Final Pronouncement
December 2019

International Standard on Auditing 315 (omarbetad 2019)

ISA 315 (omarbetad 2019)

och

följdändringar i andra internationella standarder till följd av ISA 315 (omarbetad 2019)

IAASB International Auditing and Assurance Standards Board

Om IAASB

Detta dokument har utarbetats och godkänts av International Auditing and Assurance Standards Board.

IAASB:s mål är att tillgodose allmänhetens intresse genom att fastställa revisions- och bestyrkandestandarder samt andra hänförliga standarder av hög kvalitet samt att underlätta konvergensen av internationella och nationella revisions- och bestyrkandestandarder, vilket leder till högre kvalitet och jämnare praxis i hela världen samt stärker allmänhetens förtroende för den globala revisions- och bestyrkandeprofessionen.

IAASB (International Auditing and Assurance Standards Board) utarbetar revisions- och bestyrkandestandarder samt vägledning för användning av alla revisorer/redovisningskonsulter utifrån en gemensam normgivningsprocess innefattande Public Interest Oversight Board, som tillser IAASB:s verksamhet, samt IAASB Consultative Advisory Group, som bidrar med perspektiv utifrån allmänhetens intresse vid utarbetande av standarder och vägledning. De strukturer och processer som ligger till grund för IAASB:s verksamhet stöds av IFAC (International Federation of Accountants).

INNEHÅLL

INTERNATIONAL STANDARD ON AUDITING 315 (OMARBETAD 2019)

IDENTIFIERA OCH BEDÖMA RISKERNA FÖR VÄSENTLIGA FELAKTIGHETER

(Gäller vid revision av finansiella rapporter för räkenskapsperioder som börjar den 15 december 2021 eller senare)

INNEHÅLL

Punkt

International Standard on Auditing (ISA) 315 (omarbetad 2019), *Identifiera och bedöma riskerna för väsentliga felaktigheter*, ska läsas tillsammans med ISA 200 *Den oberoende revisorns övergripande mål samt utförandet av en revision enligt International Standards on Auditing*.

ISA 315 (omarbetad 2019) har godkänts av Public Interest Oversight Board (PIOB) som drog slutsatsen att förankringsprocessen hade följts i utarbetandet av standarden och att allmänhetens intresse hade beaktats på vederbörligt sätt.

Inledning

Denna standards tillämpningsområde

1. Denna internationella revisionsstandard (ISA) behandlar revisorns ansvar för att identifiera och bedöma riskerna för väsentliga felaktigheter.

Nyckelbegrepp i denna standard

2. ISA 200 behandlar revisorns övergripande mål när han eller hon utför en revision av de finansiella rapporterna[1], däribland att uppnå tillräckliga och ändamålsenliga revisionsbevis för att minska revisionsrisken till en godtagbart låg nivå.[2] Revisionsrisk följer av riskerna för väsentliga felaktigheter och upptäcktsrisk.[3] I ISA 200 förklaras att risken för väsentliga felaktigheter kan föreligga på två nivåer:[4] den övergripande rapportnivån och påståendenivån för transaktionsslag, konton och upplysningar.

3. ISA 200 kräver att revisorn använder sitt professionella omdöme vid planeringen och genomförandet av revisionen, samt planerar och genomför revisionen med en professionellt skeptisk inställning som innebär att han eller hon är medveten om att det kan föreligga omständigheter som kan orsaka väsentliga felaktigheter i de finansiella rapporterna.[5]

4. Risker på rapportnivån avser risker som påverkar de finansiella rapporterna som helhet och kan påverka många påståenden. Risker för väsentliga felaktigheter på påståendenivån består av två delar, nämligen inneboende risker och kontrollrisker:

   - Inneboende risk beskrivs som känsligheten hos ett påstående om ett transaktionsslag, ett konto eller en upplysning för en felaktighet som skulle kunna vara väsentlig, antingen enskilt eller tillsammans med andra felaktigheter, före beaktande av eventuella kontroller.
   - Kontrollrisk beskrivs som risken för att en felaktighet som skulle kunna finnas i ett påstående om ett transaktionsslag, ett konto eller en upplysning och som skulle kunna vara väsentlig, antingen enskilt eller tillsammans med andra felaktigheter, inte förhindras eller upptäcks och rättas i tid via företagets system för intern kontroll.

5. I ISA 200 förklaras att risker för väsentliga felaktigheter bedöms på påståendenivån för att avgöra karaktären på, tidpunkten för och omfattningen av de fortsatta granskningsåtgärder som krävs för att inhämta tillräckliga och ändamålsenliga revisionsbevis.[6] För de identifierade riskerna för väsentliga felaktigheter på påståendenivån krävs enligt denna standard en separat bedömning av inneboende risk och kontrollrisk. Enligt förklaringen i ISA 200 är de inneboende riskerna högre för vissa påståenden och tillhörande transaktionsslag, konton och upplysningar än för andra. I vilken grad den inneboende risken varierar kallas i denna standard för ”spektrumet av inneboende risker”.

---

1 ISA 200 *Den oberoende revisorns övergripande mål samt utförandet av en revision enligt International Standards on Auditing*

2 ISA 200, punkt 17

3 ISA 200, punkt 13(c)

4 ISA 200, punkt A36

5 ISA 200, punkterna 15–16

6 ISA 200, punkt A43a och ISA 330, *Revisorns hantering av bedömda risker*, punkt 6

6. Risker för väsentliga felaktigheter som har identifierats och bedömts av revisorn omfattar både dem som beror på oegentligheter och dem som beror på misstag. Även om båda omfattas av denna ISA är oegentligheter av sådan betydelse att ytterligare krav och vägledning finns i ISA 240[7] avseende riskbedömning och näraliggande aktiviteter för att skaffa sig information som används för att identifiera, bedöma och vidta åtgärder avseende riskerna för väsentliga felaktigheter som beror på oegentligheter.

7. Revisorns process för identifiering och bedömning av risker är iterativ (med upprepning) och dynamisk. Revisorns förståelse av företaget och dess miljö, det tillämpliga ramverket för finansiell rapportering samt företagets system för intern kontroll hänger samman med och är beroende av kraven på att identifiera och bedöma riskerna för väsentliga felaktigheter. För att skaffa sig den förståelse som krävs enligt denna standard går det att ta fram inledande uppfattningar om riskerna, som sedan kan förfinas ytterligare när revisorn går vidare i processen för identifiering och bedömning av risker. Dessutom kräver denna standard och ISA 330 att revisorn reviderar riskbedömningen och ytterligare modifierar övergripande åtgärder och fortsatta granskningsåtgärder, baserat på de revisionsbevis som har inhämtats vid genomförandet av fortsatta granskningsåtgärder i enlighet med ISA 330, eller om ny information framkommer.

8. ISA 330 kräver att revisorn utformar och inför övergripande åtgärder för att hantera de bedömda riskerna för väsentliga felaktigheter på rapportnivån.[8] ISA 330 förklarar vidare att revisorns bedömning av riskerna för väsentliga felaktigheter på rapportnivån, och revisorns övergripande åtgärder, påverkas av revisorns förståelse för kontrollmiljön. ISA 330 kräver också att revisorn utformar och utför fortsatta granskningsåtgärder vilkas karaktär, tidpunkter för genomförande och omfattning baseras på och beaktar de bedömda riskerna för väsentliga felaktigheter på påståendenivån.[9]

Skalbarhet

9. ISA 200 anger att vissa standarder omfattar överväganden om skalbarhet, vilka illustrerar tillämpningen av kraven för alla företag, oavsett om deras karaktär och omständigheter är mindre komplexa eller mer komplexa.[10] Denna standard är avsedd för revisioner av alla företag, oavsett storlek och komplexitet och tillämpningen inbegriper därmed särskilda överväganden som är specifika för både mindre och mer komplexa företag, efter omständigheterna (i det enskilda fallet). Även om storleken på ett företag kan vara ett mått på dess komplexitet, kan vissa mindre företag vara mer komplexa och vissa större företag mindre komplexa.

Ikraftträdande

10. Denna standard gäller vid revision av finansiella rapporter för räkenskapsperioder som börjar den 15 december 2021 eller senare.

---

7 ISA 240, *Revisorns ansvar avseende oegentligheter i en revision av finansiella rapporter*

8 ISA 330, punkt 5

9 ISA 330, punkt 6

10 ISA 200, punkt A65a

Mål

11. Revisorns mål är att identifiera och bedöma riskerna för väsentliga felaktigheter, vare sig dessa beror på oegentligheter eller misstag, på rapport- och påståendenivåerna för att skapa en grund för att utforma och utföra åtgärder utifrån de bedömda riskerna för väsentliga felaktigheter.

Definitioner

12. I ISA har nedanstående termer följande betydelser:

    (a) Påståenden – uttalanden, uttryckliga eller på annat sätt uttalade, med avseende på redovisningen, värderingen, presentationen och lämnandet av information i de finansiella rapporterna som ligger i ledningens försäkran om att de finansiella rapporterna upprättas i enlighet med det tillämpliga ramverket för finansiell rapportering. Revisorn använder påståenden när han eller hon beaktar de olika typerna av potentiella felaktigheter som kan uppstå när han eller hon identifierar, bedömer och hanterar riskerna för väsentliga felaktigheter. (Se punkt A1)

    (b) *Affärsrisk* – en risk som härrör från betydelsefulla förhållanden, händelser, omständigheter, åtgärder eller passivitet som kan inverka negativt på ett företags möjlighet att nå sina mål och genomföra sina strategier, eller från olämpliga mål och strategier.

    (c) *Kontroller* – Riktlinjer och rutiner som ett företag inför för att uppnå ledningens eller styrelsens mål med kontrollen. I det här sammanhanget: (Se punkt A2–A5)

        (i) Riktlinjer är uttalanden om vad som bör, och inte bör, göras inom företaget för att utöva kontroll. Sådana uttalanden kan dokumenteras, formuleras uttryckligen i kommunikationen eller införas genom handlingar och beslut.

        (ii) Rutiner är handlingar för att införa riktlinjer.

    (d) *Allmänna IT-kontroller* – Kontroller av företagets IT-processer som stödjer den fortlöpande korrekta driften av IT-miljön, däribland att informationsbearbetningskontrollerna förblir effektiva och att integriteten i företagets information upprätthålls (dvs. att informationen är komplett, korrekt och giltig) i företagets informationssystem. Se även definitionen av *IT-miljö*.

    (e) *Informationsbearbetningskontroller* – Kontroller avseende bearbetningen av information i IT-program eller manuella informationsprocesser i företagets informationssystem som direkt riktar sig mot risker gällande informationens integritet (dvs. att transaktioner och övrig information är fullständiga, korrekta och giltiga). (Se punkt A6)

    (f) *Inneboende riskfaktorer* – Egenskaper hos händelser eller omständigheter som påverkar känsligheten för felaktigheter, vare sig dessa beror på oegentligheter eller misstag, i ett påstående om ett transaktionsslag, konto eller en upplysning, före beaktandet av kontroller. Sådana faktorer kan vara kvalitativa eller kvantitativa, och kan omfatta komplexitet, subjektivitet, förändring, osäkerhet eller känslighet för felaktigheter till följd av bristande

objektivitet hos företagsledningen eller andra riskfaktorer avseende oegentligheter[11] i den mån de påverkar den inneboende risken. (Se punkt A7–A8)

(g) *IT-miljö* – De IT-applikationer och den stödjande IT-infrastruktur, samt de IT-processer och den IT-personal som ingår och är delaktig i de processer som ett företag använder för att stödja affärsverksamheten och uppnå sina affärsstrategier. I standarden har nedanstående termer följande betydelser:

(i) En IT-applikation är ett program eller en uppsättning program som används vid införandet, bearbetningen, arkiveringen och rapporteringen av transaktioner eller information. IT-applikationer omfattar datalager och rapportgenerator.

(ii) IT-infrastrukturen omfattar nätverk, operativsystem samt databaser och dessas tillhörande hård- och mjukvara.

(iii) IT-processer är företagets processer för att hantera tillgång till IT-miljön, hantera förändringar av program eller förändringar av IT-miljön och IT-driften.

(h) *Relevanta påståenden* – Ett påstående om ett transaktionslag, konto eller en upplysning är relevant när det åtföljs av en identifierad risk för väsentliga felaktigheter. Fastställandet av huruvida ett påstående är ett relevant påstående görs före beaktande av eventuella tillhörande kontroller (dvs. den inneboende risken). (Se punkt A9)

(i) *IT-relaterade risker* – Känslighet hos informationsbearbetningskontroller, och risker gällande informationens integritet (dvs. att transaktioner och övrig information är fullständiga, korrekta och giltiga) i företagets informationssystem, till följd av en bristfällig utformning eller funktion av kontrollerna i företagets IT-processer (se IT-miljö).

(j) *Riskbedömningsåtgärder* – De granskningsåtgärder som utformas och utförs för att identifiera och bedöma riskerna för väsentliga felaktigheter, vare sig dessa beror på oegentligheter eller misstag, på rapport- och påståendenivåerna.

(k) *Betydande transaktionsslag, konton eller upplysningar* – Ett transaktionsslag, konto eller en upplysning som det finns ett eller flera relevanta påståenden om.

(l) *Betydande risk* – En identifierad risk för väsentliga felaktigheter: (Se punkt A10)

(i) för vilken bedömningen av den inneboende risken ligger nära den övre delen av spektrumet av inneboende risker till följd av den grad i vilken de inneboende riskfaktorerna påverkar kombinationen av sannolikheten för att en felaktighet uppkommer och omfattningen av den eventuella felaktigheten om den skulle uppkomma, eller

(ii) att den ska behandlas som en betydande risk enligt kraven i andra standarder.[12]

(m) *System för intern kontroll* – Det system som utformas, införs och upprätthålls av dem som har ansvar för företagets styrning (styrelsen), företagsledningen och annan personal för att ge rimlig säkerhet att företagets mål nås i fråga om finansiell rapportering, effektivitet i

[11] ISA 240, punkterna A24–A27

[12] ISA 240, punkt 27 och ISA 550, *Närståendeförhållanden*, punkt 18

verksamheten och att tillämpliga lagar och andra författningar följs. I ISA består systemet för intern kontroll av fem inbördes relaterade komponenter:

(i) kontrollmiljö

(ii) företagets riskbedömningsprocess

(iii) företagets process för att övervaka systemet för intern kontroll

(iv) informationssystem och kommunikation

(v) kontrollaktiviteter.

Krav

Riskbedömning och näraliggande aktiviteter

13. Revisorn ska utforma och genomföra riskbedömning för att erhålla revisionsbevis som erbjuder en ändamålsenlig grund för (Se punkt A11–A18)

    (a) att identifiera och bedöma risker för väsentliga felaktigheter, vare sig dessa beror på oegentligheter eller misstag, på rapport- och påståendenivåerna, och

    (b) utformningen av fortsatta granskningsåtgärder enligt ISA 330.

    Revisorn ska utforma och genomföra sin riskbedömning på ett sätt som inte är partiskt med/emot att inhämta revisionsbevis som kan vara stödjande eller mot att exkludera revisionsbevis som kan vara motsägelsefulla (Se punkt A14).

14. I riskbedömningen ska följande ingå: (Se punkt A19–A21)

    (a) frågor till företagsledningen och andra lämpliga personer inom företaget, däribland personer inom internrevisionsfunktionen (om sådan finns på företaget) (Se punkt A22–A26)

    (b) analytisk granskning (Se punkt A27–A31)

    (c) observation och inspektion. (Se punkt A32–A36)

Information från andra källor

15. När revisorn inhämtar revisionsbevis i enlighet med punkt 13 ska revisorn beakta information från (Se punkt A37–A38)

    (a) revisorns åtgärder avseende om han eller hon ska acceptera eller behålla en klientrelation eller revisionsuppdraget, och

    (b) när det är tillämpligt, andra uppdrag som utförs av den ansvariga revisorn för företaget.

16. När revisorn avser att använda den information som har inhämtats vid tidigare arbete åt företaget och från granskningsåtgärder i samband med tidigare revisioner, ska revisorn utvärdera om denna information fortfarande är relevant och tillförlitlig som revisionsbevis för den aktuella revisionen. (Se punkt A39–A41)

Diskussion i uppdragsteamet

17. Den ansvariga revisorn och andra nyckelpersoner i uppdragsteamet ska diskutera tillämpningen av det tillämpliga ramverket för finansiell rapportering och hur känsliga företagets finansiella rapporter är för väsentliga felaktigheter. (Se punkt A42–A47)

18. När det finns personer i uppdragsteamet som inte deltar i uppdragsteamets diskussion ska den ansvariga revisorn fastställa vilka frågor som dessa teammedlemmar ska informeras om.

Skaffa sig en förståelse av företaget och dess miljö, det tillämpliga ramverket för finansiell rapportering och företagets system för intern kontroll (se punkt A48–A49)

Förstå företaget och dess miljö samt det tillämpliga ramverket för finansiell rapportering (se punkt A50–A55)

19. Revisorn ska genomföra riskbedömning för att skaffa sig en förståelse av

    (a) följande aspekter av företaget och dess miljö:

        (i) företagets organisationsstruktur, ägande och styrning och dess affärsmodell, däribland i vilken grad affärsmodellen integrerar användningen av IT (se punkt A56–A67)

        (ii) branschspecifika faktorer, regelverk och andra externa faktorer (se punkt A68–A73) och

        (iii) vilka mått som används, intern och externt, för att bedöma företagets finansiella ställning (se punkt A74–A81)

    (b) det tillämpliga ramverket för finansiell rapportering och företagets redovisningsprinciper, samt skälen till eventuella förändringarna av dessa (se punkt A82–A84), och

    (c) hur inneboende riskfaktorer påverkar känsligheten i påståenden för felaktigheter och i vilken grad de gör det vid upprättandet av de finansiella rapporterna i enlighet med det tillämpliga ramverket för finansiell rapportering, baserat på den förståelse som revisorn skaffade sig under (a) och (b). (Se punkt A85–A89)

20. Revisorn ska bedöma om företagets redovisningsprinciper är ändamålsenliga och förenliga med det tillämpliga ramverket för finansiell rapportering.

Förstå komponenterna i företagets system för intern kontroll (se punkt A90–A95)

Kontrollmiljön, företagets riskbedömningsprocess och företagets process för att övervaka systemet för intern kontroll (se punkt A96–A98)

Kontrollmiljö

<table>
<tr><td colspan="2">21. Revisorn ska skaffa sig en förståelse av de delar av kontrollmiljön som är relevanta för upprättandet av de finansiella rapporterna genom att genomföra riskbedömning, genom att (Se punkt A99–A100)</td></tr>
<tr><td>(a) förstå den uppsättning kontroller, processer och strukturer som avser: (Se punkt A101–A102)</td><td>och
(b) utvärdera huruvida (se punkt A103–A108)</td></tr>
</table>

(i) hur ledningen utövar sitt tillsynsansvar över t.ex. företagets kultur och hur engagerad ledningen är i hederlighet och etiska värderingar (ii) när styrelsen är fristående från ledningen, styrelsens oberoende och dess tillsyn över företagets system för intern kontroll (iii) företagets fördelning av befogenheter och ansvar (iv) hur företaget attraherar, utvecklar och behåller kompetenta medarbetare, och (v) hur företaget håller olika personer ansvariga för deras ansvarsområden för att nå målen med systemet för intern kontroll	(i) företagsledningen, under tillsyn av styrelsen, har utvecklat och upprätthållit en kultur präglad av ärlighet och etiskt korrekt agerande (ii) kontrollmiljön erbjuder en tillräcklig grund för de andra komponenterna i företagets system för intern kontroll med beaktande av företagets karaktär och komplexitet, och (iii) brister i kontrollerna som identifieras i kontrollmiljön undergräver de andra komponenterna i företagets system för intern kontroll.

