010). Minst objektiv är en person som utför granskning av sitt eget arbete; självgranskning (eng. self-review). I detta steg är en person minst effektiv i att ge grund för slutsatser om effektiviteten i interna kontroller. Trots bristen på objektivitet kan en självgranskning ändå ge nyttig information i ett tidigt skede om en brist i en kontrolls funktion (COSO, 2010). Nästa steg är kollegial granskning (eng. peer review), i vilken personen har viss grad av objektivitet. Steget därefter benämns överordnandegranskning (eng. supervisory review), vilket innebär att personen är ytterligare något mer objektiv. Båda dessa former kan ge god övervakning eftersom de utförs av personer som är nära kontrollen och därför kan identifiera brister och korrigera dessa i tid. Self-assessments[3] kan innefatta olika typer av övervakning med varierande styrka i objektiviteten hos övervakarna. Här ingår bedömningar utförda av allt från personer som har hand om kontrollen, till personer som inte är ansvariga för en kontroll och som utför peer review eller supervisory review. Mest objektiv är den som utför en opartisk granskning (eng. impartial review), och kan utföras av personer som är opartiska till hur kontrollen opererar. Så som framfördes ovan kan förutom internrevisorer enligt COSO även personer från andra organisatoriska enheter eller externa parter ha denna form av objektivitet. (COSO, 2010)

I vägledningen föreslås att företagsledningen etablerar ett övervakande ledarskap på organisationens verkställande nivå. För att fördela ansvaret för övervakningen ut över de områden som den interna kontrollen har till uppgift att täcka avgörs vilka personer som kan

[3] Den engelska beteckningen 'self-assessments' används här utan översättning eftersom den är allmänt spridd även i Sverige.

utgöra lämpliga utförare av övervakningsaktiviteter (COSO, 2010). Dessa befattningshavare behöver tillräcklig kompetens för att förstå de risker som påverkar organisationens förmåga att uppfylla satta mål, och kunna hantera dessa risker. I vägledningen föreslås att ansvaret fördelas till Chief financial officer och controllers för att övervaka den finansiella rapporteringen, Chief information officer för att övervaka informationssystemen och Chief risk officer eller Chief legal officer för att övervaka efterlevnaden av lagar och förordningar. I nästa steg ser dessa chefer till att de kontroller som behöver övervakning får utvärderare som har den kompetens och objektivitet som behövs, eller ser till att de utvalda utvärderarna får rätt utbildning för uppgiften. Utvärderare måste ha en hög objektivitet om de ska övervaka processer som är känsliga för ersättningar eller är stöldbegärliga eller på annat sätt löper risk för bedrägligt beteende. Även styrelsen behöver utföra bedömningar av vilka som är lämpliga att övervaka kontroller. På vissa områden kan styrelsen finna att internrevisorer behövs för övervakningen eller skötas av styrelseledamöter med lämplig kompetens. (COSO, 2010).

2.4 Arbetsuppgifter i COSOs internkontrollsystem

För att kunna bedöma vilka roller som potentiellt sett skulle kunna utföra kontrollaktiviteter och övervakningsaktiviteter enligt COSO med avseende på kompetens och objektivitet har en analys genomförts av avsnitt 2.1 till 2.3 i ovanstående text. Resultatet av analysen sammanfattas i tabell 1 med avseende på vilka uppgifter inom kontrollaktiviteter och övervakning som förekommer i internkontrollsystemet, och med tillägg av vilka krav, uttryckta i kompetens och objektivitet som utförare behöver besitta, och med en jämförelse av dessa krav på basis av den sammanställning som givits ovan.

Av ovanstående genomgång framgår att kompetenskravet innefattar att den som utför en utvärdering ska ha rätt kompetens för att arbeta med att förebygga, upptäcka och åtgärda fel och brister, och därmed förstå en kontrolls funktion, kunna identifiera avvikelser i kontrollen, genomföra analys av orsakerna till dessa, och dra rimliga och relevanta slutsatser av sin analys för att få kontrollen att fungera på avsett sätt. För att kunna utföra den här utvärderingen behöver utvärderaren ha kunskap både om vilken specifik uppgift en kontroll syftar till, och också om vilka risker kontrollen ska hantera.

Av genomgången framgår också att objektivitetskravet innefattar att en utförare inte är involverad i vare sig det operativa arbetet med eller den del av interna kontrollen som är

föremål för övervakningsaktiviteten. Objektivitetskravet innefattar att utföraren står fri från personliga konsekvenser på till exempel ersättningar och kompensationsplan och som annars kan innebära manipulering av testresultat och övervakningsaktiviteter vid rapportering till överordnade. Utföraren ska också vara separerad från bedrägligt beteende såsom stöd eller annat.

COSOs ramverk	**Aktivitet-ernas syfte**	**Uppgifter i systemet**	**Krav på utförare**	**Potentiell utförare, kompetens**	**Potentiell utförare, objektivitet**
Välja ut och utveckla kontroll-aktiviteter	Begränsa risker för att kunna uppnå mål	- Sköta matriser och hålla workshops för riskkartläggning - Sköta om och utveckla kontrollaktiviteter - Bedöma kontrollaktiviteter för separering av ansvarsområden	Kompetens	Controller Internrevisor i form av rådgivning	E/T Orsakar oberoendehot vid senare granskning
Välja ut och utveckla kontroll-aktiviteter över teknologi	Stödja mål-uppfyllelsen	- Sköta matriser för risk och kontroll över teknik - Dokumentera teknikberoende - Utvärdera slutanvändarberäkningar - Konfigurera infrastrukturen för IT för begränsad åtkomst och åtskillnad av arbetsuppgifter - Konfigurera, processa, administrera och tillämpa mjukvaror och -åtkomst inom IT-systemet	Kompetens	Controller med IT-inriktning IT-specialist Internrevisor/ IT i form av rådgivning	E/T E/T Orsakar oberoendehot vid senare granskning
Utföra kontroll-aktiviteter utifrån fastställda riktlinjer och rutiner	Upprätthålla måluppfyllelsen	- Utveckla och dokumentera rutiner och riktlinjer - Sprida kontrollaktiviteterna genom affärsenheter - Utföra regelbundna eller tillfälliga analyser av kontrollaktiviteter	Kompetens	Controller Internrevisor/ IT i form av rådgivning	E/T Orsakar oberoendehot vid senare granskning
Utföra övervakning-aktiviteter genom löpande eller särskilda utvärderingar	Verifiera effektiviteten i kontrollerna	Granska sammansättningen av övervakningsaktiviteter Indirekt utvärdering genom analys av nyckeltal, intern statistik eller riskindikatorer, och extern	Kompetens Objektiv-itet Auktoritet Resurser	Controller Annan operativ personal Extern specialist	Svag Svag Medel (saknar etisk kod)

		information såsom marknads/branschdata Dashboard för visuella data Genomföra utvärderingar eller granskningar, av egen eller inhyrd personal Direkt utvärdering genom inspektion, observation, förfrågan, bekräftelse, omgörning, återupprepa en kontroll, eller genom analytiska procedurer Utvärderingar kan, med stigande objektivitet, utföras som self-review, peer review, supervisory review, self-assessments eller opartisk granskning		Internrevisor	Stark
Utföra övervakningsaktiviteter för att utvärdera och kommunicera brister till ledning och styrelse	Vidmakthålla systemets relevans och effektivitet genom att mobilisera ansvarighet från de högsta befattningshavarna.	Bedöma och rapportera brister. Övervaka hur korrigeringar och rättelser görs. Utforma vägledningar för hur brister ska rapporteras.	Kompetens Objektivitet Auktoritet Resurser	Controller Annan operativ personal med rätt kompetens Extern specialist Internrevisor	Svag Svag Medel Stark

Tabell 1: Resultat av analys av de uppgifter som enligt COSO behöver utföras inom kontrollaktiviteter och övervakning för att styrelsen ska erhålla säkerhet, samt krav på utförare och vilka roller som då potentiellt sett kan utföra dessa (tabellen utgör författarens konstruktion baserat på den genomförda analysen). (E/T: ej tillämpligt)

Ett resultat av analysen är att när det gäller övervakningsaktiviteter kan en controller ha rätt kompetens för uppgiften att övervaka kontrollerna, det vill säga kunskap om systemet för intern kontroll och dess funktion. En controllers kompetens innefattar också förmåga att känna igen och identifiera avvikelser och brister. Controllern behöver också resurser till sitt förfogande, vilka behöver ges av överordnade, samt auktoritet att genomföra aktiviteterna och rapportera resultaten. När det gäller objektiviteten däremot saknar controllern i normalfallet den objektivitet som krävs, det vill säga vara opåverkad av personliga konsekvenser av arbetet, och utan intresse av att manipulera systemet eller testresultaten. Det beror på att en controller ingår i verksamheten och står i beroendeförhållande till ledningen genom sin ersättning (lön och eventuell kompensationsplan), sina rapporteringsvägar, och

eventuellt även på grund av naturliga personliga relationer med personer i ledningsgruppen och som uppstår genom det dagliga arbetet i det interna kontrollsystemet.