Företagets riskbedömningsprocess

22. Revisorn ska skaffa sig en förståelse av den del av företagets riskbedömningsprocess som är relevant för upprättandet av de finansiella rapporterna genom att genomföra riskbedömning, genom att	
(a) förstå företagets process för: (Se punkt A109–A110) (i) identifiering av affärsrisker som är relevanta för den finansiella rapporteringens mål (Se punkt A62) (ii) bedömning av betydelsen av dessa risker, samt hur sannolikt det är att de uppkommer, och (iii) vidta åtgärder mot dessa risker	och (b) utvärdera huruvida företagets riskbedömningsprocess är anpassad till företagets omständigheter med beaktande av företagets karaktär och komplexitet. (Se punkt A111–A113)

23. Om revisorn identifierar risker för väsentliga felaktigheter som företagsledningen misslyckats att identifiera, ska revisorn

(a) fastställa huruvida sådana risker är av en karaktär att revisorn förväntar sig att de skulle ha identifierats i företagets riskbedömningsprocess och, i så fall, skaffa sig en förståelse av varför företagets riskbedömningsprocess inte lyckades identifiera dessa risker för väsentliga felaktigheter, och

(b) överväga konsekvenserna för revisorns utvärdering i punkt 22(b).

Företagets process för att övervaka systemet för intern kontroll

24. Revisorn ska skaffa sig en förståelse av företagets process för att övervaka den del av systemet för intern kontroll som är relevant för upprättandet av de finansiella rapporterna genom att genomföra riskbedömning, genom att (se punkt A114–A115)

(a) förstå de aspekter av företagets processer som innefattar (i) fortlöpande och separata utvärderingar för att övervaka kontrollernas funktion, samt identifieringen och åtgärderna av de brister i kontrollerna som har identifierats (se punkt A116–A117) och (ii) företagets internrevisionsfunktion, om sådan finns, inklusive dess karaktär, ansvarsområden och aktiviteter (se punkt A118) (b) förstå de informationskällor som används i företagets process för övervakning av internrevisionen och den grund företagsledningen har för att bedöma om informationen är tillräckligt tillförlitlig för sitt syfte (se punkt A119–A120)	och (c) utvärdera huruvida företagets process för att övervaka systemet för intern kontroll är tillräcklig för företagets omständigheter med beaktande av företagets karaktär och komplexitet. (Se punkt A121–A122)

Informationssystem och kommunikation, samt kontrollaktiviteter (se punkt A123–A130)

Informationssystem och kommunikation

25. Revisorn ska skaffa sig en förståelse av de delar av företagets informationssystem och kommunikation som är relevanta för upprättandet av de finansiella rapporterna genom att genomföra riskbedömning, genom att (Se punkt A131)	
(a) förstå företagets informationsbearbetningsaktiviteter, inklusive dess data och information, de resurser som ska användas inom ramen för sådana aktiviteter och de riktlinjer som definierar, för väsentliga transaktionsslag, konton och upplysningar (se punkt A132–A143) (i) hur informationen flödar genom företagets informationssystem, däribland hur a. transaktioner initieras och hur information om dem registreras, bearbetas, i förekommande fall rättas, överförs till huvudboken och redovisas i de finansiella rapporterna, och b. information om händelser och omständigheter utöver transaktioner, som tas upp, bearbetas och redovisas i de finansiella rapporterna (ii) räkenskapsmaterialet, specifika konton i de finansiella rapporterna och övriga underlag hänförliga till informationsflödena i informationssystemet,	och (c) utvärdera om företagets informationssystem och kommunikation på ett bra sätt stödjer upprättandet av företagets finansiella rapporter i enlighet med det tillämpliga ramverket för finansiell rapportering. (Se punkt A146)

(iii) den process för finansiell rapportering som används för att upprätta företagets finansiella rapporter, inkluderande upplysningar, och (iv) företagets resurser, inklusive IT-miljön, relevanta för (a)(i) till (a)(iii) ovan (b) förstå hur företaget kommunicerar väsentliga frågor som stödjer upprättandet av de finansiella rapporterna och tillhörande ansvarsområden i informationssystemet och andra komponenter i systemet för intern kontroll: (Se punkt A144–A145) (i) mellan personer inom företaget, inklusive hur information förmedlas om roller och ansvarsområden inom den finansiella rapporteringen (ii) mellan företagsledning och styrelse, och (iii) med externa parter, t.ex. med tillsynsmyndigheter	

Kontrollaktiviteter

26. Revisorn ska skaffa sig en förståelse av kontrollaktivitetskomponenten genom att genomföra riskbedömning, genom att (se punkt A147–A157)	
(a) Identifiera kontroller som hanterar risker för väsentliga felaktigheter på påståendenivån i kontrollaktivitetskomponenten enligt följande: (i) kontroller som avser en risk som har fastställts vara en betydande risk (se punkt A158–A159) (ii) kontroller över bokföringsposter, däribland icke standardiserade bokföringsposter som används för att redovisa transaktioner av engångskaraktär, ovanliga transaktioner eller justeringar (se punkt A160–A161) (iii) kontroller som revisorn planerar att testa funktionen av för att fastställa substansgranskningens karaktär, tidpunkt och omfattning. Detta ska omfatta kontroller som avser risker för vilka inte enbart substansgranskning kan inhämta tillräckliga och ändamålsenliga revisionsbevis för, och (se punkt A162–A164) (iv) övriga kontroller som revisorn betraktar som lämpliga för att göra det möjligt för revisorn att uppnå målen i punkt 13 med avseende på riskerna	och (d) för varje kontroll som identifieras i (a) eller (c)(ii): (Se punkt A175–A181) (i) utvärdera huruvida kontrollen är utformad på ett effektivt sätt för att hantera risken för väsentliga felaktigheter på påståendenivån, eller effektivt utformad för att stödja funktionen av andra kontroller, och (ii) avgöra huruvida kontrollerna har införts genom att utföra åtgärder utöver att ställa frågor till företagets anställda.

på påståendenivån, grundat på revisorns professionella omdöme (se punkt A165) (b) baserat på kontroller identifierade vid (a), identifiering av IT-applikationer och andra aspekter av företagets IT-miljö som är föremål för IT-relaterade risker (se punkt A166–A172) (c) för sådana IT-applikationer och andra aspekter av IT-miljö som identifierats vid (b), identifiering av: (Se punkt A173–A174) (i) de relaterade IT-riskerna, och (ii) företagets allmänna IT-kontroller som hanterar sådana risker	

Brister i kontrollerna i företagets system för intern kontroll

27. Baserat på revisorns utvärdering av var och en av komponenterna i företagets system för intern kontroll ska revisorn fastställa huruvida en eller flera brister i kontrollerna har identifierats. (Se punkt A182–A183)

Identifiera och bedöma riskerna för väsentliga felaktigheter (se punkt A184–A185)

Identifiera risker för väsentliga felaktigheter

28. Revisorn ska identifiera riskerna för väsentliga felaktigheter och avgöra om de föreligger på (se punkt A186–A192)

    (a) rapportnivån (se punkt A193–A200) eller

    (b) påståendenivån för transaktionsslag, konton och upplysningar. (Se punkt A201)

29. Revisorn ska fastställa de relevanta påståendena och de tillhörande väsentliga transaktionsslagen, kontona och upplysningarna. (Se punkt A202–A204)

Bedöma riskerna för väsentliga felaktigheter på rapportnivån

30. för identifierade risker för väsentliga felaktigheter på rapportnivån ska revisorn bedöma riskerna och (se punkt A193–A200)

    (a) fastställa huruvida sådana risker påverkar bedömningen av risker på påståendenivån, och

    (b) utvärdera karaktären på och omfattningen av deras genomgripande effekt på de finansiella rapporterna.

Bedöma risker för väsentliga felaktigheter på påståendenivån

Bedöma inneboende risker (se punkt A205–A217)

31. För identifierade risker för väsentliga felaktigheter på påståendenivån ska revisorn bedöma de inneboende riskerna genom att bedöma sannolikheten för och omfattningen av felaktigheterna. När revisorn gör det ska han eller hon beakta hur och i vilken grad

    (a) de inneboende riskfaktorerna påverkar de relevanta påståendenas känslighet för väsentliga felaktigheter, och

    (b) riskerna för väsentliga felaktigheter på rapportnivån påverkar bedömningen av inneboende risker för risker för väsentliga felaktigheter på påståendenivån. (Se punkt A215–A216)

32. Revisorn ska fastställa huruvida några av de bedömda riskerna för väsentliga felaktigheter utgör betydande risker. (se punkt A218–A221)

33. Revisorn ska fastställa huruvida enbart substansgranskning inte räcker för att ge tillräckliga och ändamålsenliga revisionsbevis för vissa av riskerna för väsentliga felaktigheter på påståendenivån. (Se punkt A222–A225)

Bedöma kontrollrisken

34. Om revisorn planerar att granska kontrollernas funktion ska revisorn bedöma kontrollrisken. Om revisorn inte planerar att granska kontrollernas funktion ska revisorns bedömning av kontrollrisken vara sådan att bedömningen av risken för väsentliga felaktigheter är samma som bedömningen av inneboende risker. (Se punkt A226–A229)

Utvärdera revisionsbevisen inhämtade från riskbedömningsprocessen

35. Revisorn ska utvärdera huruvida revisionsbevisen inhämtade från riskbedömningen ger en ändamålsenlig grund för identifieringen och bedömningen av riskerna för väsentliga felaktigheter. Om så inte är fallet ska revisorn genomföra ytterligare riskbedömning till dess att revisionsbevis har inhämtats för att ge en sådan grund. När revisorn identifierar och bedömer risken för väsentliga felaktigheter ska han eller hon beakta samtliga revisionsbevis som har inhämtats från riskbedömningen, vare sig de stöder eller motsäger påståenden som görs av ledningen. (Se punkt A230–A232)

Transaktionsslag, konton och upplysningar som inte är betydande, men som är väsentliga

36. För väsentliga transaktionsslag, konton eller upplysningar som inte har bedömts vara betydande transaktionsslag, konton eller upplysningar ska revisorn utvärdera om hans eller hennes bedömningar fortfarande är riktiga. (Se punkt A233–A235)

Ändring av riskbedömning

37. Om revisorn erhåller ny information som är oförenlig med de revisionsbevis som revisorn ursprungligen grundade sin identifiering eller bedömning av risken för väsentliga felaktigheter på, ska revisorn omarbeta sin identifiering eller bedömning. (Se punkt A236)

Dokumentation

38. Revisorn ska i revisionsdokumentationen innefatta följande:[13] (se punkt A237–A241)

    (a) uppdragsteamets diskussion och de betydelsefulla beslut som fattas

    (b) viktiga delar av revisorns förståelse i enlighet med punkterna 19, 21, 22, 24 och 25, de informationskällor revisorns förståelse bygger på samt de riskbedömningsåtgärder som har utförts

    (c) utvärderingen av utformningen av identifierade kontroller, och fastställandet av huruvida sådana kontroller har införts, i enlighet med bestämmelserna i punkt 26, och

    (d) de identifierade och bedömda riskerna för väsentliga felaktigheter på rapport- och påståendenivån, däribland betydande risker och risker för vilka enbart substansgranskning inte ger tillräckliga och ändamålsenliga revisionsbevis samt skälen till de väsentliga bedömningar som görs.

Tillämpning och andra förtydliganden

Definitioner (se punkt 12)

Påståenden (se punkt 12(a))

A1. Revisorer använder kategorier av påståenden för att beakta de olika typerna av potentiella felaktigheter när de identifierar, bedömer och hanterar riskerna för väsentliga felaktigheter. Exempel på dessa kategorier av påståenden beskrivs i punkt A190. Påståendena skiljer sig från de skriftliga uttalanden som krävs enligt ISA 580,[14] för att bekräfta vissa förhållanden eller stödja övriga revisionsbevis.

Kontroller (se punkt 12(c))

A2. Kontroller är inbyggda i komponenterna i företagets system för intern kontroll.

A3. Riktlinjer införs genom handlingar utförda av företagets personal, eller genom att personalen avhåller sig från att vidta åtgärder som skulle kunna vara i strid med sådana riktlinjer.

A4. Rutiner kan införas genom formell dokumentation eller annan kommunikation från ledningen eller styrelsen, eller kan vara ett resultat av beteenden som inte är formellt införda utan snarare är en följd av företagskulturen. Rutiner kan upprätthållas genom att aktiviteter tillåts av de IT-applikationer som används av företaget eller andra aspekter av företagets IT-miljö.

A5. Kontroller kan vara direkta eller indirekta. Direkta kontroller är kontroller som har tillräcklig precision för att bemöta risker för väsentliga felaktigheter på påståendenivån. Indirekta kontroller är kontroller som understödjer direkta kontroller.

---

[13] ISA 230, *Dokumentation av revisionen*, punkterna 8–11 och A6–A7

[14] ISA 580, *Skriftliga uttalanden*

Informationsbearbetningskontroller (se punkt 12(e))

A6. Risker avseende informationens integritet uppkommer genom känsligheten för ett mindre verkningsfullt införande av företagets informationsriktlinjer, som är riktlinjer som definierar informationsflöden, informationslagring och redovisningsprocesser i företagets informationssystem. Informationsbearbetningskontroller är processer som stödjer ett ändamålsenligt införande av företagets riktlinjer avseende information. Informationsbearbetningskontroller kan vara automatiserade (dvs. inbäddade i IT-applikationer) eller manuella (t.ex. kontroller av in- eller utdata) och kan vara beroende av andra kontroller, däribland andra informationsbearbetningskontroller och allmänna IT-kontroller.

Inneboende riskfaktorer (se punkt 12(f))

> **Bilaga 2** anger ytterligare överväganden hänförliga till förståelsen av inneboende riskfaktorer.

A7. Inneboende riskfaktorer kan vara kvalitativa eller kvantitativa och påverkar påståendenas känslighet för väsentliga felaktigheter. Kvalitativa inneboende riskfaktorer avseende upprättandet av information som krävs enligt det tillämpliga ramverket för finansiell rapportering omfattar

- komplexitet
- subjektivitet
- förändring
- osäkerhet, och
- känslighet för felaktigheter till följd av bristande objektivitet hos företagsledningen eller andra riskfaktorer avseende oegentligheter i den mån de påverkar den inneboende risken.

A8. Övriga inneboende riskfaktorer som påverkar känsligheten för felaktigheter i ett påstående om ett transaktionsslag, konto eller en upplysning kan bland annat omfatta:

- den kvalitativa eller kvantitativa betydelsen av transaktionsslaget, kontot eller upplysningen, eller
- volymen eller brist på enhetlighet i sammansättningen av de poster som ska bearbetas genom transaktionsslaget eller kontot, eller återspeglas i upplysningen.

Relevanta påståenden (se punkt 12(h))

A9. En risk för väsentliga felaktigheter kan avse ett eller flera påståenden, och i så fall är samtliga påståenden, som en sådan risk avser, relevanta påståenden. Om ett påstående inte innehåller en identifierad risk för väsentliga felaktigheter är det inte ett relevant påstående.

Betydande risk (se punkt 12(l))

A10. Betydelsen kan beskrivas som hur viktig ett relativt förhållande är, och bedöms av revisorn i det sammanhang där förhållandet bedöms. För inneboende risker kan betydelsen bedöms inom sammanhanget av hur, och i vilken grad, de inneboende riskfaktorerna påverkar kombinationen av

sannolikheten för att en felaktighet uppkommer och omfattningen av den eventuella felaktigheten om den skulle uppkomma.

Riskbedömning och näraliggande aktiviteter (se punkt 13–18)

A11. I de risker för väsentliga felaktigheter som ska identifieras och bedömas ingår både de som beror på oegentligheter och de som beror på misstag, och båda omfattas av denna standard. Oegentligheter är emellertid av sådan betydelse att ytterligare krav och vägledning finns i ISA 240 avseende riskbedömning och näraliggande aktiviteter för att skaffa sig information som används vid identifiering och bedömning av riskerna för väsentliga felaktigheter som beror på oegentligheter.[15] Därutöver erbjuder följande standarder ytterligare krav och vägledning vad gäller att identifiera och bedöma risker för väsentliga felaktigheter avseende specifika frågor eller omständigheter:

- ISA 540 (omarbetad)[16] med avseende på uppskattningar i redovisningen;
- ISA 550[22] med avseende på relationer och transaktioner med närstående.
- ISA 570 (omarbetad)[17] med avseende på företagets förmåga att fortsätta verksamheten; och
- ISA 600[18] med avseende på koncernredovisningar.

A12. En professionellt skeptisk inställning är nödvändig för en kritisk bedömning av de revisionsbevis som har inhämtats vid genomförandet av riskbedömningen, och hjälper revisorn att förbli uppmärksam på att revisionsbevisen inte brister i objektivitet så att de bekräftar förekomsten av risker eller kan vara motsägelsefulla i fråga om förekomsten av risker. En professionellt skeptisk inställning är en hållning som intas av revisorn när han eller hon gör professionella bedömningar som sedan utgör grund för revisorns åtgärder. Revisorn använder professionellt omdöme för att avgöra när revisorn har revisionsbevis som erbjuder en ändamålsenlig grund för riskbedömningen.

A13. Tillämpningen av en professionellt skeptisk inställning från revisorns sida kan omfatta att

- ifrågasätta motsägelsefull information och dokuments tillförlitlighet
- beakta svar på frågor och övrig information som har inhämtats från ledning och styrelse
- vara uppmärksam på omständigheter som kan tyda på möjliga felaktigheter vare sig dessa beror på oegentligheter eller misstag, och
- bedöma huruvida de revisionsbevis som har inhämtats stödjer revisorns identifiering och bedömning av risken för väsentliga felaktigheter mot bakgrund av företagets karaktär och omständigheter.

Varför det är viktigt att inhämta revisionsbevis på ett opartiskt sätt (se punkt 13)

---

15 ISA 240, punkterna 12–27

16 ISA 540 (omarbetad), *Granskning av uppskattningar i redovisningen med tillhörande upplysningar*

17 ISA 570 (omarbetad), *Fortsatt drift*

18 ISA 600, *Särskilda överväganden – revision av koncernredovisningar (däribland arbete som utförs av revisorer för delar av arbetet)*

A14. Att på ett opartiskt sätt utforma och genomföra riskbedömning för att identifiera eventuella motsägelsefulla upplysningar, kan hjälpa revisorn att tillämpa en professionellt skeptisk inställning när han eller hon identifierar och bedömer riskerna för väsentliga felaktigheter.

Källor till revisionsbevis (se punkt 13)

A15. Att utforma och genomföra riskbedömning för att inhämta revisionsbevis på ett opartiskt sätt kan omfatta att inhämta bevis från olika källor inom och utom företaget. Revisorn behöver emellertid inte utföra en uttömmande sökning för att identifiera alla möjliga källor till revisionsbevis. Utöver information från andra källor[19], kan informationskällor till riskbedömningsprocesser omfatta

- kontakter med ledningen, styrelsen och andra nyckelpersoner inom företaget, såsom internrevisorer
- vissa externa parter, såsom tillsynsmyndigheter, vare sig informationen inhämtas direkt eller indirekt
- offentligt tillgänglig information om företaget, t.ex. pressmeddelanden publicerade av företaget och material till analytiker eller möten med investerargrupper, analytikers rapporter eller information om handelsaktivitet.

Oavsett informationskällan ska revisorn beakta relevansen och tillförlitligheten hos den information som ska användas som revisionsbevis i enlighet med ISA 500.[20]

Skalbarhet (se punkt 13)

A16. Karaktären på och omfattningen av riskbedömningen varierar baserat på företagets karaktär och omständigheter (t.ex. formaliteten i företagets riktlinjer och rutiner, samt processer och system). Revisorn ska använda sitt professionella omdöme för att avgöra karaktären på och omfattningen av de åtgärder som ska genomföras för att uppfylla kraven i denna standard.

A17. Även om graden av hur formaliserade ett företags riktlinjer och rutiner samt processer och system är kan variera, måste revisorn ändå skaffa sig den förståelsen enligt punkterna 19, 21, 22, 24, 25 och 26.

> **Exempel**:
>
> Vissa företag, inklusive mindre komplexa företag, och i synnerhet ägarledda företag, kanske inte har etablerade strukturerade processer och system (t.ex. en riskbedömningsprocess eller en process för att övervaka systemet för intern kontroll) eller kanske har etablerade processer eller system med begränsad dokumentation eller brist på konsekvens i hur de genomförs. När sådana system och processer saknar formalitet kan revisorn ändå genomföra riskbedömningen genom observationer och frågor.

[19] Se punkterna A37 och A38.

[20] ISA 500, *Revisionsbevis*, punkt 7

Andra företag, vanligtvis mer komplexa företag, förväntas ha mer formaliserade och dokumenterade riktlinjer och rutiner. Revisorn kan använda sådan dokumentation när han eller hon genomför riskbedömningen.

A18. Karaktären på och omfattningen av riskbedömningen som ska genomföras första gången ett uppdrag utförs kan vara mer omfattande än åtgärderna vid ett återkommande uppdrag. Under efterföljande perioder kan revisorn ha fokus på förändringar som har inträffat sedan den föregående perioden.

Typer av riskbedömningsåtgärder (se punkt 14)

A19. ISA 500[21] förklarar vilka typer av granskningsåtgärder som kan genomföras för att inhämta revisionsbevis från riskbedömningen och fortsatta granskningsåtgärder. Granskningsåtgärdernas art, tidpunkt och omfattning kan påverkas av det faktum att en del av redovisningsuppgifterna och övriga bevis kanske bara finns tillgängliga i elektronisk form eller bara vid vissa tidpunkter.[22] Revisorn kan utföra substansgranskning eller granskning av kontroller, i enlighet med ISA 330, samtidigt som riskbedömningen görs, när det är effektivt att göra så. Revisionsbevis som inhämtas som stödjer identifiering och bedömning av risker för väsentliga felaktigheter kan också stödja upptäckten av felaktigheter på påståendenivån eller utvärderingen av kontrollernas funktion.

A20. Även om revisorn är skyldig att utföra all den riskbedömning som beskrivs i punkt 14 för att skaffa sig en förståelse av företaget och dess miljö, det tillämpliga ramverket för finansiell rapportering och företagets system för intern kontroll (se punkterna 19–26), behöver han eller hon inte utföra den avseende alla aspekter av den förståelsen. Andra åtgärder kan utföras när den information som avses inhämtas kan bidra till att risker för väsentliga felaktigheter identifieras. Exempel på sådana åtgärder kan omfatta att ställa frågor till företagets externa juridiska rådgivare eller externa tillsynsorgan, eller till värderingsspecialister som företaget har anlitat.

Automatiserade verktyg och tekniker (se punkt 14)

A21. När revisorn använder automatiserade verktyg och tekniker kan han eller hon genomföra riskbedömning av stora datavolymer (från huvudboken, reskontror eller annan verksamhetsdata) för bland annat analyser, omräkningar, upprepning eller avstämningar.

Frågor till företagsledningen och andra personer inom företaget (se punkt 14(a))

Varför frågor ställs till företagsledningen och andra personer inom företaget

A22. Information som inhämtas av revisorn för att stödja en ändamålsenlig grund för identifieringen och bedömningen av riskerna, samt utformningen av fortsatta granskningsåtgärder, kan uppnås genom att ställa frågor till ledningen och de personer som ansvarar för den finansiella rapporteringen.

A23. Frågor till ledningen och de personer som ansvarar för den finansiella rapporteringen och till andra anställda på olika nivåer kan ge revisorn olika perspektiv när han eller hon identifierar och bedömer risker för väsentliga felaktigheter.

---

[21] ISA 500, punkterna A14–A17 och A21–A25

[22] ISA 500, punkterna A12

Exempel:

- Frågor till styrelsen kan hjälpa revisorn att förstå omfattningen av den tillsyn som styrelsen har över ledningens upprättande av de finansiella rapporterna. ISA 260 (omarbetad)[23] identifierar vikten av effektiv tvåvägskommunikation som stöd för revisorn när han eller hon inhämtar information av styrelsen i detta avseende.
- Frågor till personer som ansvarar för att initiera, bearbeta eller registrera komplicerade eller ovanliga transaktioner kan hjälpa revisorn att bedöma hur lämpligt valet och tillämpningen av vissa redovisningsprinciper är.
- Frågor till internjurister kan ge information om frågor som tvister, om lagar och andra författningar följs, kännedom om oegentligheter eller misstänkta oegentligheter som påverkar företaget, garantier, förpliktelser efter försäljning, överenskommelser (t.ex. samriskföretag) med affärspartner och innebörden av avtalsmässiga villkor.
- Frågor till marknads- eller försäljningspersonal kan ge information om förändringar i företagets marknadsstrategier, försäljningstrender eller dess avtal med kunder.
- Frågor till riskhanteringsfunktionen (eller frågor till dem som har sådana roller) kan ge information om verksamhets- eller regulatoriska risker som kan påverka den finansiella rapporteringen.
- Frågor till IT-personal kan ge information om systemändringar, incidenter avseende system- eller kontroller eller andra risker som rör IT.

Överväganden som särskilt gäller företag inom den offentliga sektorn

A24. När revisorerna ställer frågor till dem som kan ha information som sannolikt kan vara till hjälp vid identifieringen av risker för väsentliga felaktigheter kan revisorer i företag inom offentlig sektor inhämta information från ytterligare källor, t.ex. från de revisorer som är delaktiga i effektivitetsrevision eller andra revisioner hänförliga till företaget.

Frågor till internrevisionsfunktionen

Bilaga 4 anger vad som behöver beaktas för att förstå ett företags internrevisionsfunktion.

Varför frågor ställs till internrevisionsfunktionen (om funktionen finns)

A25. Om ett företag har en internrevisionsfunktion kan frågor till lämpliga personer inom funktionen hjälpa revisorn att skaffa sig en förståelse av företaget och dess miljö, samt företagets system för intern kontroll vid identifieringen och bedömningen av riskerna.

[23] ISA 260 *Kommunikation med dem som har ansvar för företagets styrning* (omarbetad), punkt 4 b.

Överväganden som särskilt gäller företag inom den offentliga sektorn

A26. Revisorer i företag i den offentliga sektorn har ofta ytterligare ansvarsområden med avseende på intern kontroll och att tillämpliga lagar och andra författningar följs. Frågor till lämpliga personer inom internrevisionsfunktionen kan hjälpa revisorerna att identifiera riskerna för väsentliga överträdelser av tillämpliga lagar och andra författningar, och riskerna för brister i den interna kontrollen över finansiell rapportering.

Analytisk granskning (se punkt 14(b))

Varför analytisk granskning är en åtgärd vid riskbedömning

A27. Analytisk granskning bidrar till att identifiera inkonsekvenser, ovanliga transaktioner eller händelser, och belopp, nyckeltal och trender som kan vara tecken på förhållanden som kan påverka revisionen. Ovanliga eller oväntade relationer som identifieras kan hjälpa revisorn att identifiera risker för väsentliga felaktigheter, framför allt risker för väsentliga felaktigheter som beror på oegentligheter.

A28. Analytisk granskning som en åtgärd vid riskbedömning kan därför vara till hjälp för att identifiera och bedöma riskerna för väsentliga felaktigheter genom att identifiera aspekter på företaget som revisorn inte var medveten om eller förstå hur inneboende riskfaktorer, såsom förändringar, påverkar känsligheten i påståenden för felaktigheter.

Typer av analytisk granskning

A29. Analytisk granskning som genomförs som riskbedömning kan

- innefatta både finansiell och icke-finansiell information, t.ex. relationen mellan försäljning och försäljningsyta eller försäljningsvolym (icke-finansiell)
- använda sig av data som har samlats in på hög nivå. Följaktligen kan resultaten från den analytiska granskningen ge en grov första indikation på sannolikheten för väsentliga felaktigheter.

> **Exempel**:
>
> Vid revisionen av många företag, däribland sådana med mindre komplexa affärsmodeller och processer samt ett mindre komplext informationssystem kan revisorn genomföra en enkel jämförelse av informationen, t.ex. förändringen i delårsmässiga eller månatliga kontosaldon från saldon under tidigare perioder för att få en indikation på områden med potentiellt högre risk.

A30. Denna standard behandlar revisorns användning av analytisk granskning som riskbedömning. ISA 520[24] behandlar revisorns användning av analytisk granskning som substansgranskning (”substansinriktad analytisk granskning”) och revisorns ansvar för att genomföra en analytisk granskning nära slutet av revisionen. Följaktligen krävs det inte att analytisk granskning utförd som riskbedömning utförs enligt kraven i ISA 520. Däremot kan kraven och tillämpningsmaterialet i ISA

[24] ISA 520, *Analytisk granskning*

520 ge revisorn användbar vägledning när revisorn genomför analytisk granskning som en del av riskbedömningen.

Automatiserade verktyg och tekniker

A31. Analytisk granskning kan genomföras med användning av ett antal verktyg eller tekniker, som kan vara automatiserade. Att tillämpa automatiserad analytisk granskning på data kan gå under benämningen dataanalys.

> **Exempel**:
>
> Revisorn kan använda ett kalkylark för att jämföra faktiska redovisade belopp med budgeterade belopp, eller kan använda ett mer avancerat tillvägagångssätt genom att extrahera data från företagets informationssystem, och sedan analysera dessa data med hjälp av visualiseringstekniker för att identifiera transaktionsslag, konton eller upplysningar som det kan krävas ytterligare specifika riskbedömningsåtgärder för.

Observation och inspektion (se punkt 14(c))

Varför observation och inspektion genomförs som riskbedömning

A32. Observation och inspektion kan stödja, bekräfta eller motsäga förfrågningar till företagsledningen och andra, och kan även ge information om företaget och dess miljö.

Skalbarhet

A33. I de fall där riktlinjer eller rutiner inte är dokumenterade, eller företaget har mindre formaliserade kontroller, kan revisorn ändå inhämta vissa revisionsbevis för att stödja identifieringen och bedömningen av risker för väsentliga felaktigheter genom att observera eller inspektera hur kontrollen genomförs.

> **Exempel**:
>
> - Revisorn kan skaffa sig en förståelse av kontrollerna över en inventering, även om dessa inte har dokumenterats av företaget, genom direkta observationer.
> - Revisorn kan observera arbetsfördelningen.
> - Revisorn kan observera hur lösenord skrivs in.

Observation och inspektion som riskbedömning

A34. Riskbedömningen kan omfatta observation eller inspektion av följande:

- företagets verksamhet
- interna dokument (såsom affärsplaner och affärsstrategier), annan dokumentation och handböcker för intern kontroll

- rapporter som har upprättats av företagsledningen (t.ex. interna kvartalsrapporter till/från företagsledningen och delårsrapporter) och styrelsen (t.ex. protokoll från styrelsemöten)
- företagets lokaler och produktionsanläggningar
- information från externa källor, t.ex. branschtidningar och ekonomiska tidskrifter, rapporter från analytiker, banker eller kreditvärderingsinstitut, publikationer från tillsynsorgan och ekonomiska publikationer, eller andra externa dokument om företagets finansiella ställning (t.ex. de som anges i punkt A79)
- hur ledningen eller styrelsen beter sig och agerar (som att observera ett möte med revisionsutskottet).

Automatiserade verktyg och tekniker

A35. Automatiserade verktyg och tekniker kan också användas för att observera eller inspektera i synnerhet tillgångar, till exempel genom användning av fjärrstyrda observationsverktyg (t.ex. en drönare).

Överväganden som särskilt gäller företag inom den offentliga sektorn

A36. Riskbedömning som genomförs av revisorer av företag inom den offentliga sektorn kan också omfatta observation och inspektion av dokument upprättade av ledningen för ett lagstiftande organ, t.ex. hänförliga till obligatorisk resultatrapportering.

Information från andra källor (se punkt 15)

Varför revisorn beaktar information från andra källor

A37. Information som har inhämtats från andra källor kan vara relevant för identifiering och bedömning av riskerna för väsentliga felaktigheter genom att ge information och insikter om

- företagets karaktär och dess affärsrisker och vad som han ha förändrats från tidigare perioder
- ledningens och styrelsens hederlighet och etiska värderingar, som också kan vara relevanta för revisorns förståelse av kontrollmiljön
- det tillämpliga ramverket för finansiell rapportering och dess tillämpning på företagets karaktär och omständigheter.

Andra relevanta källor

A38. Andra relevanta informationskällor omfattar:

- Revisorns processer avseende om han eller hon ska acceptera eller behålla en klientrelation eller ett revisionsuppdrag enligt ISA 220, inbegripet de slutsatser som har dragits vid dessa.[25]
- Andra uppdrag som utförs för företaget av den ansvariga revisorn. Den ansvariga revisorn kan ha inhämtat kunskaper relevanta för revisionen, däribland om företaget och dess miljö, när han eller hon utför andra uppdrag för företaget. Vissa uppdrag kan omfatta granskning enligt

[25] ISA 220, *Kvalitetskontroll för revision av finansiella rapporter,* punkt 12

särskild överenskommelse eller andra revisions- eller bestyrkandeuppdrag, däribland uppdrag att hantera tillkommande rapporteringskrav i jurisdiktionen.

Information från revisorns tidigare erfarenhet av företaget och tidigare revisioner (se punkt 16)

Varför information från tidigare revisioner är viktig för den aktuella revisionen

A39. Revisorns tidigare erfarenhet av företaget och från de granskningsåtgärder som har utförts under tidigare revisioner kan ge revisorn information som är relevant för revisorns fastställande av karaktären på och omfattningen av riskbedömningsåtgärderna, samt identifieringen och bedömningen av risker för väsentliga felaktigheter.

Karaktären på informationen från tidigare revisioner

A40. Revisorns tidigare erfarenhet av företaget och de granskningsåtgärder som har utförts under tidigare revisioner kan ge revisorn information om frågor som

- tidigare felaktigheter och huruvida de rättades till utan onödigt dröjsmål
- karaktären på företaget och dess miljö samt företagets system för intern kontroll (innefattande brister i intern kontroll)
- eventuella betydelsefulla förändringar i företaget eller dess verksamhet sedan föregående räkenskapsperiod
- de särskilda typer av transaktioner eller andra händelser eller konton (och tillhörande upplysningar) där revisorn hade problem med att utföra de granskningsåtgärder som behövdes, t.ex. på grund av deras komplexitet.

A41. Det åligger revisorn att avgöra huruvida den information som har inhämtats vid tidigare arbete åt företaget och från granskningsåtgärder i samband med tidigare revisioner förblir relevant och tillförlitlig, om revisorn har för avsikt att använda den informationen som revisionsbevis för den aktuella revisionen. Om företagets karaktär eller omständigheter har förändrats eller ny information har inhämtats kanske informationen från tidigare perioder inte längre är relevant eller tillförlitlig för den aktuella revisionen. För att avgöra om förändringarna kan påverka informationens relevans eller tillförlitlighet kan revisorn ställa frågor och utföra andra lämpliga granskningsåtgärder, t.ex. följa transaktioner genom relevanta redovisningssystem, s.k. ”walk-through”-test. Om information inte är tillförlitlig kan revisorn överväga att genomföra ytterligare granskningsåtgärder som är lämpliga i sammanhanget.

Diskussion i uppdragsteamet (se punkt 17–18)

Varför uppdragsteamet måste diskutera tillämpningen av det tillämpliga ramverket för finansiell rapportering och hur känsliga företagets finansiella rapporter är för väsentliga felaktigheter.

A42. Diskussionen inom uppdragsteamet om tillämpningen av det tillämpliga ramverket för finansiell rapportering och hur känsliga företagets finansiella rapporter är för väsentliga felaktigheter tillför följande:

- Ger tillfälle för mer erfarna medlemmar i uppdragsteamet, däribland den ansvariga revisorn, att dela med sig av sina insikter utifrån deras kunskap om företaget. Informationsutbyte bidrar till en förbättrad förståelse hos alla medlemmar i uppdragsteamet.
- Möjliggör för medlemmarna i uppdragsteamet att utbyta information om de affärsrisker som företaget är utsatt för, hur inneboende riskfaktorer kan påverka känsligheten för felaktigheter i transaktionsslag, konton och upplysningar, samt om hur och var väsentliga felaktigheter som beror på oegentligheter eller misstag kan tänkas förekomma i de finansiella rapporterna.
- Hjälper medlemmarna i uppdragsteamet att få en bättre förståelse av risken för väsentliga felaktigheter i de finansiella rapporterna inom de särskilda områden som de har tilldelats, och hjälper dem att förstå hur resultaten av de granskningsåtgärder som de utför kan påverka andra delar av revisionen, däribland beslut om fortsatta granskningsåtgärders art, tidpunkter och omfattning. Framför allt hjälper diskussionen uppdragsteamets medlemmar att ytterligare beakta motsägelsefull information baserat på varje enskild medlems förståelse av företagets karaktär och omständigheter.
- Utgör en grund som uppdragsteamets medlemmar kan använda för att kommunicera och utbyta ny information som de har inhämtat under revisionen och som kan påverka bedömningen av risker för väsentliga felaktigheter eller de granskningsåtgärder som utförs för att hantera dessa risker.

ISA 240 kräver att uppdragsteamets diskussion lägger särskild vikt vid hur och var företagets finansiella rapporter kan vara känsliga för väsentliga felaktigheter som beror på oegentligheter, inklusive hur oegentligheterna kan uppkomma.[26]

A43. En professionellt skeptisk inställning är nödvändig för en kritisk bedömning av revisionsbevis, och en robust och öppen diskussion i teamet, däribland för återkommande revisioner, kan leda till en förbättrad identifiering och bedömning av risken för väsentliga felaktigheter. Ett annat resultat av diskussionen kan vara att revisorn identifierar särskilda områden i revisionen där en professionellt skeptisk inställning kan vara särskilt betydelsefull, och kan leda till att han eller hon engagerar mer erfarna medlemmar i uppdragsteamet som har lämplig kompetens att delta i granskningsåtgärder hänförliga till dessa områden.

Skalbarhet

A44. När uppdraget utförs av en enda person, såsom en enmansbyrå (dvs. där det inte skulle vara möjligt med en diskussion i uppdragsteamet), kan ett beaktande av frågorna som anges i punkterna A42 och A46 ändå kan hjälpa revisorn att identifiera var det kan finnas en risk för väsentliga felaktigheter.

A45. När ett uppdrag utförs av ett stort uppdragsteam, exempelvis vid revisionen av koncernredovisningar, är det inte alltid nödvändigt eller praktiskt att alla medlemmar deltar i en gemensam diskussion (t.ex. vid en revision som omfattar flera olika orter) och alla medlemmar i uppdragsteamet inte heller behöver informeras om alla beslut som fattats vid diskussionen. Den ansvariga revisorn kan diskutera vissa frågor med nyckelpersoner i uppdragsteamet och, om det anses lämpligt, personer med särskild kompetens eller kunskap och personer som ansvarar för revision av koncernenheter, och

[26] ISA 240, punkt 16

delegera diskussioner med andra i uppdragsteamet med hänsyn tagen till den kommunikation som anses nödvändig. En kommunikationsplan som har godkänts av ansvarig revisor kan komma väl till pass.

Diskussion om upplysningar i det tillämpliga ramverket för finansiell rapportering

A46. Som del av diskussionen i uppdragsteamet är det till hjälp att beakta upplysningskraven i det tillämpliga ramverket för finansiell rapportering för att tidigt under revisionen identifiera var det kan finnas risker för väsentliga felaktigheter med avseende på upplysningar, även under omständigheter där det tillämpliga ramverket för finansiell rapportering enbart kräver förenklade upplysningar. Frågor som uppdragsteamet kan diskutera innefattar följande:

- Ändringar i krav i ramverk för finansiell rapportering, som kan leda till betydande nya eller ändrade upplysningar.
- Ändringar eller förändringar i företagets miljö, ekonomi eller verksamhet som kan leda till betydande nya eller ändrade upplysningar, t.ex. ett betydande rörelseförvärv under den period som revideras.
- Upplysningar för vilka det tidigare varit svårt att inhämta tillräckliga och ändamålsenliga revisionsbevis.
- Upplysningar om komplexa frågor, däribland dem som innefattar betydande bedömningar av företagsledningen om vilka upplysningar som ska lämnas.