Analysen visar att uppgifterna inom det interna kontrollsystemet kan utföras av personal i ett flertal olika befattningar. Där ingår styrelsens ledamöter, revisionskommitténs ledamöter, företagsledningar på olika nivåer i organisationens hierarkiska struktur, såsom finansdirektörer och koncernredovisningschefer, koncerncontrollers, affärsområdescontrollers, internrevisorer, och eventuellt inhyrda specialister. Av ovanstående genomgång av COSO-modellens vägledning om arbete med övervakning framgår att andra aktörer än internrevisorer skulle kunna genomföra övervakningsaktiviteter förutsatt att de har rätt kompetens för uppgiften, ges resurser och lämplig auktoritet, och uppfyller objektivitetskravet. COSO innehåller ett spann för att bedöma i vilken mån en annan aktör än en internrevisor skulle kunna vara objektiv. Operativ personal kan ha sådan objektivitet, och COSO (2010) ger en bandbredd i objektivitetssteg i stigande skala från självgranskning, kollegial granskning och överordnandegranskning. Ytterligare en form av övervakning är self-assessments, som kan utföras på olika sätt och med varierande grad av objektivitet beroende på utförande, och opartisk granskning.

Controllern har potentiellt sett rätt kompetens för att övervaka kontroller, men på grund av sin plats i organisationen och närhet till ledningen saknas normalt sett den objektivitet som krävs. Detta väcker intressanta frågor om i vilken mån en styrelse kan få säkerhet från controllerns arbete med övervakningsaktiviteter när internrevision saknas. Å andra sidan är det möjligt att styrelser inte har samma syn på betydelsen av objektivitet som den ges i litteraturen, då studier visar att internrevisorer inte heller alltid har de rapporteringsvägar och andra lösningar som krävs för att garantera deras oberoende (Neu mfl, 2013; Norman mfl, 2010). Internrevisorer å andra sidan har den kompetens som krävs, men så snart de utför uppgifter inom kontrollaktiviteter kan deras objektivitet och oberoende försvagas inför efterföljande revisionsuppdrag inom organisationen. För att den interna kontrollen ska kunna fungera tillfredsställande måste tydliga roller och ansvarsområden fastställas för organisationens olika behov, och detta är ett viktigt uppdrag för trelinjemodellen, vilken behandlas härnäst.

3. IIA's trelinjemodell

I det här avsnittet behandlas vägledningarnas beskrivningar av de tre linjerna och de roller som dessa rymmer. Syftet är att behandla modellens beskrivningar av de olika roller som ingår i de tre linjerna, särskilt mellan linje två och tre eftersom fokus här är att utröna olika uppgifter fördelade på roller för att förstå eventuella glidningar mellan nytillkomna och etablerade roller som utför granskningsarbete. Den vägledning som framtagits av IIA (IIA, 2020a) är något otydlig när det gäller kopplingen mellan trelinjemodellen och den interna kontrollen enligt COSO. Framställningen kompletteras därför med vägledningar om intern kontroll för att klargöra trelinjemodellens koppling till internkontrollsystemet.

3.1 Om trelinjemodellen

Trelinjemodellen är från och med år 2020, efter viss bearbetning (se Eulerich, 2021), benämningen på den modell som tidigare kallades de tre försvarslinjernas modell (IIA 2020a; IIA Sweden, 2020; IIA 2020b; IIA, 2013). De tre försvarslinjernas modell var vida spridd inom stora företag redan under 1990-talet (Leech och Hanlon, 2016), och nämns av brittiska the Financial Services Authority år 2003 (Valkenburg och Bongiovanni, 2024), i punkt B39, där det framgår att ett antal av de företag som ingick i deras undersökning då tillämpade ett tillvägagångssätt med tre försvarslinjer där affärslinjeledningarna utgjorde första försvarslinjen, riskfunktionerna den andra och internrevisionen den tredje (Financial Services Authority, 2003).

Trelinjemodellen presenteras som en enkel och effektiv modell som klargör de roller och funktioner som behövs för att stärka organisationers styrning och riskhantering (IIA 2020b). Primärt syftade förändringen av modellen från försvarslinjer till enbart linjer till att anpassa modellen till de uppdaterade standarderna för internrevision, IPPF (International Professional Practices Framework). Ändringen innebar också att internrevisionsfunktionen och dess chef kan utföra arbete utanför sin linje genom rådgivning och konsultarbete på ett tydligare sätt, vilket inte fungerade om rollen enbart betraktas som ett 'försvar' (IIA, 2020a). IIA har givit följande beskrivning av trelinjemodellen (IIA, 2020b, sid. 2, författarens översättning).

> Trelinjemodellen hjälper organisationer att identifiera strukturer och processer som bäst bistår måluppfyllelsen samt främjar styrning och riskhantering.

IIAs trelinjemodell är inriktad på att beskriva de roller som är verksamma inom det interna kontrollsystemet för att undvika ineffektivitet och dubbelarbete, och två betydelsefulla uppdrag för olika roller är dels revision, dels rådgivning. Säkerhet (eng. assurance) är det övergripande behov styrelsen behöver tillgodose, vilket framgår av följande citat (IIA Sweden, 2020, sid 9-10, parentesen om att ’försäkran’ är synonymt med ’intygar’ ingår i källans text).

> 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 (intygar) 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.

Den här beskrivningen ger en god bild av styrelsens behov och grunderna för den säkerhet dess ledamöter skaffar sig. Citatet visar att försäkran och intygande används synonymt. Detta tyder på en syn på försäkran såsom något som passivt kan förmedlas via system, en sorts tyst kunskap om förhållanden, när den traditionella synen inom revisionsteori är att försäkran utförs av en granskare i en trepartsrelation genom en granskningsprocess av ett särskilt utformat informationsunderlag som avgivits av en agent och där granskaren har till uppgift att avrapportera slutsatserna av sin granskning till en uppdragsgivare, principalen (se särskilt Power, 1997, och Pentland, 1993). Frågan är vad *försäkran* (assurance) betyder inom IIA? I den svenska översättningen av modellen finns följande definition (IIA Sweden, 2020, sid. 2).

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

Här framgår att försäkran sker utan att rapportering först utförts, och något resultat i form av en rapport till granskningsutförarens uppdragsgivare ges nödvändigtvis inte heller. Det framgår att arbetet med försäkran ofta sker fragmenterat och av olika parter, till exempel i IIAs beskrivning av hur COSO möter trelinjemodellen, och det är därför viktigt att samordna arbetet (COSO, 2015, sid 11, där fotnoten refererar till IPPF, 2013, författarens översättning).

> Noggrann samordning är nödvändig för att undvika onödigt dubbelarbete och samtidigt säkerställa att alla betydande risker hanteras på lämpligt sätt. Denna samordning är så viktig att enligt Standard 2050 har internrevisionschefer en skyldighet att "dela information och samordna aktiviteter med andra interna och externa leverantörer av revisions- och konsulttjänster för att säkerställa korrekt täckning och minimera dubbelarbete."[5]

Enligt denna beskrivning kan flera olika roller utföra försäkran. Gränsen mellan försäkran och rådgivning eller konsulting framställs emellertid tydligt, till exempel avseende tredje linjens arbete inom COSOs första princip om att organisationen ska demonstrera sitt engagemang för integritet och etiska värderingar. Där kan internrevisorerna ”ge bestyrkande (eng. assurance) om utvecklingen och prestationerna i interna kontroller, utvärdera om kontrollerna utformats ändamålsenligt, genomförts effektivt och fungerar på avsett sätt”, och “ge rådgivningstjänster (eng. consulting services) för att hjälpa organisationen etablera ett robust etikprogram och förbättra dess effektivitet för att uppnå den uppsatta prestationsnivån” (COSO, 2015, sid. 15).

Även om modellen benämns de tre linjernas modell, framförs i IIAs vägledningar att begreppet ’linjer’ tonats ner och betoningen på ’roller’ lyfts fram (IIA, 2020a). Begreppet ’linjer’ har behållits för att modellen ändå ska kunna kännas igen, men istället för att styra tankarna mot struktur ska ’linjer’ innebära en åtskillnad mellan roller inom de tre linjerna (IIA, 2020a, fotnot 3). När de tre försvarslinjernas modell används i samband med riskhantering fungerar beteckningen ansvarslinjer bättre än försvarslinjer eftersom företagande, som ju innebär ansvar under risk, utgör grunden för värdeskapande (Arwinge, 2016). Enligt modellen har styrelsen ansvaret för alla tre linjerna, medan linje ett och två omfattar företagsledningens ansvar och den tredje linjen omfattar internrevisionens oberoende granskning (IIA, 2024). Styrelsen ses primärt som modellens förvaltare och utgör därför inte någon ytterligare linje till de tre som ingår i modellen (IIA, 2013; IIA 2020b). Detta har ifrågasatts (Leech och Hanlon, 2016), vilket vi återkommer till i avsnitt 3.3.

3.1.1 Modellens tre delar- linjerna

IIA (2013) har beskrivit de tre linjerna på så sätt att den första linjen består av riskägarskapet, där risk ägs och styrs, den andra linjen består av översyn över risk där risk kontrolleras och efterlevs, och den tredje där säkerhet ges över de andra två linjernas riskarbete (se Leech och Hanlon, 2016). Den första linjen utgörs av företagsledningens styrning (eng. control) över riskhanteringen och den andra linjen utgörs av riskkontroll och efterlevnad. Varje linje ska ha tydligt definierade roller och ansvarsområden, med tillhörande rutiner, riktlinjer och rapporteringsformer. Då modellen är principbaserad anses den anpassningsbar till olika organisationers mål och förutsättningar (IIA, 2020a). Internrevisionsfunktionen är enligt modellen inte den enda formen av övervakning, då det finns flera olika sådana (COSO,

2015). I vissa dokument framförs en fjärde linje; den externa revisionen, och därefter kommer regulatorisk tillsyn (COSO, 2015; Eklöv Alander, 2019).

Roller i den första linjen sköter produktion och leverans eller tjänsteutförande till organisationens kunder och innefattar roller som både möter kund (eng. front of house) och i bakgrunden (eng. back office) stöttar dessa med administration, IT, HR-funktioner och fastighetstjänster (IIA, 2020a). I första linjen sker riskhantering (eng. managing risk). All riskhantering är företagsledningens ansvar (IIA, 2020a). Den här linjen äger riskhanteringen, och också utformning av och genomförandet av kontroller för att hantera dessa risker (COSO, 2015).

Den andra linjens funktioner är åtskilda från första linjen men utför vissa ledningsfunktioner och lyder under företagsledningen som ger dem uppdrag och leder deras arbete (COSO, 2015). De arbetar inom riskorganisationen och controllerfunktionen och rapporterar till företagsledningen. I andra linjen finns specialister, som stöttar första linjen med kunskap, stöd, uppföljning och övervakning och utmanar även den första linjens roller på olika sätt. I andra linjen sker arbete med riskhantering kring uppfyllande av relevant lagstiftning och regleringar som är tillämpliga för organisationen, etiska frågor, hållbarhet, intern styrning och kontroll, kvalitetssäkring, teknisk säkerhet och IT-säkerhet (IIA Sweden, 2020). Den andra linjen innehåller funktioner som syftar till att säkerställa att systemen för riskhantering och intern styrning och kontroll fungerar; de kontrollerar och övervakar systemen och processerna i den första linjen. Andra linjens roller gör också analyser av riskhanteringen och förser ledningen med rapporter om riskhanteringen är tillräcklig och effektiv (IIA Sweden, 2020). För att denna andra linje ska vara till nytta fokuserar den inte enbart på kontroll utan också på stöd och vägledning till den första linjen; den hjälper till att utveckla första linjens system och processer. Personer verksamma inom den andra linjen har typiskt sett inget verksamhetsansvar. Enligt COSO (2015) äger denna linje ett flertal funktioner inom riskhanteringen för företagsledningens del. Andra linjen är inte ansvarig för att fastställa eller godkänna mål på organisationsnivån men kan däremot stötta företagsledningen med utkast, införande, övervakning och rapportering av mål som hör till deras kompetensområden inom till exempel regelefterlevnad och kvalitetskontroll. Ett annat exempel är företagsledningens ansvar för internkontrollsystemet och för att identifiera och bedöma förändringar som potentiellt skulle kunna ha en väsentlig påverkan på internkontrollsystemet (COSO, 2015). Där kan andra linjen bistå med att bedöma förändringars påverkan på det interna kontrollsystemet. Enligt IIA (IIA, 2020a) kan seniora befattningshavare rapportera direkt till

styrelsen för att på så sätt stärka sitt oberoende från företagsledningen, även om de då ändå befinner sig inom företagsledningens domän.

Internrevisorerna rapporterar till styrelsen, primärt dess revisionsutskott. På så sätt vidmakthåller de sitt oberoende gentemot företagsledningen, och styrelsen och dess revisionsutskott får tillgång till information som ska vara opåverkad av företagsledningen. Enligt trelinjemodellens femte princip förmedlas den tredje linjens oberoende på följande sätt (IIA, 2020b, sid. 5, författarens översättning).

> Internrevisionens oberoende från ledningens ansvarsområden är avgörande för dess objektivitet, auktoritet och trovärdighet. Det säkerställs genom ansvar gentemot den styrande instansen; obegränsad tillgång till de personer, resurser och information som behövs för att utföra arbetet; samt frihet från partiskhet eller inblandning i planering och genomförande av revisionsuppdrag.

Internrevisorernas arbete går ut på att granska både första och andra linjens funktioner och de ska därför inte ha något ansvar för hur dessa fungerar eller för att utveckla dem, dvs de ska inte ha något som helst ledningsansvar (COSO, 2015). IIA påpekar att jämfört med första och andra linjens roller är internrevisionens roll helt annorlunda, den är fri från kopplingen till företagsledningen (IIA, 2020a, sid 8, författarens översättning).

> Den är inte enbart ytterligare en konsultfunktion inom andra linjen. Den är oberoende från ledningens ansvarsområden, beslut och inblandning och svarar direkt inför styrelsen.

Den organisation som vill kombinera den andra och tredje linjen bör enligt IIA låta styrelsen (eng. the governing body) avgöra detta, men IIA påpekar också att rollerna i andra och tredje linjen inte är förenliga: ”En person kan inte både vara ansvarig för något och också ge oberoende bestyrkande av det” (IIA, 2020a, sid. 8, författarens översättning). För att bevara internrevisionens oberoende ska internrevisorer avstå från att utveckla kontrollaktiviteter, men kan däremot ge rekommendationer om kontroller när så efterfrågas (COSO, 2015). IIA (2020a) öppnar upp för att internrevisionen ska kunna ta uppgifter som hör till den andra linjen men att någon annan roll då ska ge en oberoende granskning i deras ställe.

3.2 Kopplingen mellan COSO och trelinjemodellen för roller och ansvar

För att ytterligare belysa hur trelinjemodellen framställer vilka funktioner rollerna har inom den interna kontrollen sker här en koppling till COSO (2015), särskilt avseende den andra och den tredje linjen. Det operativa ledningsansvaret i första linjen är kopplat till COSO genom kontrollaktiviteter på så sätt att denna linje ansvarar för att välja ut, utveckla och

underhålla kontrollaktiviteter och övervakningsaktiviteter inbyggda i organisationens processer och dagliga aktiviteter hos personalen för hela organisationens verksamhet (COSO, 2015). Kontrollaktiviteterna, liksom generella IT-kontroller, väljs ut och utvecklas, och rutiner och riktlinjer för tillämpning av dessa kontrollaktiviteter utformas. I företagsledningens ansvar i första linjen ingår att leda personal som med rätt kompetens, behörighet och resurser utför kontrollaktiviteter, vilket ska vara fastställt i riktlinjer och rutiner och ske i rätt tid. I första linjens ansvar ingår också att löpande granska kontrollaktiviteterna för att bedöma om de är relevanta och vid behov uppdatera dem (COSO, 2015).

Övervakningsaktiviteterna som utförs inom den första linjen innefattar löpande och särskilda utvärderingar, och också utvärdering av avvikelser och brister och kommunikationen om dessa. De som utför dessa aktiviteter är chefer i frontlinjen och mellanlinjechefer som löpande leder risk och kontrollfrågor. De utvecklar olika kontroller och riskhantering, ser till att de införs och löpande underhålls. De interna kontrollprocesserna ska vara utformade för att identifiera och bedöma materiella risker, se till att kontrollaktiviteterna utförs, att identifierade avvikelser eller brister hanteras, och se till att informationsflödet fungerar inom enheten till dem som ska innefattas av kontrollaktiviteterna. Företagsledningen kan också ha tillsyn över dessa ledningsfunktioner, eller utför eventuellt själv vissa av dessa ansvarsområden inom första linjen. Riskägare och chefer inom första linjen håller uppsikt över hur brister avhjälps och hjälps åt inom företagsledningen med att rapportera till styrelsen om hur den interna kontrollen fungerar. (COSO, 2015)

De ansvarsområden som ingår i andra linjen utgörs till exempel av risk management, informationssäkerhet, finansiell kontroll, kvalitetskontroll, efterlevnad av regler, juridiska frågor, miljö, och leveranskedjan (COSO, 2015). Andra linjens roller och ansvar ska enligt COSO (2015) omfatta övervakning av kontroller och riskhanteringen och sköts av riskhanterings- och efterlevnadsfunktioner som är kopplade till företagsledningen. Även om dessa roller ska vara separerade från företagsledningen finns de under dess ledning och kontroll, och företagsledningen är fortsatt ansvarig för hela systemet för intern kontroll och riskhantering (COSO, 2015). Andra linjen har till uppgift att bistå med strategiarbete och införande av intern kontroll, kompetens kring risker, samt för informationsinsamling för hela organisationens risk- och kontrollarbete. Vilka befattningshavare som arbetar i andra linjen kan variera stort, de kan till exempel utgöras av första linjens chefer som utför de uppgifter som hör till övervakningen i andra linjen (COSO, 2015). De övervakningsaktiviteter som

täcks av den andra linjen omfattar alla de tre målområdena för COSO-ramverket; verksamheten, rapporteringen och efterlevnaden av regler. I COSO (2015) beskrivs att de funktioner som ryms inom den andra linjen har ett visst men begränsat oberoende från första linjen men att de ändå utgör delar av företagets ledning. Här finns processer för utveckling, införande och förändringar av interna kontroller och riskhantering, och här kan också tas beslut kring dessa delar. Andra linjens roller är därför inte oberoende från första linjens aktiviteter på det sätt som internrevisionsfunktionen avser att vara (COSO, 2015).