Överväganden som särskilt gäller företag inom den offentliga sektorn

A47. Som en del av diskussionen i uppdragsteamet för revisorer i företag inom den offentliga sektorn kan revisorerna även beakta ytterligare och bredare mål samt tillhörande risker hänförliga till krav eller skyldigheter för revision av företag inom den offentliga sektorn.

Skaffa sig en förståelse för företaget och dess miljö, det tillämpliga ramverket för finansiell rapportering och företagets system för intern kontroll (se punkt 19–27)

> **Bilagorna 1 till 6** redogör för ytterligare överväganden hänförliga till att skaffa sig en förståelse av företaget och dess miljö, det tillämpliga ramverket för finansiell rapportering och företagets system för intern kontroll.

Skaffa sig den nödvändiga förståelsen (se punkt 19–27)

A48. Att skaffa sig en förståelse av företaget och dess miljö, det tillämpliga ramverket för finansiell rapportering och företagets system för intern kontroll är en dynamisk och iterativ process med att samla in, uppdatera och analysera information och fortgår under hela revisionen. Därför kan revisorns förväntningar ändras vartefter ny information inhämtas.

A49. Revisorns förståelse av företaget och dess miljö och det tillämpliga ramverket för finansiell rapportering kan också hjälpa revisorn att utveckla initiala förväntningar på vilka transaktionsslag, konton och upplysningar som kan vara betydande transaktionsslag, konton och upplysningar. Dessa

förväntade betydande transaktionsslag, konton och upplysningar utgör basen för omfattningen av revisorns förståelse av företagets informationssystem.

Varför en förståelse av företaget och dess miljö samt det tillämpliga ramverket för finansiell rapportering är nödvändig (se punkt 19–20)

A50. Revisorns förståelse av företaget och dess miljö samt det tillämpliga ramverket för finansiell rapportering hjälper revisorn att förstå de händelser och omständigheter som är relevanta för företaget och att identifiera hur inneboende riskfaktorer påverkar känsligheten i påståenden för felaktigheter i enlighet med det tillämpliga ramverket för finansiell rapportering och i vilken grad de gör det. Sådan information bildar en referensram inom vilken revisorn identifierar och bedömer risker för väsentliga felaktigheter. Denna referensram hjälper också revisorn att planera revisionen och göra professionella bedömningar och visa prov på en professionellt skeptisk inställning under hela revisionen, t.ex. när revisorn

- identifierar och bedömer risker för väsentliga felaktigheter i de finansiella rapporterna enligt ISA 315 (omarbetad 2019) eller andra relevanta standarder (t.ex. avseende risk för oegentligheter i enlighet med ISA 240 eller när revisorn identifierar eller bedömer risker avseende uppskattningar i redovisningen enligt ISA 540 (omarbetad))
- utför åtgärder för att hjälpa till att identifiera fall av överträdelser av lagar och andra författningar som kan ha en betydande påverkan på de finansiella rapporterna enligt ISA 250[27]
- utvärderar huruvida de finansiella rapporterna innefattar adekvata upplysningar enligt ISA 700 (omarbetad)[28]
- fastställer väsentlighet eller arbetsväsentlighet enligt ISA 320[29], eller
- överväger hur ändamålsenligt valet och tillämpningen av redovisningsprinciper är, och hur väl avpassade upplysningarna i de finansiella rapporterna är.

A51. Revisorns förståelse av företaget och dess miljö samt det tillämpliga ramverket för finansiell rapportering ger också information för hur revisorn planerar och genomför fortsatta granskningsåtgärder, t.ex. när han eller hon

- utarbetar förväntningar inför den analytiska granskningen i enlighet med ISA 520[30]
- utformar och utför fortsatta granskningsåtgärder för att inhämta tillräckliga och ändamålsenliga revisionsbevis i enlighet med ISA 330, eller
- bedömer inhämtade revisionsbevis tillräcklighet och ändamålsenlighet (t.ex. avseende antaganden eller företagsledningens muntliga och skriftliga uttalanden).

---

27 ISA 250 (omarbetad) *Beaktande av lagar och andra författningar vid revision av finansiella rapporter*, punkt 14

28 ISA 700 (omarbetad), *Bilda sig en uppfattning och uttala sig om finansiella rapporter,* punkt 13(e)

29 ISA 320, *Väsentlighet vid planering och utförande av en revision*, punkterna 10–11

30 ISA 520, punkt 5

Skalbarhet

A52. Karaktären på och omfattningen av den nödvändiga förståelsen är en fråga för revisorns professionella omdöme och varierar från företag till företag baserat på företagets karaktär och omständigheter, däribland

- företagets storlek och komplexitet, däribland dess IT-miljö
- revisorns tidigare erfarenhet av företaget
- karaktären på företagets system och processer, inklusive huruvida de är formaliserade eller inte, och
- karaktären och formen på företagets dokumentation.

A53. Revisorns riskbedömning för att uppnå den nödvändiga förståelsen kan vara mindre omfattande i revisioner av mindre komplexa företag och mer omfattande för företag som är mer komplexa. Den förståelse som revisorn måste ha förväntas inte vara lika ingående som den som krävs av företagets ledning.

A54. Vissa ramverk för finansiell rapportering tillåter att mindre företag lämnar enklare och mindre detaljerade upplysningar i de finansiella rapporterna. Men det fråntar inte revisorn ansvaret för att skaffa sig en förståelse av företaget och dess miljö samt av det tillämpliga ramverket för finansiell rapportering så som det är tillämpligt på företaget.

A55. Företagets användning av IT samt karaktären på och omfattningen av förändringar i IT-miljön kan också påverka den specialkompetens som behövs för att hjälpa till att skaffa sig den nödvändiga förståelsen.

Företaget och dess miljö (se punkt 19(a))

Företagets organisationsstruktur, ägande och styrning samt affärsmodell (se punkt 19(a)(i))

Företagets organisationsstruktur och ägande

A56. En förståelse av företagets organisationsstruktur och ägande kan göra det möjligt för revisorn att förstå sådana frågor som

- komplexiteten i företagets struktur

> **Exempel**:
>
> Företaget kan vara ett enskilt företag eller också kan företagets struktur innefatta dotterföretag, divisioner eller andra enheter på flera olika platser. Vidare kan den juridiska strukturen skilja sig från verksamhetsstrukturen. Komplexa strukturer innebär ofta att det finns faktorer som kan ge upphov till en ökad känslighet för risker för väsentliga felaktigheter. Sådana förhållanden kan handla om huruvida goodwill, samriskföretag, investeringar eller företag för särskilda ändamål redovisas korrekt och huruvida tillräckliga upplysningar om sådana förhållanden har lämnats i de finansiella rapporterna.

- ägandet och relationer mellan ägare och andra personer eller företag, däribland närstående. Förståelse av detta kan hjälpa revisorn att avgöra om transaktioner med närstående har identifierats korrekt samt redovisats och beskrivits på ett riktigt sätt i de finansiella rapporterna[31]
- skillnaden mellan ägare, styrelse och företagsledning

  Exempel:

  I mindre komplexa företag kan företagets ägare vara engagerade i att leda verksamheten, och därmed finns det ingen eller liten distinktion. I motsats till det kan det, som är fallet i vissa börsnoterade företag, finnas en tydlig distinktion mellan ledningen, företagets ägare och styrelsen.[32]

- strukturen på och komplexiteten i företagets IT-miljö

  Exempel:

  Ett företag kan

  - ha ett flertal äldre IT-system i ett flertal olika verksamheter som inte är väl integrerade, vilket ger en komplex IT-miljö,
  - använda externa eller interna tjänsteleverantörer för vissa aspekter av sin IT-miljö (t.ex. outsourca sin IT-miljö till en tredje part eller använda ett gemensamt servicecenter för central hantering av IT-processer i en koncern).

Automatiserade verktyg och tekniker

A57. Revisorn kan använda automatiserade verktyg och tekniker för att förstå transaktionsflöden och bearbetning som en del av revisorns åtgärder för att förstå informationssystemet. Ett resultat av dessa åtgärder kan vara att revisorn erhåller information om företagets organisationsstruktur eller om dem som företaget gör affärer med (t.ex. leverantörer, kunder, närstående).

Överväganden som särskilt gäller företag inom den offentliga sektorn

A58. Ägandet i ett företag inom den offentliga sektorn kanske inte har samma betydelse som i den privata sektorn, eftersom beslut hänförliga till företaget kan fattas utanför företaget som ett resultat av politiska processer. Därför kanske inte företagsledningen har kontroll över vissa beslut som fattas. Frågor som kan vara relevanta omfattar att förstå företagets förmåga att fatta ensidiga beslut samt förmågan hos andra företag inom den offentliga sektorn att kontrollera eller påverka företagets mandat och strategiska inriktning.

Exempel:

[31] ISA 550 fastställer krav och ger vägledning om revisorns överväganden avseende närståendeförhållanden.

[32] ISA 260 (omarbetad), punkterna A1 och A2, ger vägledning till identifieringen av styrelsen och förklarar att i vissa fall kan hela eller delar av styrelsen vara engagerad i att leda företaget.

Ett företag inom den offentliga sektorn kan lyda under lagar eller direktiv från myndigheterna som kräver att företaget erhåller godkännande från parter utanför företaget för sin strategi eller sina mål innan dessa införs. Därför kan frågor hänförliga till att förstå företagets juridiska struktur omfatta tillämpliga lagar och andra författningar samt klassificeringen av företaget (dvs. huruvida företaget är ett ministerium, departement, myndighet eller annan typ av enhet).

Styrning

Varför revisorn skaffar sig en förståelse av styrningen

A59. Att förstå hur företaget styrs kan hjälpa revisorn med förståelsen av företagets förmåga att tillhandahålla en lämplig tillsyn över sitt system för intern kontroll. Men den här förståelsen kan också erbjuda bevis på brister, vilket kan tyda på en ökad känslighet för väsentliga felaktigheter i företagets finansiella rapporter.

Förstå företagets styrning

A60. Frågor som kan vara relevanta för revisorn att beakta när han eller hon skaffar sig en förståelse av styrningen av företaget omfattar

- huruvida någon eller alla i styrelsen är engagerad i att leda företaget
- om styrelsen är extern och i vilken utsträckning den är åtskild från företagsledningen
- huruvida personerna i styrelsen innehar positioner som är en integrerad del av företagets juridiska struktur, t.ex. som styrelseledamöter
- förekomsten av utskott i styrelsen, som ett revisionsutskott, samt ett sådant utskotts ansvarsområden
- styrelsens ansvar för tillsynen av den finansiella rapporteringen, däribland att godkänna de finansiella rapporterna.

Företagets affärsmodell

Bilaga 1 anger ytterligare frågor att beakta för att skaffa sig en förståelse av företaget och dess affärsmodell, samt ytterligare frågor att beakta vid revisionen av företag för särskilda ändamål.

Varför revisorn skaffar sig en förståelse av företagets affärsmodell

A61. Att förstå företagets mål, strategi och affärsmodell hjälper revisorn att förstå företaget på strategisk nivå samt förstå de affärsrisker som företaget tar och står inför. Förståelse av de affärsrisker som påverkar de finansiella rapporterna hjälper revisorn att identifiera risker för väsentliga felaktigheter, eftersom de flesta affärsrisker på sikt även får ekonomiska konsekvenser och således påverkar de finansiella rapporterna.

Exempel:

Ett företags affärsmodell kan vara beroende av användning av IT på olika sätt:

- Företaget säljer skor från en fysisk butik och använder ett avancerat system för lager och försäljning för att redovisa skoförsäljningen, eller
- Företaget säljer skor online så att all försäljning bearbetas i en IT-miljö, inklusive initieringen av transaktionerna genom en webbplats.

För båda dessa företag skulle de affärsrisker som uppkommer från helt olika affärsmodeller skilja sig väsentligt åt, trots att båda företagen säljer skor.

Förstå företagets affärsmodell

A62. Det är inte alla aspekter av affärsmodellen som är relevanta för revisorns förståelse. Affärsrisker är ett vidare begrepp än risken för väsentliga felaktigheter i de finansiella rapporterna, även om affärsriskerna omfattar det senare. Revisorn har inte ansvar för att förstå eller identifiera alla affärsrisker, eftersom inte alla affärsrisker ger upphov till risker för väsentliga felaktigheter.

A63. Affärsrisker som ökar känsligheten för väsentliga felaktigheter kan uppkomma genom följande:

- Olämpliga mål eller strategier, ineffektivt genomförande av strategier, eller förändring eller komplexitet.
- En affärsrisk kan också uppstå om man inte inser behovet av förändringar, till exempel till följd av:
  - Misslyckad utveckling av nya varor eller tjänster.
  - En marknad som inte är stor nog för en vara eller tjänst, även om introduktionen går bra.
  - Brister i en vara eller tjänst, vilket kan medföra risk för rättsligt ansvar och påverka företagets rykte.
- Incitament till och påtryckningar på företagsledningen, vilket kan leda till avsiktlig eller oavsiktlig partiskhet från ledningens sida, och därmed påverka rimligheten i väsentliga antaganden och ledningens eller styrelsens förväntningar.

A64. Exempel på förhållanden som revisorn kan beakta när han eller hon skaffar sig en förståelse av företagets affärsmodell, mål, strategier och affärsrisker som sammanhänger med dessa, som kan medföra en risk för väsentliga felaktigheter i de finansiella rapporterna:

- Branschutvecklingen, såsom brist på personal eller sakkunskap som krävs för att hantera förändringarna i branschen.
- Nya produkter och tjänster som kan leda till ökat produktansvar.
- Expansion av företagets verksamhet och att efterfrågan inte har bedömts korrekt.
- Nya redovisningskrav som har införts ofullständigt eller felaktigt.
- Regleringar som leder till ökad rättslig exponering.

- Aktuella eller kommande finansieringskrav, så som att företaget går miste om finansiering på grund av att det inte kan uppfylla kraven.
- Användning av IT, så som införandet av ett nytt IT-system som påverkar både verksamheten och den finansiella rapporteringen, eller
- Effekterna av införandet av en strategi, framför allt sådana effekter som medför nya redovisningskrav.

A65. Vanligtvis identifierar företagsledningen affärsriskerna och utarbetar metoder för att hantera dem. En sådan riskbedömning är en del av företagets system för intern kontroll och diskuteras i punkt 22, och punkterna A109–A113.

Överväganden som särskilt gäller företag inom den offentliga sektorn

A66. Företag som bedriver verksamhet i den offentliga sektorn kan skapa och leverera värde på andra sätt än de som genererar rikedom till sina ägare, men har ändå en ”affärsmodell” med ett särskilt syfte. Frågor som revisorer inom den offentliga sektorn kan skaffa sig en förståelse av som är relevanta för företagets affärsmodell omfattar

- kunskap om relevanta statliga aktiviteter, inklusive relaterade program
- programmål och strategier, inklusive element för allmän politik.

A67. Vid revisioner av företag inom den offentliga sektorn kan ”företagsledningens mål” påverkas av krav på offentlig redovisningsskyldighet och kan innehålla mål som har sitt ursprung i lagar eller andra författningar.

Branschspecifika faktorer, regelverk och andra externa faktorer (se punkt 19(a)(ii))

Branschspecifika faktorer

A68. Bland de branschspecifika faktorerna finns konkurrenssituation, leverantörs- och kundrelationer samt teknisk utveckling. Frågor som revisorn kan beakta omfattar:

- marknaden och konkurrensen, däribland efterfrågan, kapacitet och priskonkurrens
- cyklisk eller säsongsmässig verksamhet
- produktteknik hänförligt till företagets produkter
- energiförsörjning och energikostnader.

A69. I den bransch där företaget verkar kan det finnas särskilda risker för väsentliga felaktigheter på grund av verksamhetens karaktär eller graden av reglering.

Exempel:

I byggbranschen kan långvariga kontrakt inbegripa betydande uppskattningar av intäkter och kostnader som ger upphov till risker för väsentliga felaktigheter. I sådana fall är det viktigt att i uppdragsteamet ingår medlemmar som har tillräcklig och relevant kunskap och erfarenhet.[33]

Regelverk

A70. Den rättsliga miljön ingår i de relevanta regulatoriska faktorerna. Den rättsliga miljön består bland annat av det tillämpliga ramverket för finansiell rapportering samt den rättsliga och politiska miljön och eventuella förändringar av dessa. Frågor som revisorn kan beakta omfattar

- det ramverk av lagar och andra författningar som gäller för en reglerad bransch, t.ex. principer för försiktighet, däribland tillhörande upplysningar
- lagar och andra författningar som har betydande påverkan på företagets verksamhet, t.ex. arbetslagar och förordningar
- skattelagstiftning och förordningar
- regeringspolitik som i dagsläget påverkar hur företaget bedriver sin verksamhet, t.ex. penningpolitik, däribland valutakontroller, finanspolitik, ekonomiska bidrag (t.ex. statliga stödprogram) och tullar eller handelshinder
- miljökrav som påverkar branschen och företagets verksamhet.

A71. ISA 250 (omarbetad) innehåller vissa specifika krav som rör det tillämpliga ramverket av lagar och andra författningar för företaget och den bransch eller sektor som företaget bedriver verksamhet i.[34]

Överväganden som särskilt gäller företag inom den offentliga sektorn

A72. Vid revisioner av företag i den offentliga sektorn kan det finnas särskilda lagar eller regler som påverkar företagets verksamhet. Sådana faktorer kan vara ett viktigt övervägande när man bildar sig en uppfattning om företaget och dess miljö.

Övriga externa faktorer

A73. Övriga externa faktorer som påverkar företaget och som revisorn kan beakta är konjunkturen, räntenivåer och tillgången på finansiering, inflation och valutaförändringar.

Företagsledningens mått för att bedöma företagets finansiella ställning (se punkt 19(a)(iii))

Varför revisorn ska förstå de mått som företagsledningen använder

A74. En förståelse av företagets mätetal hjälper revisorn att beakta huruvida sådana mått, vare sig de används externt eller internt, skapar tryck på företaget att uppnå sina prestationsmål. Detta tryck kan i sin tur motivera företagsledningen att vidta åtgärder som ökar känsligheten för felaktigheter till följd

[33] ISA 220, punkt 14

[34] ISA 250 (omarbetad), punkt 13

av att företagsledningen är partisk eller gör sig skyldig till oegentligheter (t.ex. att förbättra företagets resultat eller att avsiktligt felaktigt upprätta de finansiella rapporterna) (se ISA 240 för krav och riktlinjer i samband med risken för oegentligheter).

A75. Måtten kan också indikera för revisorn sannolikheten för risker för väsentliga felaktigheter i näraliggande information i de finansiella rapporterna. Prestationsmått kan t.ex. visa att företaget har en ovanligt snabb tillväxt eller lönsamhet jämfört med andra företag inom samma bransch.

Mått som används av ledningen

A76. Företagsledningen och andra personer mäter vanligtvis och går igenom saker som de anser är viktiga. Frågor till företagsledningen kan visa att denna förlitar sig på vissa nyckeltal, vare sig dessa är offentliga eller inte, för att utvärdera det finansiella utfallet och vidta åtgärder. I sådana fall kan revisorn identifiera relevanta resultatmål, vare sig de är interna eller externa, genom att bedöma den information som företaget använder för att driva verksamheten. Om det av dessa frågor framgår att det inte finns något resultatmått eller någon genomgång kan det finnas ökad risk för att felaktigheter inte upptäcks och rättas till.

A77. Nyckeltal som används för att utvärdera den finansiella prestationen kan omfatta

- olika mått (ekonomiska och icke ekonomiska) och nyckeltal, trender och statistik om verksamheten
- jämförande analyser av ekonomiskt utfall för olika räkenskapsperioder
- budgetar, prognoser, analyser av budgetavvikelser, information om segment och resultatrapporter från divisioner, avdelningar eller andra nivåer
- prestationsmått för medarbetarna och riktlinjer för incitamentsersättning
- jämförelser av ett företags utfall med konkurrenternas.