Den andra linjens uppgifter när det gäller att välja ut och utveckla kontrollaktiviteter handlar om att övervaka att särskilda kontroller fungerar på avsett sätt, och att medverka vid urval av särskilda kontroller för att bidra till deras utveckling. Arbetet går ut på att hantera och begränsa risker för att mål ska kunna uppfyllas. När det gäller att välja ut och utveckla kontrollaktiviteter över teknologi utgörs andra linjens uppgifter av att övervaka att särskilda kontroller över teknologi fungerar ändamålsenligt. Här kan arbetsfördelning göras så att grupper med särskilda kompetenser, till exempel om IT-säkerhet, på ledningens uppdrag kan sköta utveckling och underhåll av sådan teknologi. Det är också andra linjens uppgift att övervaka att de riktlinjer och rutiner för kontrollaktiviteter som ledningens fastställt tillämpas på avsett sätt. (COSO, 2015)

De ansvarsområden för andra linjen som har med övervakning att göra omfattar att utforma aktiviteter för att övervaka och mäta måluppfyllelse utifrån företagsledningens satta mål, övervaka lämpligheten i och effektiviteten i internkontroller, och att identifiera och övervaka sådana förhållanden som kan påverka organisationens risker och interna kontroller. De övervakningsaktiviteter som utförs av andra linjen sker genom löpande eller särskilda utvärderingar, för att ta reda på statusen hos internkontrollsystemets komponenter, och om uppnådda mål ryms inom fastställda risktoleranser (COSO, 2015). Andra linjen kan också utföra övervakning av kontrollbrister och rapportera de iakttagelser som då görs till företagsledningen och till styrelsen (COSO, 2015).

Den tredje linjens koppling till COSO beskrivs som en funktion som ger bestyrkande om effektiviteten i styrning (eng. governance), riskhantering och intern kontroll, och kan omfatta olika aspekter av organisationens verksamhet. Det är dess objektivitet och oberoende som särskiljer internrevisionen från de andra två linjerna och gör dem bäst lämpade att ge säkerhet till styrelsen. Oberoendet härrör från att internrevisionen inom sina normala uppgifter varken utformar eller implementerar interna kontroller, inte har något ansvar för organisationens verksamhet, samt rapporterar direkt till styrelsen (COSO, 2015). Det är till exempel viktigt att

internrevisorerna inte väljer ut eller utvecklar kontrollaktiviteterna över teknologi eller andra områden men däremot kan de ge rekommendationer däröver (COSO, 2015). För den princip som handlar om att organisationen tar fram kontrollaktiviteter arbetar tredje linjen med att granska att kontrollerna utformats på ett korrekt sätt, att de implementerats effektivt och att de fungerar ändamålsenligt. Tredje linjen kan också få i uppgift att bedöma om styrningen av IT är till stöd för organisationens mål och strategier, granska om kontroller över teknologi är effektiva och fullständiga, och ge rekommendationer om hur kontrollaktiviteter relaterade till teknologi kan förbättras. Inom den tredje linjen ryms att ge säkerhet om riktlinjernas och rutinernas utformning och implementering. Avseende COSOs principer för övervakning är tredje linjens uppgifter av naturliga skäl mer omfattande. Den tredje linjen kan ge säkerhet om de utvärderingar som sker i första och andra linjerna ingår i affärsprocesserna, och om de justeras när förhållandena ändras. Tredje linjen kan ge säkerhet om huruvida företagsledningens rapportering om utförda utvärderingar presenteras korrekt. Den tredje linjen kan också ge säkerhet om huruvida internkontrollsystemets funktion överensstämmer med förväntningarna och om risker hanteras inom fastställd riskaptit och risktolerans. För att tredje linjens utförda granskningar ska komma till nytta på bästa sätt kan tredje linjen också utforma och underhålla ett system för att övervaka hanteringen av dess rapportering till företagsledningen, främst tredje linjens iakttagelser och rekommendationer. Där kan ingå en tidsram för svarstider från företagsledningen, utvärdering av svaren som ges och eventuellt verifiera dessa och planera och genomföra uppföljningar, och rapportera till företagsledningen eller styrelsen om åtgärder inte genomförs eller utförs på ett bristfälligt sätt. (COSO, 2015)

3.3 Arbetsuppgifter i trelinjemodellens andra och tredje linjer

I tabell 2 ges en sammanfattning av de aktiviteter som, med avseende på den finansiella rapporteringen, utförs av andra linjen och tredje linjen avseende uppföljning, övervakning och granskning. Tabellen är sammansatt genom en sammanställning av ovanstående text. Av de 17 COSO-principerna är liksom tidigare i rapporten de tre principerna för kontrollaktiviteter och de två principerna för övervakningsaktiviteter de mest relevanta för framställningen eftersom de lyfter fram fokuset på arbete med kontrollaktiviteter och övervakning som utförs av roller inom dels den andra, dels den tredje linjen.

COSO-princip	Andra linjens uppgifter	Tredje linjens uppgifter
Välja ut och utveckla kontrollaktiviteter	Övervaka särskilda kontroller. Medverka i urval och utveckling av särskilda kontroller.	Granska att kontrollerna utformats adekvat, implementerats effektivt, och fungerar ändamålsenligt. Ge rekommendationer baserat på sin granskning om hur de interna kontrollerna kan förbättras.
Välja ut och utveckla kontrollaktiviteter över teknologi	Övervaka särskilda kontroller över teknologi. IT-specialister kan medverka vid urval, utveckling, och underhåll av teknologi.	Bedöma om organisationens styrning av IT stödjer organisationens mål och strategier. Bestyrka effektiviteten och fullständigheten hos kontroller över teknologi. Rekommendera, där så är lämpligt, förbättringar av särskilda kontrollaktiviteter.
Utföra kontrollaktiviteter utifrån fastställda riktlinjer och rutiner	Övervaka hur riktlinjer och rutiner praktiseras. Hjälpa företagsledningen att underhålla riktlinjer och rutiner och se till att sprida information om dem.	Ge säkerhet om design och implementering av riktlinjer, rutiner och kontroller i övrigt, och ge rekommendationer baserat på sin granskning.
Genomföra övervaknings-aktiviteter genom löpande eller särskilda utvärderingar	Övervaka funktionen hos komponenter i intern-kontrollsystemet genom att löpande eller efter särskilt behov utvärdera dessa, och övervaka om uppnådda mål ryms inom fastställda risktoleranser.	Granska och ge säkerhet om följande: - Om företagsledningens utvärderingar ingår i affärsprocesserna och justeras vid förändrade omständigheter. - Om information om företagsledningens utvärderingar är riktig och korrekt presenterad. - Om internkontrollsystemet fungerar enligt förväntan. - Om risker hanteras inom organisationens fastställda nivåer.
Utföra övervaknings-aktiviteter för att utvärdera och kommunicera brister till ledning och styrelse	Övervaka och rapportera särskilda kontrollbrister.	Utforma och underhålla ett system för att övervaka planläggningen av internrevisionens iakttagelser och rekommendationer som rapporteras till företagsledningen. Här ingår tidsramar för företagsledningens svar, utvärdering av svaren, uppföljningsuppdrag, och kommunikation till företagsledningen eller styrelsen då svar eller åtgärder är otillfredsställande.

Tabell 2: Sammanställning av aktiviteter som utförs av andra linjen och tredje linjen avseende uppföljning, övervakning och granskning, primärt avseende den finansiella rapporteringen (författarens konstruktion baserad på sammanställning av kapitlet).

Sammanställningen av ovanstående avsnitt visar att rollerna inom de tre linjerna i vägledningarnas domän faller prydligt sida vid sida utan större överlappningar men att enligt trelinjemodellens framställning internrevisorerna uppenbart kan röra sig relativt fritt mellan andra och tredje linjen. Viktigt att notera är också att den andra linjens övervakning tycks ske på företagsledningens direktiv och uppdrag, till skillnad från den tredje linjen som utför

övervakningsaktiviteter baserat på granskningsrutiner vilket inbegriper fristående riskanalys och planering för val av granskningsobjekt.

3.4 Forskning om trelinjemodellen

På sin tid efterfrågade Jensen (1993) intern kontroll eftersom han menade att de rättsliga, politiska och regulatoriska systemen var alltför tröga för att kunna hantera problemet med företagsledningarnas slösaktighet på ett verkningsfullt sätt. Han ansåg att den tidens rådande internkontrollsystem inte fungerade tillfredsställande och uppmanade till att finna vägar att förbättra dem. Efter de båda kriser som briserade under 2002 och 2007 har allt större fokusering skett till system för intern kontroll och riskhantering, och då är det primärt den första linjen som avses och företagsledningens arbete med att utforma och upprätthålla system för intern kontroll och riskhantering inom organisationer (Van Staveren, 2021). Enligt Bantleon mfl. (2021) har trelinjemodellen refererats i olika texter som en effektiv modell för riskhantering och utgör best practice för stora börsnoterade företag. Även dess föregångare med de tre försvarslinjerna är ännu en spirande genre inom forskningen med endast ett fåtal genomförda studier publicerade i vetenskapliga tidskrifter (Bantleon mfl., 2021), och därför presenteras i det här avsnittet de mest relevanta artiklarna enligt den litteratursökning som företagits för den här rapporten.

3.4.1 Modellens fördelar

Eulerich (2021) anser att modellens stora spridning beror på att den är flexibel och ger en struktur för bolagsstyrning, och ett ramverk för organiseringen av individuella (alltså i meningen uppdelade) bolagsstyrningsfunktioner, genom att linjerna delar upp uppgifterna inom det interna kontrollsystemet på ett sätt som ger tydliga definitioner av funktioner och ansvarsområden. Även Bantleon mfl. (2021) ser de tre försvarslinjerna som ett ramverk, och kopplar samman detta ramverk med agentteorin då de menar att ramverket bidrar till att minska den informationsasymmetri som kan förekomma mellan principaler och agenter i de olika hierarkiska nivåerna och minimera risken att agenterna tar beslut som är oförenliga med

principalernas intressen.[4] Bantleon mfl (2021) påpekar att företagsledningen och styrelsen är de främsta intressenterna till trelinjemodellen och de är ju också av bolagsstyrningens olika aktörer bäst skickade att se till att säkerställa att organisationens riskhantering och kontrollprocesser omfattas av trelinjemodellen. Trelinjemodellen är uppdelad i de olika rollerna på så sätt att chefer och professionella aktörer i den första linjen *utför* (eng. execute) riskhantering genom supportfunktioner som finns back office, primärt arbetar business controllers i den andra linjen med *stöd* (eng. support) till första linjen och i den tredje linjen finns internrevisionsfunktionen som på ett oberoende sätt *säkerställer* (eng. ensure) kvaliteten i de aktiviteter som utförts av första och andra linjen och lämnar råd om hur dessa kan förbättras (Bantleon mfl, 2021; Tawfik mfl., 2023; van Staveren, 2021). Van Staveren (2021) påpekar också att mycket av den policy som finns inom riskhanteringsområdet tar fasta på att det är företagsledningen, det vill säga den första linjen, som har ansvar för att riskägarskapet tillämpas fullt ut inom organisationer, och därmed också för att integrera riskhanteringen inom organisationens alla aktiviteter och processer. Studier har främst fokuserat på första och andra linjens samarbete, där en viss oklarhet finns om i vilken linje av den första och den andra som egentligen har riskägarskapet (Van Staveren, 2021; Eulerich 2021; Davies and Zhivitskaya, 2018; Mabwe mfl., 2017).

Den första linjen handlar om företagsledningens ansvar för den operativa verksamheten, interna kontroller och risker att uppnå målen (Bantleon *et al.*, 2021; Van Staveren, 2021). Detta inkluderar vanligtvis IT-personal, systemadministratörer och operativ cybersäkerhetspersonal, såsom Security Operations Centre, som hanterar och övervakar organisationens digitala infrastruktur för att säkerställa att den är skyddad och motståndskraftig mot cyberhot (Valkenburg och Bongiovani, 2024). En förutsättning för att de andra och tredje linjerna ska kunna uppfylla sina funktioner är att den första linjen fungerar tillfredsställande (Power, 2009; Van Staveren, 2021).

[4] En utförlig beskrivning av agentteorin ges av Jensen och Meckling (1976), Fama (1980) och Fama och Jensen (1983), samt Eisenhardt (1989) som diskuterat dess betydelse inom forskningen om organisationer. För den här framställningen betonas i korthet att principaler utgörs av dem som givit agenter i uppdrag att förvalta egendom eller driva verksamheter och som då behöver ett tillförlitligt informationsunderlag, vilket tillhandahålls av agenterna. Inom en stor organisation med nationell eller multinationell täckning kan alltså principaler och agenter förekomma på olika hierarkiska nivåer. Traditionellt sett har revisorer till uppgift att granska informationsunderlaget och yttra sig över detta inför principalerna. För betydelsen av agentteorin inom revisionsforskning - se även Eklöv Alander (2019).

I den andra linjen finns de företagsövergripande funktionerna för risk, regelefterlevnad och finans (Leech och Hanlon, 2016). Den består av specialister, såsom controllers och riskansvariga, som ger kunskap och expertis för att stödja verksamheten (Van Staveren, 2021) såsom en form av efterlevnadsövervakning för företagsledningen (Bantleon *et al.*, 2021). Den andra linjen tillhandahåller också analyser och rapporter över intern kontroll och riskhantering, för att ständigt förbättra, utveckla och implementera delar av det interna kontrollsystemet och ge säkerhet om olika aspekter såsom kontrollsystemet, strategisk kontroll, antikorruption, kvalitetsledning och cybersäkerhet (Cantù, Langella och Vannini, 2024). Det handlar om team eller avdelningar som fastställer cybersäkerhetspolicys, övervakar regelöverensstämmelse och säkerställer att organisationen följer bästa praxis (Valkenburg och Bongiovani, 2024).

Den tredje linjen, som består av internrevisionsfunktionen, har till uppgift att oberoende bestyrka kvaliteten i de aktiviteter som sker i de första två linjerna (Bantleon *et al.*, 2021; Roussy and Rodrigue, 2018; Van Staveren, 2021). Där ingår också att granska att de första och andra linjerna effektivt arbetar med och förhindrar cyberrisker (Valkenburg och Bongiovani, 2024). Enligt Tawfik mfl. (2023) kan trelinjemodellen åstadkomma effektiva resultat för bolagsstyrningen om de tre linjerna är organiserade på ett effektivt sätt. Tawfik mfl. (2023) framför att eftersom den tredje linjen, bestående av internrevisionsfunktionen, utvärderar effektiviteten hos riskhanterings- och styrningsfunktionerna så har den tredje linjen potential att stärka organisationens styrning.

3.4.2 Kritik mot modellen

Även om trelinjemodellen anses vara ett effektivt sätt att skapa ordning och struktur i den interna kontrollen och förbättra riskhanteringen har den fått kritik. Trots att modellen har använts inom riskhantering i stora organisationer, inklusive inom den finansiella sektorn sedan 1990-talet, har den inte lyckats förhindra stora bedrägerier och misslyckanden (Leech och Hanlon, 2016). I trelinjemodellen har styrelsen inte beskrivits som en linje (Leech och Hanlon, 2016; Eulerich, 2021), vilket kommenteras på följande sätt av IIA (IIA, 2020b, sid. 5 fotnot 1, författarens översättning).

> Logiskt sett utgör styrande organs roller också en ”linje”, men denna konvention har inte anammats för att undvika förvirring.