Skalbarhet (se punkt 19(a)(iii))

A78. De åtgärder som vidtas för att förstå företagets mått kan variera beroende på företagets storlek eller komplexitet, samt ägarnas eller styrelsens engagemang i ledningen av företaget.

Exempel:

- För vissa mindre komplexa företag kan villkoren för företagets banklån (dvs. bankens villkor) vara kopplade till särskilda prestationsmål hänförliga till företagets resultat eller finansiella ställning (t.ex. ett maxbelopp för rörelsekapital). Revisorns förståelse av de resultatmått som används av banken kan hjälpa till att identifiera områden där det finns en ökad känslighet i risken för väsentliga felaktigheter.
- För vissa företag vilkas karaktär och omständigheter är mer komplexa, så som de företag som bedriver verksamhet inom försäkringsbranschen eller bankbranschen, kan resultat eller finansiell ställning mätas mot krav enligt lagar och andra författningar (t.ex. myndighetskrav som kapitaltäckning och likviditetskrav). Revisorns förståelse av dessa prestationsmått kan

hjälpa till att identifiera områden där det finns en ökad känslighet i risken för väsentliga felaktigheter.

Övriga överväganden

A79. Externa parter kan också granska och analysera företagets finansiella utveckling, i synnerhet för företag där den finansiella informationen är offentlig. Revisorn kan också beakta offentlig information för att få hjälp att förstå verksamheten eller att identifiera motsägelsefull information såsom information från

- analytiker eller kreditinstitut
- nyheter eller andra medier, däribland sociala medier
- skattemyndigheter
- tillsynsmyndigheter
- fackföreningar
- finansiärer.

Sådan finansiell information kan ofta hämtas från det företag som revideras.

A80. Att mäta och gå igenom det ekonomiska utfallet är inte detsamma som att övervaka systemet för intern kontroll (vilket diskuteras som en komponent i systemet för intern kontroll i punkterna A114–A122), även om syftena överlappar varandra:

- Syftet med att mäta och gå igenom resultatet är att fastställa om företagets resultat uppfyller de mål som företagsledningen (eller externa parter) har satt upp.
- I motsats till det handlar övervakning av systemet för intern kontroll om att övervaka kontrollernas funktion, inklusive dem som avser ledningens mätning och genomgång av finansiella resultat.

I vissa fall ger resultatmåtten emellertid information som företagsledningen kan använda för att identifiera brister i kontrollen.

Överväganden som särskilt gäller företag inom den offentliga sektorn

A81. Utöver att beakta de relevanta mått som används av ett företag inom den offentliga sektorn för att bedöma företagets finansiella prestation kan revisorer i företag i den offentliga sektorn beakta icke-finansiell information såsom hur företaget uppnår resultat för allmännyttiga ändamål (t.ex. antalet personer som får hjälp av ett visst program).

Det tillämpliga ramverket för finansiell rapportering (se punkt 19(b))

Förstå det tillämpliga ramverket för finansiell rapportering och företagets redovisningsprinciper

A82. Frågor som revisorn kan beakta när han eller hon skaffar sig en förståelse av företagets tillämpliga ramverk för den finansiella rapporteringen och hur det tillämpas med hänsyn till företagets karaktär och omständigheter samt dess miljö omfattar följande:

- Företagets metoder för finansiell rapportering i enlighet med tillämpligt ramverk för finansiell rapportering, så som
    - redovisningsprinciper och branschpraxis, däribland branschspecifika betydelsefulla transaktionsslag, konton och tillhörande upplysningar i de finansiella rapporterna (t.ex. lån och investeringar för banker eller forskning och utveckling för läkemedelsföretag)
    - intäktsredovisning
    - redovisning av finansiella instrument, inklusive relaterade kreditförluster
    - tillgångar, skulder och transaktioner i utländsk valuta
    - redovisning av ovanliga eller komplicerade transaktioner, däribland transaktioner inom kontroversiella eller framväxande områden (t.ex. redovisning av kryptovalutor).
- En förståelse av företagets val och tillämpning av redovisningsprinciper, inklusive eventuella ändringar av dessa samt anledningarna till sådana, kan innefatta frågor som
    - vilka metoder företaget använder för att redovisa, mäta, presentera och lämna information om betydande och ovanliga transaktioner
    - effekten av betydelsefulla redovisningsprinciper inom kontroversiella eller framväxande områden där det saknas auktoritativ vägledning eller konsensus
    - förändringar i miljön, t.ex. förändringar i det tillämpliga ramverket för finansiell rapportering eller skattereformer som kan göra det nödvändigt med en förändring av företagets redovisningsprinciper
    - standarder, lagar och andra författningar för finansiell rapportering som är nya för företaget samt när och hur företaget kommer att börja tillämpa eller följa sådana krav.

A83. Att skaffa sig en förståelse av företaget och dess miljö kan hjälpa revisorn att bedöma var förändringar i företagets finansiella rapportering (t.ex. från tidigare perioder) kan förväntas.

> **Exempel**:
>
> Om företaget till exempel har gjort ett betydande rörelseförvärv under perioden skulle revisorn sannolikt förvänta sig förändringar i transaktionsslag, konton och upplysningar på grund av detta rörelseförvärv. Om det däremot inte har skett några väsentliga förändringar i ramverket för den finansiella rapporteringen under perioden förblir den förståelse revisorn har skaffat sig under tidigare perioder tillämplig.

Överväganden som särskilt gäller företag inom den offentliga sektorn

A84. Det tillämpliga ramverket för finansiell rapportering i ett företag inom den offentliga sektorn bestäms av det tillämpliga ramverket av lagar och andra författningar som är relevant för respektive jurisdiktion eller inom respektive geografiskt område. Frågor som kan beaktas vid företagets tillämpning av kraven på den finansiella rapporteringen, och hur detta gäller med hänsyn till företagets karaktär och miljö, omfattar huruvida företaget tillämpar fullständiga bokföringsmässiga grunder eller

kontantmetoden för bokföring enligt International Public Sector Accounting Standards, eller en kombination av dessa.

Hur inneboende riskfaktorer påverkar hur känsliga påståenden är för felaktigheter (se punkt 19(c))

> **Bilaga 2** innehåller exempel på händelser och förhållanden som kan ge upphov till risk för väsentliga felaktigheter, kategoriserade efter inneboende riskfaktor.

Varför revisorn förstår de inneboende riskfaktorerna när han eller hon förstår företaget och dess miljö samt det tillämpliga ramverket för finansiell rapportering

A85. Att förstå företaget och dess miljö samt det tillämpliga ramverket för finansiell rapportering hjälper revisorn att identifiera händelser eller omständigheter, vilkas egenskaper kan påverka hur känsliga påståenden om transaktionsslag, konton eller upplysningar är för felaktigheter. Dessa egenskaper utgör inneboende riskfaktorer. Inneboende riskfaktorer kan påverka hur känsliga påståenden är för felaktigheter genom att påverka hur sannolikt det är att felaktigheterna uppkommer eller felaktigheternas storlek om de skulle uppkomma. Att förstå hur inneboende riskfaktorer påverkar hur känsliga påståenden är för felaktigheter kan hjälpa revisorn med en preliminär förståelse av sannolikheten för att felaktigheterna uppkommer eller hur omfattande de kan vara, vilket hjälper revisorn att identifiera riskerna för väsentliga felaktigheter på påståendenivån enligt punkt 28(b). Att förstå i vilken grad inneboende riskfaktorer påverkar hur känsliga påståenden är för felaktigheter hjälper också revisorn att bedöma sannolikheten för och omfattningen av möjliga felaktigheter när han eller hon bedömer inneboende risker enligt punkt 31(a). Följaktligen kan en förståelse av de inneboende riskfaktorerna hjälpa revisorn att utforma och utföra fortsatta granskningsåtgärder i enlighet med ISA 330.

A86. Revisorns identifiering av risker för väsentliga felaktigheter på påståendenivån och bedömning av inneboende risker kan också påverkas av revisionsbevis som inhämtas av revisorn när han eller hon utför andra riskbedömningar, fortsatta granskningsåtgärder eller uppfyller andra krav i standarderna (se punkterna A95, A103, A111, A121, A124 och A151).

Påverkan från inneboende riskfaktorer på ett transaktionsslag, ett konto eller en upplysning

A87. Hur stor känsligheten för felaktigheter är för ett transaktionsslag, ett konto eller en upplysning som uppkommer genom komplexitet eller subjektivitet har ofta en nära koppling till i vilken omfattning de är föremål för förändring eller osäkerhet.

> **Exempel**:
>
> Om ett företag har en uppskattning i redovisningen som bygger på antaganden för vilka urvalet är föremål för väsentliga subjektiva bedömningar påverkas värderingen av uppskattningen i redovisningen sannolikt av både subjektivitet och osäkerhet.

A88. I ju högre grad ett transaktionsslag, ett konto eller en upplysning är känsliga för felaktigheter beroende på komplexitet eller subjektivitet, desto större är behovet av att revisorn har en professionellt skeptisk inställning. Dessutom, när ett transaktionsslag, ett konto eller en upplysning

är känsliga för felaktigheter beroende på komplexitet eller subjektivitet kan dessa inneboende riskfaktorer skapa utrymme för att företagsledningen är partisk, vare sig det är avsiktligt eller oavsiktligt, och påverka känsligheten för felaktigheter till följd av företagsledningens bristande objektivitet. Revisorns identifiering av risker för väsentliga felaktigheter och bedömning av inneboende riskfaktorer på påståendenivån påverkas också av inbördes samband mellan de inneboende riskfaktorerna.

A89. Händelser eller omständigheter som kan påverka känsligheten för felaktigheter till följd av företagsledningens bristande objektivitet kan också påverka känsligheten för felaktigheter till följd av andra riskfaktorer avseende oegentligheter. Följaktligen kan detta utgöra relevant information för användning enligt punkt 24 i ISA 240, som kräver att revisorn utvärderar om informationen som har inhämtats från de övriga riskbedömningsprocesserna och relaterade aktiviteter tyder på att det finns en eller flera riskfaktorer för oegentligheter.

Skaffa sig en förståelse för företagets system för intern kontroll (se punkt 21–27)

> **Bilaga 3** beskriver ytterligare karaktären på företagets system för intern kontroll och inneboende begränsningar i den interna kontrollen. I bilaga 3 förklaras också delarna i ett system för intern kontroll såsom begreppen används i standarderna.

A90. Revisorns förståelse av företagets system för intern kontroll inhämtas genom riskbedömning som genomförs för att förstå och utvärdera var och en av komponenterna i systemet för intern kontroll enligt vad som anges i punkterna 21 till 27.

A91. Komponenterna i företagets system för intern kontroll enligt denna standard avspeglar inte nödvändigtvis hur ett företag utformar, inför och upprätthåller sitt system för intern kontroll eller hur det klassificerar en viss komponent. Företagen kan använda en annan terminologi eller andra ramverk för att beskriva de olika aspekterna på systemet för intern kontroll. I en revision kan revisorerna också använda en annan terminologi eller andra ramverk förutsatt att alla komponenter som beskrivs i denna ISA behandlas.

Skalbarhet

A92. Det sätt på vilket företagets system för intern kontroll utformas, införs och upprätthålls beror på företagets storlek och komplexitet. Till exempel kan mindre komplexa företag använda mindre strukturerade eller enklare kontroller (t.ex. riktlinjer och rutiner) för att nå sina mål.

Överväganden som särskilt gäller företag inom den offentliga sektorn

A93. Revisorer i företag i den offentliga sektorn har ofta längre gående ansvarsområden när det gäller intern kontroll, t.ex. att rapportera om särskilda regler följs eller att rapportera om utgifter i förhållande till budget. Revisorer i företag i den offentliga sektorn kan också ha ansvar för att rapportera att lagar och andra författningar följs. Deras överväganden när det gäller den interna kontrollen kan därför vara mer omfattande och detaljerade.

Informationsteknik i komponenterna i företagets system för intern kontroll

> **Bilaga 5** ger ytterligare vägledning för att förstå informationsteknikens roll i komponenterna i systemet för intern kontroll.

A94. Det gör ingen skillnad för en revisions övergripande mål och omfattning om ett företag bedriver verksamhet i en helt manuell miljö, en helt automatiserad miljö eller en miljö som omfattar en kombination av manuella och automatiserade element (dvs. manuella och automatiserade kontroller och andra resurser som används i företagets system för intern kontroll).

Förstå komponenterna i företagets system för intern kontroll

A95. När revisorn utvärderar ändamålsenligheten i kontrollernas utformning och huruvida de har införts (se punkterna A175 till A181) ger revisorns förståelse av var och en av komponenterna i företagets system för intern kontroll en preliminär förståelse av hur företaget identifierar affärsrisker och hur företaget hanterar dem. Utvärderingen kan också påverka revisorns identifiering och bedömning av riskerna för väsentliga felaktigheter på olika sätt (se punkt A86). Detta hjälper revisorn att utforma och vidta fortsatta granskningsåtgärder, inklusive planer för att testa kontrollernas funktion. Exempel:

- Det är mer sannolikt att revisorns förståelse av företagets kontrollmiljö, företagets riskbedömning och företagets process för att övervaka kontrollkomponenterna påverkar identifieringen och bedömningen av risker för väsentliga felaktigheter på rapportnivån.
- Det är mer sannolikt att revisorns förståelse av företagets informationssystem och kommunikation samt företagets kontrollaktivitetskomponent påverkar identifieringen och bedömningen av risker för väsentliga felaktigheter på påståendenivån.

Kontrollmiljön, företagets riskbedömningsprocess och företagets process för att övervaka systemet för intern kontroll (se punkt 21–24)

A96. Kontrollerna i kontrollmiljön, företagets riskbedömningsprocess och företagets process för att övervaka systemet för intern kontroll är i första hand indirekta kontroller (dvs. kontroller som inte är tillräckligt precisa för att förhindra, upptäcka och rätta till felaktigheter på påståendenivån men som stöder andra kontroller och därför kan ha en indirekt påverkan på sannolikheten för att en felaktighet upptäcks eller förhindras i rätt tid). Men vissa kontroller inom dessa komponenter kan också vara direkta kontroller.

Varför revisorn måste förstå kontrollmiljön, företagets riskbedömningsprocess och företagets process för att övervaka systemet för intern kontroll

A97. Kontrollmiljön är ett fundament för hur de andra komponenterna i systemet för intern kontroll fungerar. Kontrollmiljön kan inte direkt förhindra, eller upptäcka och rätta till, felaktigheter. Däremot kan den påverka kontrollernas funktion i de andra komponenterna i systemet för intern kontroll. På liknande

sätt är företagets riskbedömning och dess process för att övervaka systemet för intern kontroll utformade för att också stödja hela systemet för intern kontroll.

A98. Eftersom de här komponenterna är grundläggande för företagets system för intern kontroll skulle eventuella brister i deras funktion kunna ha en avgörande påverkan på upprättandet av de finansiella rapporterna. Därför påverkar revisorns förståelse och utvärderingar av dessa komponenter hans eller hennes identifiering och bedömning av riskerna för väsentliga felaktigheter på rapportnivån, och kan också påverka identifieringen och bedömningen av riskerna för väsentliga felaktigheter på påståendenivån. Risker för väsentliga felaktigheter på rapportnivån påverkar revisorns utformning av övergripande åtgärder, däribland, enligt vad som förklaras i ISA 330, påverkan på karaktär, tidpunkter och omfattning av revisorns fortsatta granskningsåtgärder.[35]

Skaffa en förståelse av kontrollmiljön (se punkt 21)

Skalbarhet

A99. Karaktären på kontrollmiljön i ett mindre komplext företag skiljer sig sannolikt från kontrollmiljön i ett mer komplext företag. I mindre komplexa företag kanske styrelsen inte har någon oberoende eller extern ledamot, och bolagsstyrningen kan handhas direkt av ägaren-företagsledaren om det inte finns några andra ägare. Följaktligen kan vissa överväganden gällande företagets kontrollmiljö vara mindre relevanta eller kanske inte alls är tillämpliga.

A100. Det kan också förekomma det inte finns skriftliga revisionsbevis för delar av kontrollmiljön i mindre komplexa företag, särskilt i de fall då kommunikationen mellan företagsledningen och annan personal är informell, men bevisen kan fortfarande vara tillräckligt relevanta och tillförlitliga under omständigheterna.

Exempel:

- Organisationsstrukturen i ett mindre komplext företag är sannolikt enklare och kan omfatta ett litet antal anställda med befattningar hänförliga till den finansiella rapporteringen.
- Om bolagsstyrningen hanteras direkt av ägaren-företagsledaren kan revisorn fastställa att oberoendet för styrelsen inte är relevant.
- I mindre företag kan en skriftlig uppförandekod saknas men dessa företag kan i stället ha utvecklat en kultur som betonar vikten av hederlighet och etiskt agerande genom muntlig kommunikation och genom att företagsledningen har föregått med gott exempel. Företagsledningens eller ägaren-företagsledarens inställning, medvetenhet och handlingar är därför särskilt viktiga för revisorns förståelse av ett mindre komplext företags kontrollmiljö.

Förstå kontrollmiljön (se punkt 21(a))

A101. Revisionsbevis för revisorns förståelse av kontrollmiljön kan inhämtas genom en kombination av frågor och annat riskbedömningsarbete, t.ex. att svar bekräftas genom observation eller inspektion av dokument.

[35] ISA 330, punkterna A1–A3

A102. När revisorn bedömer i vilken mån ledningen betonar vikten av hederlighet och etiska värderingar kan han eller hon bilda sig en uppfattning genom frågor till ledningen och de anställda samt genom att beakta information från externa källor om

- hur företagsledningen kommunicerar sin syn på affärssed och etiskt agerande till de anställda, och
- inspektioner av ledningens skriftliga uppförandekod och observation av huruvida ledningen agerar på ett sätt som stödjer den koden.

Utvärdera kontrollmiljön (se punkt 21(b))

Varför revisorn utvärderar kontrollmiljön

A103. Revisorns utvärdering av hur företaget uppvisar ett beteende som är i enlighet med företagets mål att ha en kultur av hederlighet och etiska värderingar; huruvida kontrollmiljön erbjuder en ändamålsenlig grund för de andra komponenterna i företagets system för intern kontroll och huruvida några identifierade brister i kontrollerna undergräver de andra komponenterna i systemet för intern kontroll, hjälper revisorn att identifiera möjliga problem i de andra komponenterna i systemet för intern kontroll. Det beror på att kontrollmiljön är grundläggande för de andra komponenterna i företagets system för intern kontroll. Denna utvärdering kan också hjälpa revisorn att förstå de risker som företaget står inför och därmed att identifiera och bedöma risken för väsentliga felaktigheter på rapport- och påståendenivån (se punkt A86).

Revisorns utvärdering av kontrollmiljön

A104. Revisorns utvärdering av kontrollmiljön grundar sig på förståelsen som har inhämtats enligt punkt 21(a).

A105. Vissa företag kan domineras av en person som kan utöva ett stort mått av självbestämmande. En sådan persons handlingar och attityder kan genomsyra företagets kultur, vilket i sin tur kan få en avgörande påverkan på kontrollmiljön. En sådan påverkan vara positiv eller negativ.

> **Exempel**:
>
> En enskild persons direkta engagemang kan vara nyckeln till att företaget uppnår sina tillväxtmål och andra mål och kan också bidra väsentligt till ett effektivt system för intern kontroll. Å andra sidan kan en sådan koncentration av kunskap och auktoritet leda till en ökad känslighet för felaktigheter genom att ledningen sätter sig över kontrollerna.

A106. Revisorn kan överväga hur de olika delarna i kontrollmiljön kan påverkas av högsta ledningens filosofi och ledningsmetoder genom att beakta engagemanget från oberoende styrelseledamöter.

A107. Även om kontrollmiljön kan erbjuda en ändamålsenlig grund för systemet för intern kontroll och kan hjälpa till att minska risken för oegentligheter är en ändamålsenlig kontrollmiljö inte nödvändigtvis ett effektivt sätt för att förhindra oegentligheter.