Leech och Hanlon (2016) framför att sett från det stora antal stämningar som aktieägare har riktat mot styrelser, särskilt i USA, betraktar en stor del av aktieägarna styrelsen som den sista försvarslinjen. Enligt trelinjemodellens andra princip (IIA 2020b) har styrelsen till uppgift att tilldela ledningsgruppen befogenheter och resurser, så att de kan uppnå företagets mål och samtidigt se till att lagar, regler och etiska krav efterlevs. Styrelsen är också ansvarig för att inrätta och övervaka IAF och stödja dess oberoende, objektivitet och kompetens så att den kan uppnå sina mål. För att modellen ska fungera menar Eulerich (2021) att styrelseledamöter och revisionskommittéer måste visa integritet, sunda styrningsmetoder och upprätthålla höga krav på transparens. Modellen pekar på internrevisorernas dubbla roll att ge både stöd till ledningen och oberoende försäkran till dem som ansvarar för styrningen. Detta understryker dilemmat med internrevisorns otydliga roll (Brender et al, 2015; Eklöv Alander och Holmgren Caicedo, 2023; Everett och Tremblay, 2014; Fazli Aghghaleh et al., 2014; Gustafsson Nordin, 2023; Lenz och Sarens, 2012; Mihret och Grant, 2017; Mihret, 2014; Roussy, 2013, 2015; Roussy och Brivot, 2016; Roussy och Perron, 2018; Soh och Martinov-Bennie, 2011) och väcker frågor om internrevisionens effektivitet som den föreskrivna tredje försvarslinjen (Roussy och Rodrigue, 2018). Av litteraturen framgår att den tredje linjen beskrivs på ett otydligt sätt avseende vem som kan utföra dess roll och även dess koppling till den interna kontrollen. Den tredje linjen kan bestå av internrevisorer men dess uppgifter kan även utföras av andra oberoende aktörer. Enligt COSOs bestämmelser är internrevisionens roll att stötta företagsledningen vid definition av internkontrollen och dess mål, att fastställa internkontrollen och dess komponenter, bestämma utvärderingsverktygen för att mäta internkontrollens lämplighet och effektivitet, och övervaka den interna kontrollen löpande för att säkerställa att dess mål uppfylls. Rezaee (1995) menade på sin tid att detta är en mer proaktiv roll än den traditionella, som innefattar att identifiera brister i det interna kontrollsystemet och föreslå förbättringar. Parker och Johnson (2017) har observerat att internrevisorers praktik utvecklats för att möta COSOs krav. IIA har sökt vägar att utveckla internrevisorsrollen så att den blir mer strategiskt inriktad och mot att innefatta rådgivning. Power (2007) framför att intern kontroll omformas i termer av riskhantering på grund av att kontrollförmågor måste uttryckas i termer av strategiarbete, vilket sker på en arena där olika roller strider om organisatorisk signifikans.

Av litteraturen framgår en skillnad om huruvida de två första linjerna anses vara separata eller är synkroniserade. Vissa forskare ser en tydlig avgränsning mellan den första och den andra försvarslinjen. Enligt Davies och Zhivitskaya (2018) arbetar de tre linjerna oberoende av

varandra, vilket de anser kan invagga företagsledningen i en falsk upplevelse av kontroll. Tawfik mfl. (2023) framför att första linjen och andra linjen både kan utföras separat eller genom olika kombinationer. Tawfik mfl. (2023) menar att andra linjen stöttar ledningen av den första linjen så att de risker som uppstår i den första linjen dämpas, och kan liknas vid en funktion som är specialiserad på att stötta första linjen. Eulerich (2021) menar å sin sida att den andra försvarslinjen inte enbart stöttar utan till och med leder och styr den första försvarslinjen. Bantleon mfl. (2021) menar att kravet på ett uttalat oberoende (eng. independence) mellan linjerna innebär att det samtidigt finns tydliga utväxlingar (eng. tradeoffs) som skulle kunna påverka riskhanteringsfunktionens effektivitet, och för att behålla de positiva effekterna av de tre linjerna behöver deras uppgifter och resurser samordnas, eftersom dessa uppgifter och resurser inte är oberoende från de andra linjernas.

Leech och Hanlon (2016) framför också att det finns oklarheter i standarderna om rapportering, om vem som ska rapportera och exakt vad och till vem (Leech och Hanlon, 2016, sid. 338, författarens översättning):

> Det är viktigt att notera att författarna till ECIIA-rapporten, liksom författarna till IIA:s diskussionsunderlag som publicerades senare under 2013, inte såg att ledningen i den första försvarslinjen formellt har att rapportera uppåt om riskstatus efter att ha bedömt risk, eller, om de [författarna] gjorde det, så framgår det inte.

En avsaknad av rapportering från företagsledningen till styrelsen över bedömningen av riskhanteringen torde försvåra granskningen av densamma. Leech och Hanlon (2016) föreslår därför att trelinjemodellen utökas till att bli fem linjer, där en linje skulle bestå av den högsta ledningsgruppen med en underliggande linje för affärsenhetschefer, samt att styrelsen också i modellen syns som den högsta linjen i främsta ledet mot organisationens intressenter. Två linjer utgörs så som i nuvarande modell av dels specialistenheter och av internrevisorer. På så sätt skulle ansvarigheten tydliggöras avseende effektiviteten i organisationers riskhantering.

Leech och Hanlons (2016) förslag om att företagsledningen skulle kunna avge en formaliserad rapport till styrelsen över arbetet med den interna kontrollen och riskhanteringen med ett ställningstagande om dess effektivitet och ändamålsenlighet skulle på ett tydligt sätt stärka internrevisionens epistemiska oberoende, då det skulle innebära att internrevisionen har en tydlig bas som de reviderar utifrån.[5] En systematiserad rapportering enligt tydliga

[5] Det epistemiska oberoendet utgör del av det operativa oberoendet som handlar om revisorns förmåga att utföra sin revision. För att den epistemiska formen av operativt oberoende ska vara möjligt krävs dels tydliga riktlinjer för klientens arbete och dels tekniker för att avgöra efterlevnad av dessa riktlinjer, tydligt skilda från klienten (se

riktlinjer skulle utgöra både ett ansvarsfullt sätt för företagsledningen att ge information till styrelsen och, i kombination med IIAs ramverk och standarder, ge en sådan bas för granskning och uttalande över iakttagelser som epistemiskt oberoende vilar på.

Sammanfattningsvis noteras att kritik har riktats mot de tre försvarslinjernas modell då den inte tydligt klargör styrelsens ansvar för organisationens styrning och riskhantering gentemot dess intressenter, och inte heller företagsledningens ansvar för företagets styrning och riskhantering (Leech och Hanlon, 2016). Den omarbetning av trelinjemodellen som IIA utfört (se IIA 2020a) tycks ha bemött en del av kritiken mot de tre försvarslinjernas modell, så att den omarbetade versionen innefattar att styrelsen är ansvarig gentemot organisationens intressenter, samt att företagsledningen är ansvarig för de två första linjerna. Däremot tycks inte Leech och Hanlons (2016) förslag att företagsledningen ska utforma en rapport till styrelsen över företagets interna styrning och riskhantering ha införts, och således inte heller att internrevisionen skulle kunna basera sitt arbete på att granska denna rapport. En sådan ordning skulle ha klargjort både företagsledningens ansvar för organisationens styrning och riskhantering och givit styrelsen ett tydligt underlag med hög grad av säkerhet över detta arbete.

Power, 1997). Dessutom behövs det epistemiska oberoendet i form av självständighet från uppdragsgivaren för att internrevisionen ska kunna vara till nytta för denne (Eklöv Alander, 2023).

4. Slutsatser

Den här rapporten motiveras av en iakttagelse om att controllers tycks ersätta det granskningsarbete som traditionellt sett utförs av internrevisorer i ett flertal av Stockholmsbörsens large cap-bolag, där samtidigt internrevisionsfunktioner saknas (Eklöv Alander och Holmgen Caicedo, 2024). Här undersöks därför vilket utrymme som ges till en utveckling av controllerrollen i riktning mot att utföra arbete som syftar till att ge säkerhet om den interna kontrollen och riskhanteringen över finansiell rapportering, alltså en eventuell rollutvidgning av controllerrollen mot internrevisorernas klassiska domäner. Rapportens syfte motiveras av att forskning om en sådan rollutvidgning ännu, så vitt kunnat utrönas, saknas. Syftet har uppfyllts genom att studera hur COSO och trelinjemodellen hänger samman med avseende på vilka uppgifter som utförs inom intern kontroll och riskhantering, och vilka krav som ställs på dem som utför dessa med avseende på övervakning och granskning. Rapporten ger ett antal slutsatser.

Av den analys av COSO-ramverket som skett ovan kan noteras att COSO-ramverket redan innefattar arbetsuppgifterna för de roller som finns i trelinjemodellen, medan den senare tycks syfta till att klargöra internrevisionens roll inom COSOs övervakningsaktiviteter. På så sätt tydliggör IIA ett utrymme för sin profession inom COSOs ramverk. Detta torde knappast vara förvånande eftersom internrevisorer tycks sträva efter att utveckla sin profession och försvara gränserna mot andra roller.

COSO utgår från de *uppgifter* som ska utföras inom den interna kontrollen men fäster inte vikt vid vilken roll som utför dessa. Samtidigt fastställer COSO krav på de utförare som har till uppgift att arbeta med de olika komponenterna inom den interna kontrollen. IIAs trelinjemodell däremot fastställer vilka *roller* som har att utföra arbetet inom den interna kontrollen, och är tydlig med att internrevisorer har till främsta uppgift att utföra granskningsarbete. Trelinjemodellen öppnar emellertid för att även andra granskningsfunktioner kan delta i att utföra granskningsarbete i den tredje linjen, men avstår från att ge mer detaljerade uppgifter om vilka befattningshavare som då kan utföra sådan granskning.