Exempel:

Personalpolitik och personalrutiner när det gäller att anställa kompetent personal inom ekonomi, redovisning och IT kan minska risken för misstag vid bearbetning och redovisning av finansiell information. Men sådan personalpolitik och sådana personalrutiner kanske inte minskar risken att högsta ledningen sätter sig över kontrollerna (t.ex. för att överdriva intäkterna).

A108. Revisorns utvärdering av kontrollmiljön till den del den är hänförlig till företagets IT-användning kan omfatta följande frågor:

- Huruvida styrningen av IT står i proportion till företagets karaktär och komplexitet och den affärsverksamhet som möjliggörs av IT, inklusive komplexiteten och mognaden hos företagets teknikplattform eller arkitektur och i vilken grad företaget förlitar sig på IT-applikationer för att stödja sin finansiella rapportering.
- Ledningens organisationsstruktur avseende IT och de resurser som har tillförts (t.ex. om företaget har investerat i en lämplig IT-miljö och nödvändiga förbättringar, eller om ett tillräckligt antal kompetenta personer har anställts även när företaget använder kommersiell mjukvara (utan ändringar eller med begränsade ändringar)).

Skaffa sig en förståelse av företagets riskbedömningsprocess (se punkt 22–23)

Förstå företagets riskbedömningsprocess (se punkt 22(a))

A109. Såsom det förklaras i punkt A62 ger inte alla affärsrisker upphov till risker för väsentliga fel. När revisorn skaffar sig en förståelse av hur ledningen och styrelsen har identifierat affärsrisker relevanta för upprättandet av de finansiella rapporterna, och fattat beslut om åtgärder för att hantera de riskerna, kan frågor som revisorn kan överväga omfatta hur ledningen, eller i förekommande fall, styrelsen, har

- specificerat företagets mål med tillräcklig precision och tydlighet för att möjliggöra identifieringen och bedömningen av riskerna hänförliga till målen
- identifierat riskerna med att uppnå målen och analyserat dessa risker som en bas för att fastställa hur riskerna ska hanteras, och
- övervägt möjligheterna till oegentligheter när han eller hon övervägde riskerna för att inte uppnå företagets mål.[36]

A110. Revisorn kan överväga vilken betydelse sådana affärsrisker kan få för upprättandet av företagets finansiella rapporter och andra aspekter av dess system för intern kontroll.

Utvärdera företagets riskbedömning (se punkt 22(b))

Varför revisorn utvärderar huruvida företagets riskbedömning är ändamålsenlig

A111. Revisorns utvärdering av företagets riskbedömning kan hjälpa revisorn att förstå var företaget har identifierat risker som kan uppkomma, och hur företaget har svarat på de riskerna. Revisorns

[36] ISA 240, punkt 19

utvärdering av hur företaget identifierar sina affärsrisker, och hur företaget bedömer och hanterar de riskerna hjälper revisorn att förstå huruvida de risker företaget står inför har identifierats, bedömts och hanterats på lämpligt sätt med avseende på företagets karaktär och komplexitet. Denna utvärdering kan också hjälpa revisorn att identifiera och bedöma riskerna för väsentliga felaktigheter på rapport- och påståendenivån (se punkt A86).

Utvärdera huruvida företagets riskbedömningsprocess är ändamålsenlig (se punkt 22(b))

A112. Revisorns utvärdering av lämpligheten i företagets riskbedömning grundar sig på förståelsen som har inhämtats enligt punkt 22(a).

Skalbarhet

A113. Huruvida företagets riskbedömning är anpassad till företagets omständigheter med beaktande av företagets karaktär och komplexitet är en fråga för revisorns professionella bedömning.

> **Exempel**:
>
> I vissa mindre komplexa företag, och i synnerhet ägarledda företag, kan en lämplig riskbedömning utföras genom ett direkt engagemang från ledningen eller ägaren-företagsledaren (t.ex. kan företagsledaren eller ägaren-företagsledaren rutinmässigt avsätta tid till att övervaka konkurrenternas aktiviteter och annan utveckling på marknaden för att identifiera framväxande affärsrisker). Bevisen på denna riskbedömning som förekommer i sådana företag är ofta inte formellt dokumenterade, men det kan framgå av diskussioner som revisorn har med ledningen att ledningen de facto genomför riskbedömningsprocesser.

Skaffa sig en förståelse av företagets process för att övervaka företagets system för intern kontroll (se punkt 24)

Skalbarhet

A114. I mindre komplexa företag, och särskilt ägarledda företag, har revisorns förståelse av företagets process för att övervaka systemet för intern kontroll ofta fokus på hur ledningen eller ägaren-företagsledaren är direkt engagerad i verksamheten, eftersom det kanske inte finns någon annan övervakning.

> **Exempel**:
>
> Ledningen kan få klagomål från kunderna om felaktigheter i deras månatliga kontoutdrag som gör ägaren-företagsledaren uppmärksam på problem beträffande tidpunkten för när kundernas betalningar redovisas i räkenskapsmaterialet.

A115. För företag där det inte finns någon formell process för att övervaka systemet för intern kontroll, kan processen för att övervaka systemet för intern kontroll omfatta att ledningen gör regelbundna genomgångar av den finansiella rapporteringen som är utformad för att bidra till att företaget förhindrar eller identifierar felaktigheter.

Förstå företagets process för att övervaka systemet för intern kontroll (se punkt 24(a))

A116. Frågor som kan vara relevanta för revisorn att beakta när han eller hon skaffar sig en förståelse av hur företaget övervakar sitt system för intern kontroll omfattar

- utformningen av övervakningsarbetet, till exempel om det rör sig om periodisk eller fortlöpande övervakning
- övervakningsarbetets kvalitet och frekvens.
- utvärderingen av resultaten av övervakningsarbetet, utan onödigt dröjsmål, för att fastställa om kontrollerna har fungerat, och
- hur identifierade brister har hanterats genom lämpliga åtgärder, inklusive förmedling av sådana brister till dem som ansvarar för att vidta åtgärder.

A117. Revisorn kan också överväga hur företagets process för att övervaka systemet för intern kontroll hanterar att övervaka informationsbearbetningskontroller som innefattar användning av IT. Det kan till exempel omfatta följande:

- Kontroller för att övervaka komplexa IT-miljöer som
  - löpande utvärderar ändamålsenligheten i utformningen av informationsbearbetningskontroller och modifierar dessa efter vad som förändringar i omständigheterna kräver, eller
  - utvärderar funktionen i informationsbearbetningskontrollerna.
- Kontroller som övervakar de åtkomstkontroller som tillämpas i automatiserade informationsbearbetningskontroller som ligger till grund för arbetsfördelningen.
- Kontroller som övervakar hur fel eller brister i kontrollerna hänförliga till automatiseringen av den finansiella rapporteringen identifieras och hanteras.

Förstå företagets internrevisionsfunktion (se punkt 24(a)(ii))

Bilaga 4 anger vad som vidare behöver beaktas för att förstå ett företags internrevisionsfunktion.

A118. Revisorns frågor till lämpliga personer inom internrevisionsfunktionen hjälper revisorn att skaffa sig en förståelse av karaktären på internrevisionsfunktionens ansvarsområden. Om revisorn kommer fram till att funktionens ansvar har koppling till företagets finansiella rapportering, kan revisorn skaffa sig ytterligare förståelse av de aktiviteter som har utförts eller ska utföras av internrevisionsfunktionen genom att gå igenom funktionens granskningsplan för perioden, om en sådan plan finns, och diskutera den med lämpliga personer inom funktionen. Denna förståelse, tillsammans med den information som har inhämtats genom revisorns frågor kan också ge information som är direkt relevant för revisorns identifiering och bedömning av riskerna för väsentliga felaktigheter. Om, utifrån revisorns preliminära förståelse av internrevisionen, han eller hon räknar med att använda

internrevisionsfunktionens arbete för att ändra karaktär, tidpunkter och omfattningen av de granskningsåtgärder som ska utföras, gäller ISA 610 (omarbetad 2013)[37].

Andra informationskällor som används i företagets process för att övervaka systemet för intern kontroll

Förstå informationskällorna (se punkt 24(b))

A119. I företagsledningens övervakningsarbete kan man använda information från kommunikation med externa parter, t.ex. klagomål från kunder eller synpunkter från tillsynsmyndigheter som kan tyda på att det finns problem eller belysa områden som behöver förbättras.

Varför revisorn måste förstå informationskällorna som används i företagets process för att övervaka systemet för intern kontroll

A120. Revisorns förståelse av informationskällorna som används av företaget vid övervakningen av företagets system för intern kontroll, inklusive huruvida informationen som används är relevant och tillförlitlig, hjälper revisorn att utvärdera huruvida företagets process för att övervaka företagets system för intern kontroll är ändamålsenlig. Om företagsledningen förutsätter att den information som används vid övervakning är relevant och tillförlitlig men saknar grund för detta antagande kan eventuella fel i informationen medföra att företagsledningen drar felaktiga slutsatser av sin övervakning.

Utvärdera företagets process för att övervaka systemet för intern kontroll (se punkt 24(c))

Varför revisorn utvärderar huruvida företagets process för att övervaka systemet för intern kontroll är ändamålsenlig

A121. Revisorns utvärdering av hur företaget genomför fortlöpande och separata utvärderingar för att övervaka hur effektiva kontrollerna är hjälper revisorn att förstå huruvida de andra delarna i företagets system för intern kontroll finns på plats och fungerar, och bidrar därmed till att förstå de andra delarna i företagets system för intern kontroll. Denna utvärdering kan också hjälpa revisorn att identifiera och bedöma riskerna för väsentliga felaktigheter på rapport- och påståendenivån (se punkt A86).

Att utvärdera huruvida företagets process för att övervaka systemet för intern kontroll är lämplig (se punkt 24(c))

A122. Revisorns utvärdering av huruvida företagets process för att övervaka systemet för intern kontroll är godtagbar grundar sig på revisorns förståelse av företagets process för att övervaka systemet för intern kontroll.

Informationssystem och kommunikation, samt kontrollaktiviteter (se punkt 25–26)

A123. Kontrollerna i informationssystemet och kommunikationen, samt kontrollaktiviteter är främst direkta kontroller (dvs. kontroller som är tillräckligt precisa för att förhindra, upptäcka och rätta till felaktigheter på påståendenivån).

[37] ISA 610 (omarbetad 2013), *Använda det arbete som har utförts av internrevisionen*

Varför revisorn måste förstå informationssystemet och kommunikationen samt kontrollerna som utgör kontrollaktivitetskomponenten

A124. Revisorn måste förstå företagets informationssystem och kommunikation eftersom en förståelse av företagets riktlinjer som definierar transaktionsflödena och andra aspekter av företagets informationsbearbetningsaktiviteter hänförliga till upprättandet av företagets finansiella rapporter, och förstå och utvärdera om komponenten på ett lämpligt sätt stödjer upprättandet av företagets finansiella rapporter, stödjer revisorns identifiering och bedömning av risken för väsentliga felaktigheter på påståendenivån. Denna förståelse och utvärdering kan också resultera i att revisorn identifierar risker för väsentliga felaktigheter på rapportnivån när resultaten av revisorns granskningsåtgärder är oförenliga med förväntningarna på företagets system för intern kontroll som kan ha fastställts baserat på information som har inhämtats under processen med att acceptera eller fortsätta med uppdraget (se punkt A86).

A125. Revisorn måste identifiera specifika kontroller i kontrollaktivitetskomponenten och utvärdera utformningen och fastställa huruvida kontrollerna har införts, eftersom det hjälper revisorns förståelse av ledningens metod för att hantera vissa risker och därmed erbjuda en grund för utformningen och genomförandet av fortsatta granskningsåtgärder som ett svar på dessa risker enligt kraven i ISA 330. Ju högre i spektrumet av inneboende risk en risk bedöms ligga, desto mer övertygande behöver revisionsbevisen vara. Även när revisorn inte planerar att testa identifierade kontrollers funktion, kan revisorns förståelse ändå påverka utformningen av art, tidpunkter och omfattning av den substansgranskning som är ett svar på den hänförliga risken för väsentliga felaktigheter.

Den iterativa karaktären på revisorns förståelse och utvärdering av informationssystem och kommunikation, samt kontrollaktiviteter

A126. Enligt förklaringen i punkt A49 kan revisorns förståelse av företaget och dess miljö och det tillämpliga ramverket för finansiell rapportering också hjälpa revisorn att utveckla initiala förväntningar på vilka transaktionsslag, konton och upplysningar som kan vara väsentliga. När revisorn skaffar sig en förståelse för informationssystemet och kommunikationskomponenten enligt punkt 25(a) kan han eller hon använda dessa initiala förväntningar i syfte att fastställa omfattningen av förståelsen av företagets informationsbearbetningsaktiviteter som behöver inhämtas.

A127. Revisorns förståelse av informationssystemet omfattar att förstå de riktlinjer som definierar informationsflöden avseende företagets väsentliga transaktionsslag, konton och upplysningar samt övriga relaterade aspekter av företagets informationsbearbetningsaktiviteter. Denna information, och informationen som inhämtas från revisorns utvärdering av informationssystemet, kan bekräfta eller ytterligare påverka revisorns förväntningar gällande de väsentliga transaktionsslag, konton och upplysningar som identifierades inledningsvis (se punkt A126).

A128. När revisorn bildar sig en uppfattning om hur information hänförlig till väsentliga transaktionsslag, konton och upplysningar flödar in till, genom och ut från företagets informationssystem kan han eller hon också identifiera kontroller i kontrollaktiviteterna som måste identifieras enligt punkt 26(a). Revisorns identifiering och utvärdering av kontrollerna i kontrollaktivitetskomponenten kan först ha fokus på kontroller av bokföringsposter och kontroller för vilka revisorn planerar att testa funktionen vid utformningen av substansgranskningens art, tidpunkter och omfattning.

A129. Revisorns bedömning av de inneboende riskerna kan också påverka identifieringen av kontroller i kontrollaktivitetskomponenten. Revisorns identifiering av kontroller avseende väsentliga risker kanske till exempel bara går att identifiera när revisorn har bedömt den inneboende risken på påståendenivån i enlighet med punkt 31. Dessutom kanske kontroller som avser risker för vilka revisorn har fastställt att enbart substansgranskning inte erbjuder tillräckliga och ändamålsenliga revisionsbevis (enligt punkt 33) inte går att identifiera förrän revisorns bedömning av de inneboende riskerna har genomförts.

A130. Revisorns identifiering och bedömning av risker för väsentliga felaktigheter på påståendenivån påverkas både av revisorns

- förståelse av företagets riktlinjer för dess informationsbearbetningsaktiviteter i informationssystemet samt kommunikationskomponenten, och
- identifiering och utvärdering av kontroller i kontrollaktivitetskomponenten.

Skaffa sig en förståelse för informationssystem och kommunikation (se punkt 25)

> **Bilaga 3**, punkterna 15–19, anger ytterligare överväganden hänförliga till informationssystem och kommunikation.

Skalbarhet

A131. Informationssystemet och hänförliga affärsprocesser i mindre komplexa företag är sannolikt mindre sofistikerade än i större företag, och innefattar sannolikt en mindre komplex IT-miljö, men informationssystemets roll är precis lika viktig ändå. Mindre komplexa företag med en direkt engagerad företagsledning kanske inte behöver omfattande beskrivningar av redovisningsrutiner, sofistikerat räkenskapsmaterial eller skriftliga riktlinjer. Att förstå de relevanta aspekterna av företagets informationssystem kan därför kräva mindre arbete i ett mindre komplext företag, och kan omfatta en större mängd frågor än observation eller inspektion av dokumentation. Behovet av att bilda sig en uppfattning förblir emellertid viktigt för att erbjuda en grund för utformningen av fortsatta granskningsåtgärder enligt ISA 330 och kan ytterligare hjälpa revisorn att identifiera eller bedöma risker för väsentliga felaktigheter (se punkt A86).

Skaffa sig en förståelse av informationssystemet (se punkt 25(a))

A132. Inkluderat i företagets system för intern kontroll finns aspekter som är hänförliga till företagets mål för den finansiella rapporteringen, men kan också innefatta aspekter som avser dess verksamhets- eller efterlevnadsmål, när sådana aspekter är relevanta för den finansiella rapporteringen. Att förstå hur företaget initierar transaktioner och inhämtar information som en del av revisorns förståelse av informationssystemet kan omfatta information om företagets system (dess riktlinjer) utformade för att hantera verksamhets- och efterlevnadsmål eftersom sådan information är relevant för upprättandet av de finansiella rapporterna. Dessutom kan vissa företag ha informationssystem som i hög grad är integrerade, på så sätt att kontrollerna kan vara utformade för att på samma gång uppnå målen för den finansiella rapporteringen, verksamhets- och efterlevnadsmål och kombinationer av dessa.

A133. Att förstå företagets informationssystem omfattar också en förståelse av de resurser som ska användas i företagets informationsbearbetningsaktiviteter. Information om den personal som omfattas som kan vara relevant för att förstå riskerna för informationssystemets säkerhet omfattar

- kompetensen hos de personer som utför arbetet
- om det finns tillräckliga resurser, och
- om det finns en lämplig arbetsfördelning.

A134. Frågor som revisorn kan beakta när han eller hon bildar sig en uppfattning om de riktlinjer som definierar informationsflödena hänförliga till företagets väsentliga transaktionsslag, konton och upplysningar i informationssystemet och kommunikationskomponenten omfattar karaktären på

(a) data eller information hänförlig till transaktioner, andra händelser och omständigheter som ska bearbetas

(b) den informationsbearbetning som ska upprätthålla integriteten för data eller informationen, och

(c) informationsprocesserna, personalresurserna eller andra resurser som används i informationsbearbetningsprocessen.

A135. Att få en förståelse för företagets affärsprocesser, som inbegriper hur transaktioner uppstår, hjälper revisorn att förstå företagets informationssystem på ett sätt som är lämpligt med hänsyn till omständigheterna i företaget.

A136. Revisorns förståelse av informationssystemet kan inhämtas på olika sätt och kan omfatta

- frågor till relevant personal om de rutiner som används för att skapa, registrera, bearbeta och rapportera transaktioner eller om företagets process för finansiell rapportering
- inspektion av handböcker med riktlinjer eller annan dokumentation av företagets informationssystem
- observation av hur företagets personal tillämpar riktlinjer och processer, eller
- att välja transaktioner och spåra dem genom den tillämpliga processen i informationssystemet (dvs. utföra ett s. k. ”walk-through”-test).

Automatiserade verktyg och tekniker

A137. Revisorn kan också använda automatiserade tekniker för att få direkt tillgång till eller en digital nedladdning från de databaser i företagets datasystem som lagrar bokföringen av transaktioner.. Genom att använda automatiserade verktyg eller tekniker på denna information kan revisorn bekräfta den förståelse som har inhämtats om hur transaktioner flödar genom informationssystemet genom att spåra bokföringsposter eller annan digital bokföring avseende en viss transaktion, eller en hel population av transaktioner, från att de läggs in i räkenskapsmaterialet till redovisningen i huvudboken. Analyser av fullständiga eller stora mängder transaktioner kan också leda till att revisorn identifierar avvikelser från de normala, eller förväntade, processerna för att bearbeta dessa transaktioner, vilket kan leda till att revisorn identifierar risker för väsentliga felaktigheter.

Information som inte har inhämtats från huvudbok eller försystem

A138. De finansiella rapporterna kan innehålla information som inte har inhämtats från huvudbok eller försystem. Exempel på sådan information som revisorn kan beakta omfattar följande:

- Information som inhämtats från leasingavtal relevanta för upplysningar i de finansiella rapporterna.
- Upplysningar i de finansiella rapporterna som kommer från ett företags system för riskhantering.
- Information om verkligt värde som tagits fram av företagsledningens specialister och som presenteras i de finansiella rapporterna.
- Information som presenteras i de finansiella rapporterna, som kommer från modeller eller från andra beräkningar som använts för att ta fram uppskattningar för redovisningsändamål som redovisats eller presenterats i de finansiella rapporterna, däribland information avseende underliggande data och antaganden som används i dessa modeller, t.ex.:
  - antaganden som tagits fram internt som kan påverka en tillgångs nyttjandeperiod
  - data, t.ex. räntesatser som påverkas av faktorer som ligger utanför företagets kontroll.
- Information som lämnas i de finansiella rapporterna om känslighetsanalyser som härletts ur ekonomiska modeller som visar att företagsledningen har övervägt alternativa antaganden.
- Information som redovisas eller presenteras i de finansiella rapporterna som har inhämtats från ett företags deklarationer och underliggande material.
- Information som lämnas i de finansiella rapporterna som har inhämtats från analyser som upprättas till stöd för företagsledningens bedömning av företagets förmåga att fortsätta verksamheten, t.ex. eventuella upplysningar som avser händelser eller förhållanden som har identifierats, som kan leda till tvivel om företagets förmåga att fortsätta verksamheten.[38]

A139. Vissa belopp eller upplysningar i företagets finansiella rapporter (t.ex. upplysningar om kreditrisk, likviditetsrisk och marknadsrisk) kan vara baserade på information som inhämtats från företagets system för riskhantering. Men det finns inget krav på att revisorn ska förstå alla aspekter av systemet för riskhantering och revisorn använder professionell bedömning när han eller hon fastställer vilken förståelse som är nödvändig.

Företagets användning av informationsteknik i informationssystemet

Varför revisorn skaffar sig en förståelse för den IT-miljö som är relevant för informationssystemet

A140. Revisorns förståelse av informationssystemet innefattar den IT-miljö som är relevant för flödena av transaktioner och bearbetningen av information i företagets informationssystem eftersom företagets användning av IT-applikationer och andra frågor som rör IT-miljön kan ge upphov till IT-relaterade risker.

[38] ISA 570 (omarbetad), punkterna 19–20

A141. Förståelsen av företagets affärsmodell och hur den integrerar användningen av IT kan också ge ett användbart sammanhang för karaktären på och omfattningen av IT som revisorn förväntar sig finna i informationssystemet.

Förstå företagets användning av IT

A142. Revisorns förståelse av IT-miljön kan ha fokus på att identifiera, och förstå karaktären på och omfattningen av, de specifika IT-applikationerna och andra aspekter av IT-miljön som är relevanta för transaktionsflödena och informationsbearbetningen i informationssystemet. Förändringar i transaktionsflödet eller information inom ramen för informationssystemet kan vara ett resultat av förändringar i IT-applikationer, eller direkta ändringar av data i de databaser som Ingår I bearbetningen eller lagringen av dessa transaktioner eller den informationen.

A143. Revisorn kan identifiera de IT-applikationer och den stödjande IT-infrastrukturen samtidigt med revisorns förståelse av hur information hänförlig till transaktionsslag, konton och upplysningar flödar in i, genom och ut från företagets informationssystem.

Skaffa sig en förståelse för företagets kommunikation (se punkt 25(b))

Skalbarhet

A144. I större, mer komplexa, företag kan information som revisorn kan överväga när han eller hon skaffar sig en förståelse av företagets kommunikation komma från handböcker med riktlinjer och handböcker gällande finansiell rapportering.

A145. I mindre komplexa företag kan kommunikationen vara mindre strukturerad (t.ex. kanske inte formella handböcker används) eftersom det finns färre ansvarsnivåer och företagsledningen är mer synlig och tillgänglig. Oavsett företagets storlek underlättar öppna kommunikationskanaler både att rapportera avvikelser och att agera utifrån dem.

Att utvärdera om de relevanta aspekterna av informationssystemet stödjer upprättandet av företagets finansiella rapporter (se punkt 25(c))

A146. Revisorns utvärdering av huruvida företagets informationssystem och kommunikation på ett lämpligt sätt stödjer upprättandet av de finansiella rapporterna grundar sig på den förståelse som inhämtas enligt punkterna 25(a)–(b).

Kontrollaktiviteter (se punkt 26)

Kontroller i kontrollaktivitetskomponenten

Bilaga 3, punkterna 20 och 21, anger vidare överväganden hänförliga till kontrollaktiviteter.

A147. Kontrollaktivitetskomponenten omfattar kontroller som är utformade för att säkerställa en korrekt tillämpning av riktlinjerna (som också är kontroller) i alla de andra komponenterna i företagets system för intern kontroll, och omfattar både direkta och indirekta kontroller.

Exempel:

De kontroller som ett företag har inrättat för att se till att de anställda räknar och bokför den årliga lagerinventeringen på rätt sätt, hänför sig direkt till riskerna för väsentliga felaktigheter avseende påståendena om existens och fullständighet för posten varulager.

A148. Revisorns identifiering och utvärdering av kontrollerna i kontrollaktivitetskomponenten har fokus på informationsbearbetningskontroller, vilka är kontroller som tillämpas under bearbetningen av informationen i företagets informationssystem som direkt avser risker gällande informationens integritet (dvs. fullständigheten, korrektheten och giltigheten för transaktioner och övrig information). Revisorn behöver emellertid inte identifiera och utvärdera alla informationsbearbetningskontroller hänförliga till de av företagets riktlinjer som definierar transaktionsflödena och andra aspekter av företagets informationsbearbetningsaktiviteter för väsentliga transaktionsslag, konton och upplysningar.

A149. Det kan också finnas direkta kontroller i kontrollmiljön, företagets riskbedömningsprocess eller företagets process för att övervaka systemet för intern kontroll, som kan identifieras enligt punkt 26. Men ju mer indirekt relationen är mellan kontroller som stödjer andra kontroller och den kontroll som granskas, desto mindre effektiv kan den kontrollen vara för att förhindra, eller upptäcka och rätta till, relaterade felaktigheter.

Exempel:

När en försäljningschef går igenom en summering av försäljningsaktiviteten för vissa butiker fördelat på regioner hänför sig detta vanligtvis endast indirekt till riskerna för väsentliga felaktigheter avseende påståendet fullständighet av försäljningsintäkter. Den kan således vara mindre effektiv när det gäller att hantera de riskerna än kontroller som mer direkt hänför sig till dessa, t.ex. när leveransdokument jämförs med faktureringsdokument.

A150. Punkt 26 kräver också att revisorn identifierar och utvärderar allmänna IT-kontroller för IT-applikationer och andra aspekter av IT-miljön som revisorn har fastställt är föremål för IT-relaterade risker, eftersom de allmänna IT-kontrollerna stödjer att informationsbearbetningskontrollerna fortsätter att fungera på ett ändamålsenligt sätt. En allmän IT-kontroll är i sig normalt inte tillräcklig för att hantera risker för väsentliga felaktigheter på påståendenivån.

A151. De kontroller som revisorn måste identifiera och utvärdera utformningen av, samt fastställa att de har införts, enligt punkt 26 är följande:

- Kontroller för vilka revisorn planerar att granska att de fungerar vid fastställandet av substansgranskningens art, tidpunkter och omfattning. Utvärderingen av sådana kontroller lägger grunden till revisorns utformning av granskning av kontrollprocesser enligt ISA 330. Dessa kontroller omfattar även de kontroller som hanterar risker för vilka inte enbart substansgranskning kan ge tillräckliga och ändamålsenliga revisionsbevis.
- Kontroller omfattar kontroller som hanterar betydande risker och kontroller avseende bokföringsposter. Revisorns identifiering och utvärdering av sådana kontroller kan också påverka revisorns förståelse av riskerna för väsentliga felaktigheter, inklusive att identifiera

ytterligare risker för väsentliga felaktigheter (se punkt A95). Denna förståelse lägger också grunden till revisorns utformning av art, tidpunkter och omfattning av den substansgranskning som hanterar de hänförliga bedömda riskerna för väsentliga felaktigheter.

- Övriga kontroller som revisorn betraktar som lämpliga för att göra det möjligt för revisorn att uppnå målen i punkt 13 med avseende på riskerna på påståendenivån, grundat på revisorns professionella omdöme.

A152. Kontrollerna i kontrollaktivitetskomponenten måste identifieras när sådana kontroller uppfyller ett eller flera av kriterierna som ingår i punkt 26(a). När däremot flera kontrollaktiviteter uppfyller samma mål är det inte nödvändigt att identifiera varje kontrollaktivitet med samma mål.

Olika sorters kontroller i kontrollaktivitetskomponenten (se punkt 26)

A153. Exempel på kontroller i kontrollaktivitetskomponenten omfattar befogenheter och godkännanden, avstämningar, verifieringar (så som inmatnings- och valideringskontroller eller automatiserade beräkningar), arbetsfördelning samt fysiska eller logiska kontroller, inklusive dem som avser skydd av tillgångar.

A154. Kontroller i kontrollaktivitetskomponenten kan också innefatta kontroller som fastställts av företagsledningen för att hantera risker för väsentliga felaktigheter på grund av att upplysningar inte upprättas enligt det tillämpliga ramverket för finansiell rapportering. Sådana kontroller kan avse information i de finansiella rapporterna som inte har inhämtats från huvudbok med undersystem.

A155. Oavsett om kontrollerna finns i IT-system eller manuella system kan kontrollerna ha olika mål och tillämpas på olika organisations- och funktionsnivåer.

Skalbarhet (se punkt 26)

A156. Kontrollerna i kontrollaktivitetskomponenten i mindre komplexa företag liknar sannolikt dem som finns i större företag, men de kan vara mer eller mindre formella. Dessutom kan i mindre komplexa företag fler kontroller utföras direkt av ledningen.

> **Exempel**:
>
> Att företagsledningen ensam har rätt att bevilja kredit åt kunder och godkänna betydande inköp kan ge stark kontroll över viktiga konton och transaktioner.

A157. Det kan vara svårare att etablera arbetsfördelning i mindre komplexa företag som har färre anställda. I ett ägarstyrt företag kan ägaren-företagsledaren uppnå en mer effektiv tillsyn genom direkt medverkan än i ett större företag, vilket kan kompensera för de vanligtvis mer begränsade möjligheterna till arbetsfördelning. Som framgår av ISA 240, kan situationen där ledningen domineras av en person innebära en kontrollbrist, eftersom detta innebär en möjlighet för ledningen att sätta sig över kontrollerna.[39]

[39] ISA 240, punkt A28

Kontroller som hanterar riskerna för väsentliga felaktigheter på påståendenivån (se punkt 26(a))

Kontroller som hanterar risker som har fastställts som betydande (se punkt 26(a)(i))

A158. Oavsett om revisorn planerar att granska att de kontroller som hanterar betydande risker fungerar kan förståelsen som har inhämtats av ledningens sätt att hantera sådana risker utgöra grund för utformningen och genomförandet av substansgranskning som ett svar på betydande risker enligt kraven i ISA 330.[40] Även om risker som hänger samman med betydande icke rutinmässiga frågor eller bedömningar mer sällan omfattas av rutinkontroller kan företagsledningen införa andra åtgärder för att hantera sådana risker. I revisorns förståelse av huruvida företaget har utformat och infört kontroller för betydande risker som hänför sig till icke rutinmässiga frågor eller bedömningsfrågor kan följaktligen ingå att förstå om och hur företagsledningen hanterar riskerna. Sådana motåtgärder kan omfatta

- kontroller såsom att högsta ledningen eller specialister går igenom antaganden
- dokumenterade processer för uppskattningar för redovisningsändamål
- godkännande av styrelsen.

> **Exempel**:
>
> Vid enstaka händelser, såsom när företaget stäms i en betydande rättslig process, kan beaktande av hur företaget hanterar denna inbegripa frågor som huruvida ärendet har vidarebefordrats till lämpliga specialister (t.ex. intern eller extern jurist), om dess potentiella effekt har bedömts och hur man föreslår att upplysningar om situationen ska lämnas i de finansiella rapporterna.

A159. ISA 240[41] kräver att revisorn förstår kontrollerna hänförliga till de bedömda riskerna för väsentliga felaktigheter till följd av oegentligheter (som behandlas som betydande risker), och förklarar ytterligare att det är viktigt för revisorn att skaffa sig en förståelse av de kontroller som ledningen har utformat, infört och upprätthåller för att förhindra och upptäcka oegentligheter.

Kontroller av bokföringsposter (se punkt 26(a)(ii))

A160. Kontroller som hanterar risker för väsentliga felaktigheter på påståendenivån och som förväntas identifieras för alla revisioner är kontroller av bokföringsposter, eftersom det sätt som ett företag införlivar information från bearbetningen av transaktioner till huvudboken vanligtvis omfattar användningen av bokföringsposter, vare sig de är standardiserade eller inte, eller automatiserade eller manuella. I vilken grad andra kontroller identifieras kan variera beroende på företagets karaktär och revisorns planerade metod för fortsatta granskningsåtgärder.

---

[40] ISA 330, punkt 21

[41] ISA 240, punkterna 28 och A33

> **Exempel**:
>
> I en revision av ett mindre komplext företag kanske inte företagets informationssystem är komplext och revisorn kanske inte planerar att förlita sig på kontrollernas funktion. Vidare kanske inte revisorn har identifierat några betydande risker eller några andra risker för väsentliga felaktigheter som gör det nödvändigt för revisorn att utvärdera kontrollernas utformning och fastställa huruvida de har införts. I en sådan revision kanske revisorn fastställer att det inte finns några identifierade kontroller utöver företagets kontroller av bokföringsposter.

Automatiserade verktyg och tekniker

A161. I manuella huvudbokssystem kan icke standardiserade bokföringsposter identifieras genom inspektion av huvudböcker, grundböcker och verifikationer. När automatiserade rutiner används för att föra huvudbok och upprätta finansiella rapporter, kanske sådana poster enbart finns i elektronisk form och därför enklast kan identifieras genom användning av automatiserade revisionsmetoder.

> **Exempel**:
>
> I revisionen av ett mindre komplext företag kan revisorn extrahera en fullständig lista över alla bokföringsposter till ett enkelt kalkylark. Det kan då vara möjligt för revisorn att ordna bokföringsposterna genom att tillämpa ett antal olika filter som valutabelopp, namn på den som har upprättat eller granskat bokföringsposterna, bokföringsposter som ändrar nettoposter till bruttoposter, eller att studera listan per det datum då bokföringsposten fördes in i huvudboken, för att hjälpa revisorn att utforma svar på riskerna som har identifierats hänförligt till bokföringsposter.

Kontroller för vilka revisorn planerar att utföra granskning av (se punkt 26(a)(iii))

A162. Revisorn fastställer om det finns några risker för väsentliga felaktigheter på påståendenivån för vilka det inte är möjligt att erhålla tillräckliga och lämpliga revisionsbevis enbart genom substansgranskning. Revisorn måste, enligt ISA 330,[42] utforma och genomföra test av kontroller som avser sådana risker för väsentliga felaktigheter för vilka enbart substansgranskning inte ger tillräckliga och ändamålsenliga revisionsbevis på påståendenivån. Det får till följd att när det finns sådana kontroller som hanterar dessa måste de identifieras och utvärderas.

A163. I andra fall, när revisorn planerar att beakta kontrollernas funktion när han eller hon fastställer art, tidpunkter och omfattning av substansgranskning enligt ISA 330 måste sådana kontroller också identifieras eftersom ISA 330[43] kräver att revisorn utformar och genomför tester av dessa kontroller.

---

[42] ISA 330, punkt 8(b)

[43] ISA 330, punkt 8(a)

Exempel:

Revisorn kan planera att granska funktionen hos kontroller

- av rutintransaktionsslag eftersom en sådan granskning kan vara effektivare för stora volymer av homogena transaktioner
- avseende hur fullständig och riktig den information som företaget framställer är (t.ex. kontroller av upprättandet av systemgenererade rapporter) för att fastställa hur tillförlitlig den informationen är, när revisorn har för avsikt att förlita sig på dessa kontroller för att utforma och utföra fortsatta granskningsåtgärder
- avseende verksamhets- och efterlevnadsmålen när de gäller data som revisorn utvärderar eller använder när han eller hon utför granskningsåtgärder.

A164. Revisorns planer på att granska kontrollernas funktion kan också påverkas av de identifierade riskerna för väsentliga felaktigheter på rapportnivån. Om till exempel brister identifieras som är hänförliga till kontrollmiljön kan detta påverka revisorns övergripande förväntningar på de direkta kontrollernas funktion.

Andra kontroller som revisorn anser är lämpliga (se punkt 26(a)(iv))

A165. Andra kontroller som revisorn kan anse är lämpliga att identifiera, utvärdera utformningen av och fastställa att de är införda, kan omfatta

- kontroller som avser risker som bedöms ligga högre i spektrumet av inneboende risker men som inte har bedömts vara betydande risker
- kontroller hänförliga till avstämningen av detaljerat bokföringsmaterial mot huvudboken, eller
- kompletterande kontroller i företaget, om man använder sig av en serviceorganisation.[44]

Identifiera IT-applikationer och andra aspekter på IT-miljön, IT-relaterade risker och allmänna IT-kontroller (se punkt 26(b)–(c))

Bilaga 5 omfattar exempel på egenskaper hos IT-applikationer och andra aspekter av IT-miljön, samt vägledning hänförlig till dessa egenskaper, som kan vara relevanta vid identifieringen av IT-applikationer och andra aspekter av IT-miljön som är föremål för IT-relaterade risker.

Identifiera IT-applikationer och andra aspekter av IT-miljön (se punkt 26(b))

Varför revisorn identifierar IT-relaterade risker och allmänna IT-kontroller hänförliga till IT-applikationer och andra aspekter av IT-miljön

A166. Förstå de IT-relaterade riskerna och de allmänna IT-kontroller som har införts av företaget för att hantera dessa risker kan påverka

[44] ISA 402, *Revisorns överväganden vid revision av företag som anlitar en servicebyrå*

- revisorns beslut om huruvida han eller hon ska granska kontrollernas funktion för att hantera riskerna för väsentliga felaktigheter på påståendenivån.

  Exempel:

  När de allmänna IT-kontrollerna inte är utformade på ett ändamålsenligt sätt eller inte har införts på att lämpligt sätt för att hantera de IT-relaterade riskerna (t.ex. att kontrollerna inte på ett lämpligt sätt förhindrar eller upptäcker obehöriga förändringar av program eller obehörig åtkomst till IT-applikationer) kan detta påverka revisorns beslut att förlita sig på automatiserade kontroller inom de IT-applikationer som påverkas.

- Revisorns bedömning av kontrollrisk på påståendenivån.

  Exempel:

  Den löpande funktionen hos en informationsbearbetningskontroll kan bero på vissa allmänna IT-kontroller som förhindrar eller upptäcker obehöriga programändringar i IT-informationsbearbetningskontrollen (dvs. programändringskontroller av den tillhörande IT-applikationen). Under sådana omständigheter kan den allmänna funktionen (eller brist på densamma) hos den allmänna IT-kontrollen påverka revisorns bedömning av kontrollrisken (t.ex. kan kontrollrisken vara högre när sådana allmänna IT-kontroller förväntas vara bristfälliga eller om revisorn inte planerar att testa de allmänna IT-kontrollerna).

- Revisorns strategi för att granska information som tas fram av företaget som kommer från eller inbegriper företagets IT-applikationer.

  Exempel:

  När information som tas fram av företaget för att användas som revisionsbevis tas fram av IT-applikationer kan revisorn bestämma sig för att granska kontroller över systemgenererade rapporter, inklusive identifiering och testning av allmänna IT-kontroller som hanterar risker för otillbörliga eller obehöriga programändringar eller direkta ändringar av data i rapporterna.

- Revisorns bedömning av inneboende risker på påståendenivån, eller

  Exempel:

  Där det förekommer betydande eller omfattande programmeringsändringar av en IT-applikation för att hantera nya eller reviderade rapporteringskrav i det tillämpliga ramverket för finansiell rapportering kan det vara ett tecken på komplexiteten i de nya kraven och deras effekt på företagets finansiella rapporter. När sådana omfattande data- eller programmeringsändringar förekommer blir sannolikt även IT-applikationen föremål för IT-relaterade risker.