Därtill konstateras att controllers enligt COSO kan utföra sådana övervakningsaktiviteter som innefattar granskning, det vill säga glida åt höger i trelinjemodellen, så länge de har rätt kompetens, objektivitet och resurser för uppgiften, vilka varierar i vikt beroende på typ av uppgift inom systemet. COSO ger också vägledning om vilken kompetens som behövs, och

vilka krav på och problem som kan föreligga avseende objektiviteten. Internrevisionen å andra sidan glider mot controllerns domäner i sin rådgivande-, och i vissa avseenden konsultroll.

Rapporten ger också slutsatser avseende den säkerhet styrelsen kan erhålla från granskningsarbete som utförts av befattningshavare i controllerfunktionen. Samtidigt som det kan innebära effektivitetsvinster att låta controllerfunktionen utföra granskningsuppgifter som traditionellt sett skulle utföras av en internrevisionsfunktion uppstår sannolikt risker för styrelsen och dess revisionsutskott på grund av framförallt lojalitet, egenintresse och rapporteringsvägarna, det vill säga oberoendeproblematik. Om en controller uppfyller kraven enligt COSO på kompetens och resurser, förefaller ändå riskerna för objektiviteten och oberoendet svåra att hantera. Rapporteringen kan förlora i både relevans och tillförlitlighet då en controller rapporterar först till sin CFO och CEO och därefter till styrelsen (och denna rapportering kan förstås istället utförs av någon av de senare, vilket inte självklart förmår mildra problemet). Av COSOs ramverk framgår att seniora befattningshavare kan rapportera direkt till styrelsen för att på så sätt stärka sitt oberoende från företagsledningen, även om de då ändå befinner sig inom företagsledningens domän. Inom områden där företagsledningen saknar objektivitet föreslås i COSO att styrelsen utökar sin övervakning. Det torde därför vara rimligt att som styrelse välja att inrätta en internrevisionsfunktion istället för att låta controllerrollen utföra tredje linjens uppgifter eftersom controllerrollen inte utformats med förutsättningar till en oberoende rapportering, medan internrevisorer har både en väl utvecklad praxis och standarder för oberoende.[6]

Rapporten ger också grund för att dra slutsatser om internrevision. Av IIAs olika vägledande material kring trelinjemodellen kan noteras att IIA tydligt påpekar att modellen omarbetats för att öka handlingsutrymmet för internrevisorer att kunna utföra rådgivnings- och konsulttjänster för sina organisationer och inte enbart granskning och revision. Syftet är alltså att glida åt vänster i trelinjemodellen. Detta går i linje med balansgången mellan revisions- och rådgivningstjänster som IIA försöker uppnå (Brady, 2019). Här blir rådgivning till företagsledningen en betydande aktivitet. Detta kan innebära en nackdel; att internrevisorers nytta för organisationen ökar för företagsledningens del, men också att konsulttjänster kan medföra att deras oberoende och objektivitet kan komma i fara och därmed kan deras nytta

[6] Om vikten av en oberoende rapportering och villkoren för sådan – se Eklöv Alander och Holmgren Caicedo (2023).

för styrelsen och revisionsutskott komma att minska. Den vetenskapliga litteraturen inom internrevisionsfältet beskriver denna problematik (Ahmad och Taylor, 2009; Eklöv Alander, 2023; Gramling mfl., 2018; Gustafsson Nordin, 2023; Roussy, 2013; Roussy och Rodrigue, 2018). Tredje linjen är en del av den interna kontrollen enligt externa revisorer medan internrevisorerna själva gärna ser sig som verksamma utanför den interna kontrollen. Enligt Abbott mfl. (2010) hör internrevisionen hemma inom den interna kontrollen. Här behövs ett klargörande i trelinjemodellen eftersom otydligheten skapar osäkerhet om rollaktörernas oberoende.

Av de texter som ligger till grund för dessa slutsatser framgår också att det råder oklarhet om betydelserna av begreppen rådgivning och konsulting, eller konsultationer. Då rådgivning springer direkt ur granskningsuppdraget är det oklart hur stor del som är rådgivning baserat på granskningsarbete och vad som utgör konsulting baserat på internrevisorers inneboende kunskap och expertis generellt sett. Visserligen kan en oklarhet som denna ge ett utökat handlingsutrymme för internrevisionsprofessionen, men med risk att oberoendet försvagas.

Trelinjemodellen, slutligen, är för närvarande under utveckling, och det kan vara rimligt att på ett tydligare sätt utforma ansvarsförhållandena för systemet för intern kontroll och riskhantering så att de tre linjerna utökas till att innefatta företagsledningens rapporteringsansvar till styrelsen. En rapportering från företagsledningen till styrelsen över den interna kontrollens effektivitet och ändamålsenlighet skulle kunna ligga till grund för internrevisionens granskningsarbete, och skillnaden mellan övervakningsaktiviteter, utförda av controllerrollen, och revisionsarbete, utfört av internrevisionsfunktionen, skulle kunna tydliggöras som ett led i denna omarbetning. Även begreppet ’försäkran’ och dess koppling till revision och avgivande av bestyrkande, skulle då kunna tydliggöras. En uppgift för forskare skulle kunna vara att studera innebörden i begreppet ’försäkran’ så som det används inom arbete med intern kontroll och riskhantering, och hur praktiken kring försäkringsgivande utförs, eftersom begreppet tycks ha en annan innebörd än den gängse inom revisionsteori.

Referenser

Abbott, J., Parker, S. & Peters, G. (2010). Serving two masters: the association between audit Committee internal audit oversight and internal audit activities. *Accounting horizons*, 24: 1–24.

Ahmad, Z. & Taylor, D. (2009). Commitment to independence by internal auditors: The effects of role ambiguity and role conflict. *Managerial Auditing Journal*, 24(9): 899–925. DOI: 10.1108/02686900910994827.

Arwinge, O. (2016). *En introduktion till internrevision.* Stockholm: Sanoma Utbildning.

Bantleon, U., d'Arcy, A., Eulerich, M., Hucke, A., Pedell, B. & Ratzinger-Sakel N.V.S. (2021). Coordination challenges in implementing the three lines of defense model. *International Journal of Auditing,* 25: 59–74. https://doi.org/10.1111/ijau.12201

Brady, K. (2019), *Striking an Optimal Balance Between Assurance and Consulting Services. Practical Insights from Internal Audit Leaders*, A CBOK Stakeholder Report, Internal Audit Foundation, Formerly the Institute of Internal Auditors Research Foundation (IIARF).

Burns, J. & Baldvinsdottir, G. (2005). An Institutional Perspective of Accountant's New Roles: The Interplay, of Contradictions and Praxis. *The European Accounting Review*, 14(4): 725–58.

Byrne, S. & Pierce, B. (2007). Towards a More Comprehensive Understanding of the Roles of Management Accountants. *European Accounting Review*, 16(3): 469–98.

COSO (2009). Internal control – integrated framework: Guidance on monitoring internal control systems, Volume 1: Guidance. Association Sections, Divisions, Boards, Teams. 381. American Institute of Certified Public Accountants (AICPA) Historical Collection. Committee of Sponsoring Organizations of the Treadway Commission. https://egrove.olemiss.edu/aicpa_assoc/381

COSO (2010). *Internal control – integrated framework: Guidance on monitoring internal control systems, Volume II: Application. Association Sections, Divisions, Boards, Teams.* 380. American Institute of Certified Public Accountants (AICPA) Historical Collection. Committee of Sponsoring Organizations of the Treadway Commission. https://egrove.olemiss.edu/aicpa_assoc/380

COSO (2013). *Internal control - integrated framework. Executive summary.* Committee of Sponsoring Organizations of the Treadway Commission. COSO, May.

COSO (2015). *Leveraging COSO across the three lines of defense.* Research commissioned by Committee of Sponsoring Organizations of the Treadway Commission. Committee of Sponsoring Organizations of the Treadway Commission, July 2015. Retrieved 2024-09-13. https://www.coso.org/_files/ugd/3059fc_cc80a9492ca743fd90d517049736c4da.pdf

Davies, H. & Zhivitskaya, M. (2018). Three Lines of Defence: A Robust Organising Framework, or Just Lines in the Sand? *Global Policy*, 9: 34-42. https://doi.org/10.1111/1758-5899.12568

Deloitte (2015). *COSO – Information and Communication & Monitoring Activities.* (Retrieved 2024-12-04). https://www.deloitte.com/ng/en/services/audit/perspectives/coso-information-and-communication-monitoring-activities.html

Friedman, A.L. & Lyne, S.R. (1997). Activity-Based Techniques and the Death of the Beancounter. *The European Accounting Review*, 6(1): 19–44.

Eklöv Alander, G. (2019). *En bok om revision.* Studentlitteratur.

Eklöv Alander, G. (2023). Internal auditor independence as a situated practice: four archetypes. *Accounting, Auditing & Accountability Journal*, *36*(9): 108-134. https://doi.org/10.1108/AAAJ-08-2019-4137

Eklöv Alander, G. & Holmgren Caicedo, M. (2023). *Oberoendets vara och inte vara i internrevisorernas praktik.* Akademin för ekonomistyrning i staten, Rapport 2023:1, Företagsekonomiska institutionen, Stockholms universitet.

Eklöv Alander, G. & Holmgren Caicedo, M. (2024). *Configurations of assurance: The role of professional governance actors in the assurance production of audit committees*. EAA 46th Annual Congress in Bucharest.

Eulerich, M. (2021). The new three lines model for structuring corporate governance – A critical discussion of similarities and differences. *Corporate Ownership & Control, 18*(2): 180-187. https://doi.org/10.22495/cocv18i2art15

Financial Services Authority, 2003. *Building a Framework For Operational Risk management: the FSA's Observations.* Financial Services Authority, London [Online]. Available: https://www.handbook.fca.org.uk/archive/2003/08/PS142_2. pdf.

Gramling, A.A., Schneider, A., & Bhaskar, L.S. (2018). Do consulting services performed by internal auditors influence their subsequent assessments when performing assurance services? *Advances in Accounting Behavioral Research*, Emerald Publishing Limited, Bingley, 21: 69–95. DOI: 10.1108/S1475-148820180000021004.

Gupta, P.P., Sami, H., Zhang, J.H. & Zhou, H. (2025). Does the 2013 COSO internal control framework improve the information environment in the U.S. capital markets? *Managerial Auditing Journal*, *40*(4): 357-383. https://doi.org/10.1108/MAJ-11-2023-4118

Gustafsson Nordin, I. G. (2023). Narratives of internal audit: The Sisyphean work of becoming independent. *Critical Perspectives on Accounting,* 94: 102448. https://doi.org/10.1016/j.cpa.2022.102448

Holmgren Caicedo, M., Mårtensson, M., & Tamm Hallström, K. (2018). The development of the management accountant's role revisited: An example from the Swedish Social Insurance Agency. *Financial Accountability & Management*, *34*(3): 240-251.

ICAEW (1999). Internal Control: Guidance for Directors on the Combined Code. Institute of Chartered Accountants in England and Wales London: ICAEW. https://www.ecgi.global/publications/codes/internal-control-guidance-for-directors-on-the-combined-code-turnbull-report

IIA (2013). *IIA Position Paper: The Three Lines of Defense in Effective Risk Management and Control*, The Institute of Internal Auditors, Altamonte Springs, FL.

IIA (2020a). *Global Perspectives and Insights, The Three Lines Model – An Important Tool for the Success of Every Organization.* The Institute of Internal Auditors, Inc. (Retrieved 2024-10-24) https://theiia.se/wp-content/uploads/2020/12/GPAI-Three-Lines-Model-An-Important-Tool-for-the-Success-of-Every-Organization.pdf

IIA (2020b). *The IIA's Three Lines Model. An Update of the Three Lines of Defense.* The Institute of Internal Auditors, Inc. (Retrieved 24-10-24). https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf

IIA Sweden (2020). *IIA's de tre linjernas modell. En uppdatering av de tre ansvarslinjerna.* The Institute of Internal Auditors, Inc. (Retrieved 2024-10-24) https://theiia.se/wp-content/uploads/2021/08/Svensk_oversattning_Three_Lines_Model.pdf

Espinosa-Jaramillo M.T. (2024). Internal Control in Companies from the Perspective of the COSO. *Management (Montevideo) = AG Management*. 2: 28. https://doi.org/10.62486/agma202428

Jensen, M. C. (1993). The Modern Industrial Revolution, Exit, and the Failure of Internal Control Systems. *The Journal of Finance*, *48*(3): 831–880. https://doi.org/10.2307/2329018

Karlsson, B., Hersinger, A. & Kurkkio, M. (2019). Hybrid accountants in the age of the business partner: exploring institutional drivers in a mining company. *Journal of Management Control*, *30*(2): 185-211.

Kurunmäki, L. (2004). A Hybrid Profession: The Acquisition of Management Accounting Expertise by Medical Professionals. *Accounting, Organizations and Society*, 26: 327–47.

Leech, T.J. & Hanlon, L.C. (2016). Three Lines of Defense versus Five Lines of Assurance: Elevating the Role of the Board and CEO in Risk Governance. In *The Handbook of Board Governance*, R. Leblanc (Ed.). https://doi.org/10.1002/9781119245445.ch17

McCrae, M., Balthazor, L. (2000). Integrating Risk Management into Corporate Governance: The Turnbull Guidance. *Risk Management, 2*: 35–45. https://doi.org/10.1057/palgrave.rm.8240057

Mihret, D.G. & Grant, B. (2017). The role of internal auditing in corporate governance: A Foucauldian analysis. *Accounting, Auditing & Accountability Journal,* 30(3): 699–719. DOI: 10.1108/AAAJ-10-2012-1134.

Neu, D., Everett, J. & Rahaman, A.S. (2013). Internal Auditing and Corruption within Government: The Case of the Canadian Sponsorship Program. *Contemporary Accounting Research*, 30(3): 1223-1250. https://doi.org/10.1111/j.1911-3846.2012.01195.x

Nilsson, F. & Olve, N. G. (2018). *Controllerhandboken* (11). Malmö: Liber.

Norman, C.S., Rose, A.M., & Rose, J.M. (2010). Internal audit reporting lines, fraud risk decomposition, and assessments of fraud risk. *Accounting, Organizations & Society*, 35(5): 546–557. DOI: 10.1016/j.aos.2009.12.003.

Pentland, B. (1993). Getting comfortable with the numbers: Auditing and the micro-production of macro-order. *Accounting, Organizations and Society*, 18(7/8): 605–620.

Power, M. (1997). *The audit society: rituals of verification.* Oxford University Press: Oxford.

PwC (2021). Internal Control over Financial Reporting (ICFR). Driving governance through effective financial reporting. Retrieved 2024-09-16. https://www.pwc.com/m1/en/services/assurance/risk-assurance/documents/internal-control-over-financial-reporting.pdf

Rezaee, Z. (1995). What the COSO report means for internal auditors. *Managerial Auditing Journal,* 10(6): 5–9. DOI: 10.1108/02686909510088350.

Roussy, M. (2013). Internal auditors' roles: From watchdogs to helpers and protectors of the top manager. *Critical Perspectives on Accounting*, 24(7–8): 550–571. DOI: 10.1016/j.cpa.2013.08.004.

Roussy, M. (2015). Welcome to the day-to-day of internal auditors: How do they cope with conflicts? *Auditing: A Journal of Practice & Theory*, 34(2): 237–264.

Roussy, M., & Brivot, M. (2016). Internal audit quality: A polysemous notion? Accounting, Auditing and Accountability Journal, 29(5): 714–738.

Roussy, M., & Perron, A. (2018). New perspectives in internal audit research: A structured literature review. *Accounting Perspectives*, 17(3): 345–385.

Roussy, M. & Rodrigue, M. (2018). Internal Audit: Is the 'Third Line of Defense' Effective as a Form of Governance? An exploratory study of the impression management techniques chief audit executives use in their annual accountability to the audit committee. *Journal of Business Ethics,* 151(3): 853–869. DOI: 10.1007/s10551-016-3263-y.

Tawfik, OI., Durrah, O. & Aljawhar, KA. (2023). The Role of The Internal Auditor in Strengthening the Governance of Economic Organizations Using the Three Lines of Defense Model. *Journal of Risk and Financial Management,* 16(341): 1-15. https://doi.org/10.3390/jrfm16070341

Uwadiae, O. (2015). COSO - Control activities. Financial Reporting, Deloitte. (Retrieved 2024-12-02). https://www.deloitte.com/ng/en/services/audit/perspectives/coso-control-activities.html

Valkenburg, B. & Bongiovanni, I. (2024). Unravelling the three lines model in cybersecurity: a systematic literature review. *Computers & Security,* 139: 1-11. https://doi.org/10.1016/j.cose.2024.103708.

Gunilla Eklöv Alander är docent i företagsekonomi med särskilt intresse för revisionsforskning. Gunilla är aktiv forskare inom Akademin för ekonomistyrning i staten på Företagsekonomiska institutionen vid Stockholms universitet.

Akademin för ekonomistyrning i staten (AES) är ett nätverk av forskare som tillsammans med praktiker arbetar för att initiera, skapa och förmedla kunskap om ekonomi- och verksamhetsstyrning i offentlig sektor.

ISBN 978-91-984607-5-9

Företagsekonomiska institutionen
Stockholms universitet SE-106 91 Stockholm www.sbs.su.se/aes

Stockholms universitet