- Utformningen av fortsatta granskningsåtgärder.

Exempel:

Om informationsbearbetningskontroller är beroende av allmänna IT-kontroller kan revisorn bestämma sig för att testa funktionerna hos allmänna IT-kontroller, vilket då kräver att test av kontroller utformas för sådana allmänna IT-kontroller. Om revisorn under samma omständigheter bestämmer sig för att inte granska att de allmänna IT-kontrollerna fungerar, eller om de allmänna IT-kontrollerna förväntas vara ineffektiva, kan de IT-relaterade risker som revisorn granskar, behöva hanteras genom att revisorn utformar processer för substansgranskning. Men de IT-relaterade riskerna kanske inte kan hanteras när sådana risker avser risker för vilka inte enbart substansgranskning ger tillräckliga och ändamålsenliga revisionsbevis. Under sådana omständigheter kan revisorn behöva överväga betydelsen för uttalanden i revisors rapport.

Identifiera IT-applikationer som är föremål för IT-relaterade risker

A167. För de IT-applikationer som är relevanta för informationssystemet kan en förståelse av karaktären på och komplexiteten i de specifika IT-processerna och de allmänna IT-kontrollerna som företaget har inrättat hjälpa revisorn att fastställa vilka IT-applikationer som företaget förlitar sig på för att på ett korrekt sätt bearbeta och upprätthålla integriteten i informationen i företagets informationssystem. Sådana IT-applikationer kan vara föremål för IT-relaterade risker.

A168. Att identifiera de IT-applikationer som är föremål för IT-relaterade risker omfattar att beakta kontroller som identifieras av revisorn eftersom sådana kontroller kan omfatta användningen av IT eller vara beroende av IT. Revisorn kan fokusera på huruvida en IT-applikation omfattar automatiserade kontroller som ledningen förlitar sig på och som revisorn har identifierat, inklusive kontroller som hanterar risker för vilka inte enbart substansgranskningar utgör tillräckliga och ändamålsenliga revisionsbevis. Revisorn kan också beakta hur informationen lagras och bearbetas i informationssystemet avseende väsentliga transaktionsslag, konton och upplysningar samt huruvida ledningen är beroende av allmänna IT-kontroller för att upprätthålla integriteten för den informationen.

A169. De kontroller som identifieras av revisorn kan vara beroende av systemgenerade rapporter, i vilket fall IT-applikationerna som tar fram de rapporterna kan vara föremål för IT-relaterade risker. I andra fall kanske inte revisorn planerar att förlita sig på kontrollerna av de systemgenererade rapporterna och planerar att direkt granska in- eller utdata i sådana rapporter, i vilket fall revisorn kanske inte identifierar de hänförliga IT-applikationerna som föremål för IT-relaterade risker.

Skalbarhet

A170. Hur djup revisorns förståelse av IT-processerna är, inklusive i vilken omfattning företaget har allmänna IT-kontroller på plats, kommer att variera beroende på företagets karaktär och dess IT-miljö, samt baserat på arten och omfattningen av de kontroller som revisorn identifierar. Antalet IT-applikationer som är föremål för IT-relaterade risker varierar också baserat på dessa faktorer.

Exempel:

- Ett företag som använder kommersiell programvara och som inte har tillgång till källkoden för att göra några programändringar, men kan ha processer eller rutiner för att konfigurera programvaran (t.ex. kontoplanen, rapportparametrar eller tröskelvärden). Dessutom kan företaget ha en process eller rutiner för att hantera åtkomsten till programmet (t.ex. en särskilt utsedd person med administratörsrättigheter till den kommersiella programvaran). Under sådana omständigheter kommer företaget sannolikt inte att ha eller behöva några formaliserade allmänna IT-kontroller.
- I motsats till det kan ett större företag i hög grad vara beroende av IT och IT-miljön kan omfatta ett flertal IT-applikationer, och IT-processerna för att hantera IT-miljön kan vara komplexa (t.ex. kanske det finns en särskild IT-avdelning som utvecklar och gör programändringar och hanterar åtkomsträttigheter), inklusive att företaget har infört formaliserade allmänna IT-kontroller av sina IT-processer.
- När ledningen inte förlitar sig på automatiserade kontroller eller allmänna IT-kontroller för att bearbeta transaktioner eller underhålla data, och revisorn inte har identifierat några automatiserade kontroller eller andra informationsbearbetningskontroller (eller några som är beroende av allmänna IT-kontroller), kanske revisorn planerar att direkt granska information som tas fram genom företagets IT-system och kanske inte identifierar några IT-applikationer som är föremål för IT-relaterade risker.
- När ledningen förlitar sig på en IT-applikation för att bearbeta eller underhålla data och datavolymen är betydande, och ledningen förlitar sig på IT-applikationen för att utföra automatiserade kontroller som revisorn också har identifierat är IT-applikationen sannolikt föremål för IT-relaterade risker.

A171. När ett företag har en större komplexitet i sin IT-miljö krävs det sannolikt engagemang från medarbetare med specialistkompetens inom IT för att identifiera IT-applikationerna och andra aspekter på IT-miljön, och fastställa de hänförliga IT-relaterade riskerna. Ett sådant engagemang är sannolikt nödvändigt, och kan behöva vara omfattande för komplexa IT-miljöer.

Identifiera andra aspekter av företagets IT-miljö som är föremål för IT-relaterade risker

A172. Andra aspekter av företagets IT-miljö som kan vara föremål för IT-relaterade risker omfattar nätverket, operativsystem och, i vissa fall, gränssnittet mellan IT-applikationer. Andra aspekter av IT-miljön identifieras vanligtvis inte när revisorn inte identifierar IT-applikationer som är föremål för IT-relaterade risker. När revisorn har identifierat IT-applikationer som är föremål för IT-relaterade risker är det sannolikt att även andra aspekter av IT-miljön t.ex. databas, operativsystem, nätverk) identifieras eftersom sådana aspekter stödjer och samverkar med de identifierade IT-applikationerna.

Identifiera IT-relaterade risker och allmänna IT-kontroller (se punkt 26(c))

> **Bilaga 6** beskriver överväganden för att förstå de allmänna IT-kontrollerna.

A173. När revisorn identifierar de IT-relaterade riskerna kan han eller hon beakta arten på den identifierade IT-applikationen eller andra aspekter på IT-miljön och anledningen till att dessa är föremål för IT-relaterade risker. För vissa identifierade IT-applikationer eller andra aspekter på IT-miljön kan revisorn identifiera tillämpliga IT-relaterade risker som främst härrör från obehörig åtkomst eller obehöriga programändringar liksom sådana som hanterar risker hänförliga till otillbörliga ändringar av data (t.ex. risken för otillbörliga förändringar av data genom direkt åtkomst till databaser eller möjligheten att direkt manipulera information).

A174. Omfattningen av och arten på de IT-relaterade riskerna varierar beroende på arten på och egenskaperna hos de identifierade IT-applikationerna och andra aspekter av IT-miljön. Tillämpliga IT-risker kan uppkomma när företaget använder externa eller interna tjänsteleverantörer för identifierade delar av sin IT-miljö (t.ex. lägga ut värdskapet för sin IT-miljö till en tredje part eller använda ett gemensamt servicecenter för en central hantering av IT-processer i en koncern). Tillämpliga IT-relaterade risker kan också identifieras hänförliga till cybersäkerheten. Det är mer sannolikt att det förekommer fler IT-relaterade risker när volymerna eller komplexiteten i automatiserade programkontroller är större och ledningen har större tillit till de kontrollerna för en effektiv bearbetning av transaktioner eller att dessa kontroller säkerställer en effektiv underliggande information.

Utvärdera utformningen och fastställa införandet av identifierade kontroller i kontrollaktivitetskomponenten (se punkt 26(d))

A175. Vid bedömning av hur en kontroll är utformad beaktar revisorn huruvida kontrollen, ensam eller i kombination med andra kontroller, ändamålsenligt klarar att förhindra, eller upptäcka och rätta, väsentliga felaktigheter (dvs. målet med kontrollen).

A176. Revisorn bekräftar hur en identifierad kontroll har införts genom att fastställa att kontrollen finns och att företaget använder den. Det är ingen större mening med att revisorn bedömer hur en kontroll som inte är ändamålsenligt utformad har införts. Därför bedömer revisorn först kontrollens utformning. En kontroll som inte är korrekt utformad kan utgöra en brist i kontrollen.

A177. I riskbedömning med syfte att inhämta revisionsbevis om utformningen och införandet av identifierade kontroller i kontrollaktivitetskomponenten kan följande aktiviteter ingå:

- frågor till företagets anställda
- observation av utförandet av specifika kontroller
- inspektion av dokument och rapporter.

Enbart frågor är emellertid inte tillräckligt för detta ändamål.

A178. Revisorn kan förvänta sig, utifrån erfarenheter från tidigare revisioner eller baserat på det aktuella årets riskbedömning, att ledningen inte har ändamålsenligt utformade eller införda kontroller för att hantera väsentliga risker. I sådana fall kan bedömningen som genomförs för att tillgodose kraven i

punkt 26(d) bestå av att avgöra att sådana kontroller inte har utformats eller införts på ett ändamålsenligt sätt. Om resultaten av bedömningen tyder på att kontrollerna nyligen har utformats eller införts måste revisorn genomföra bedömningen i punkterna 26(b)–(d) avseende de nyligen utformade eller införda kontrollerna.

A179. Revisorn kan dra slutsatsen att en kontroll som är ändamålsenligt utformad och införd kan vara lämplig att granska för att ta dess funktion i beaktande när han eller hon utformar sin substansgranskning. När en kontroll däremot inte är ändamålsenligt utformad eller införd är det ingen mening med att testa den. När revisorn planerar att testa en kontroll utgör informationen som har inhämtats om i vilken grad kontrollen hanterar risken/riskerna för väsentliga felaktigheter, indata till revisorns bedömning av kontrollrisken på påståendenivån.

A180. Det är inte tillräckligt att utvärdera utformningen och fastställa införandet av identifierade kontroller i kontrollaktivitetskomponenten för att granska att de fungerar. För automatiserade kontroller kan revisorn emellertid planera att granska funktionen hos automatiserade kontroller genom att identifiera och granska allmänna IT-kontroller som sörjer för en konsekvent drift av en automatiserad kontroll, i stället för att utföra tester av funktionen hos de automatiserade kontrollerna direkt. Att inhämta ett revisionsbevis som avser införandet vid en viss tidpunkt av en manuell kontroll ger inte revisionsbevis avseende kontrollens funktion vid andra tidpunkter under den räkenskapsperiod som revisionen omfattar. Granskning av kontrollernas funktion, inklusive granskning av indirekta kontroller, beskrivs närmare i ISA 330.[45]

A181. När revisorn inte planerar att granska att identifierade kontroller fungerar kan revisorns förståelse ändå hjälpa till vid utformningen av art, tidpunkter och omfattning av den substansgranskning som är ett svar på den hänförliga risken för väsentliga felaktigheter.

> **Exempel**:
>
> Utfallen av denna riskbedömning kan ligga till grund för revisorns bedömning av möjliga avvikelser i en population när han eller hon utformar ett urval av transaktioner för granskning.

Brister i kontrollerna i företagets system för intern kontroll (se punkt 27)

A182. När revisorn genomför utvärderingarna av var och en av komponenterna i företagets system för intern kontroll[46] kan hon eller han fastställa att vissa av företagets riktlinjer för en komponent inte är lämplig med beaktande av företagets karaktär och omständigheter. En sådan bedömning kan vara ett tecken som hjälper revisorn att identifiera brister i kontrollerna. Om revisorn har identifierat en eller flera brister i kontrollerna kan revisorn beakta effekten av dessa brister för kontrollerna när han eller hon utformar ytterligare granskningsåtgärder i enlighet med ISA 330.

---

[45] ISA 330, punkterna 8–11

[46] Punkterna 21(b), 22(b), 24(c), 25(c) och 26(d)

A183. Om revisorn har identifierat en eller flera brister i kontrollerna kräver ISA 265[47] att revisorn avgör om dessa brister, enskilt eller i kombination med andra, utgör en betydande brist. Revisorn gör en professionell bedömning när han eller hon avgör om en brist utgör en betydande brist.[48]

> **Exempel**:
>
> Omständigheter som kan tyda på att det föreligger en betydande brist omfattar frågor som
>
> - identifieringen av oegentligheter oavsett storlek som omfattar högsta ledningen
> - identifierade interna processer som är otillräckliga avseende rapporteringen och kommunikationen av brister som har noterats av internrevisionen
> - tidigare kommunicerade brister som inte rättas till av ledningen inom rimlig tid
> - om ledningen inte hanterar väsentliga risker, t.ex. genom att inte införa kontroller avseende väsentliga risker, och
> - rättelser av tidigare publicerade finansiella rapporter.

Identifiera och bedöma riskerna för väsentliga felaktigheter (se punkt 28–37)

Varför revisorn identifierar och bedömer riskerna för väsentliga felaktigheter

A184. Risker för väsentliga felaktigheter identifieras och bedöms av revisorn för att avgöra art, tidpunkter och omfattning av de fortsatta granskningsåtgärder som krävs för att inhämta tillräckliga och ändamålsenliga revisionsbevis. Dessa bevis gör det möjligt för revisorn att uttala sig om de finansiella rapporterna med en acceptabelt låg nivå för revisionsrisk.

A185. Information som har inhämtats under riskbedömningen används som revisionsbevis för att lägga grunden till identifieringen och bedömningen av riskerna för väsentliga felaktigheter. Till exempel används information som har samlats in när revisorn bedömer utformningen av de identifierade kontrollerna och avgör om dessa kontroller har införts i kontrollaktivitetskomponenten som revisionsbevis för att stödja riskbedömningen. Sådana bevis utgör också en grund för revisorn för att utforma övergripande åtgärder för att hantera de bedömda riskerna för väsentliga felaktigheter på rapportnivån, samt för att utforma och genomföra fortsatta granskningsåtgärder vilkas art, tidpunkter och omfattning innebär en hantering av de bedömda riskerna för väsentliga felaktigheter på påståendenivån, enligt ISA 330.

Identifiera risker för väsentliga felaktigheter (se punkt 28)

A186. Identifieringen av risker för väsentliga felaktigheter genomförs före beaktandet av eventuella relaterade kontroller (dvs. inneboende risker), och grundar sig på revisorns preliminära bedömning

---

[47] ISA 265, *Kommunikation om brister i den interna kontrollen till dem som har ansvar för företagets styrning och företagsledningen*, punkt 8

[48] ISA 265, punkterna A6–A7 anger tecken på betydande brister, och frågor att överväga för att avgöra om en brist, eller en kombination av brister, i den interna kontroller utgör en betydande brist.

av felaktigheter som har en rimlig möjlighet både att uppkomma och att vara väsentliga om de skulle uppkomma.[49]

A187. Att identifiera riskerna för väsentliga felaktigheter lägger också grunden till revisorns beslut om relevanta påståenden, vilket hjälper revisorn att fatta beslut om väsentliga transaktionsslag, konton och upplysningar.

Påståenden

Varför revisorn använder påståenden

A188. När revisorn identifierar och bedömer riskerna för väsentliga felaktigheter använder han eller hon påståenden för att beakta de olika typerna av potentiella felaktigheter som kan uppstå. Påståenden för vilka revisorn har identifierat relaterade risker för väsentliga felaktigheter är relevanta påståenden.

Användning av påståenden

A189. När revisorn identifierar och bedömer riskerna för väsentliga felaktigheter kan han eller hon använda de kategorier av påståenden som beskrivs i punkt A190(a)–(b) nedan eller uttrycka dem annorlunda förutsatt att alla aspekter som beskrivs nedan täcks. Revisorn kan välja att kombinera påståendena om transaktionsslag och händelser samt tillhörande upplysningar med påståendena om konton samt tillhörande upplysningar.

A190. Påståenden som revisorn använder när han eller hon beaktar de olika typerna av potentiella felaktigheter som kan uppstå kan delas in i följande kategorier:

(a) Påståenden om transaktionsslag och händelser samt tillhörande upplysningar för den räkenskapsperiod som omfattas av revisionen:

(i) Förekomst – transaktioner och händelser som har redovisats, eller om vilka upplysning lämnats, har inträffat och dessa transaktioner och händelser hänför sig till företaget.

(ii) Fullständighet – alla transaktioner och händelser som ska ha bokförts har också bokförts och alla tillhörande upplysningar som ska tas med i de finansiella rapporterna har tagits med.

(iii) Riktighet – belopp och andra data som rör de redovisade transaktionerna och händelserna har bokförts korrekt och tillhörande upplysningar är riktigt beskrivna och värden anges korrekt.

(iv) Avklipp – transaktioner och händelser har bokförts under rätt räkenskapsperiod.

(v) Klassificering – transaktioner och händelser har bokförts på rätt konton.

(vi) Presentation – transaktioner och händelser är korrekt sammanslagna eller uppdelade samt tydligt beskrivna. Tillhörande upplysningar är relevanta och begripliga mot bakgrund av kraven i det tillämpliga ramverket för finansiell rapportering.

[49] ISA 200, punkt A15a

(b) Påståenden om saldon och tillhörande upplysningar vid räkenskapsperiodens slut:

(i) Existens – tillgångar, skulder och ägarintressen existerar.

(ii) Rättigheter och förpliktelser – företaget innehar eller kontrollerar rättigheterna till tillgångarna, och skulderna är företagets ansvar.

(iii) Fullständighet – alla tillgångar, skulder och ägarintressen som ska bokföras har också bokförts och alla tillhörande upplysningar som ska tas med i de finansiella rapporterna har tagits med.

(iv) Riktighet, värdering och allokering – tillgångar, skulder och ägarintressen har tagits upp till korrekta belopp i de finansiella rapporterna och eventuella justeringar av värderingar eller allokeringar har bokförts på lämpligt sätt. Tillhörande upplysningar är riktigt beskrivna och värden anges korrekt.

(v) Klassificering – tillgångar, skulder och ägarintressen redovisas i rätt post i balans- och resultaträkningen.

(vi) Presentation – tillgångar, skulder och ägarintressen är korrekt sammanslagna eller uppdelade samt tydligt beskrivna. Tillhörande upplysningar är relevanta och begripliga mot bakgrund av kraven i det tillämpliga ramverket för finansiell rapportering.

A191. De påståenden som beskrivs i punkt A190(a)–(b) ovan, anpassade efter vad som är tillämpligt, kan också användas av revisorn när han eller hon överväger de olika typerna av felaktigheter som kan finnas i upplysningarna och som inte har direkt koppling till bokförda transaktionsslag, händelser eller konton.

> **Exempel**:
>
> Ett exempel på den typen av upplysning inkluderar när det kan finnas krav på att företaget enligt det tillämpliga ramverket för finansiell rapportering beskriver sin exponering för risker till följd av finansiella instrument, däribland hur riskerna uppstår; mål, riktlinjer och rutiner för hantering av riskerna samt de metoder som används för att mäta riskerna.

Överväganden som särskilt gäller företag inom den offentliga sektorn

A192. När företagsledningen i företag inom den offentliga sektorn gör påståenden om de finansiella rapporterna kan företagsledningen, utöver de påståenden som anges i punkt A190(a)–(b), ofta påstå att transaktioner eller händelser har utförts enligt lagar eller andra författningar. Sådana påståenden kan ligga inom omfattningen och inriktningen för en revision av finansiella rapporter.

Risker för väsentliga felaktigheter på rapportnivån (se punkt 28(a) och 30)

Varför revisorn identifierar och bedömer riskerna för väsentliga felaktigheter på rapportnivån

A193. Revisorn identifierar riskerna för väsentliga felaktigheter på rapportnivån för att fastställa om riskerna genomsyrar de finansiella rapporterna och därmed skulle kräva ett övergripande svar enligt ISA 330.[50]

A194. Därutöver kan risker för väsentliga felaktigheter på rapportnivån även påverka enskilda påståenden, och att identifiera dessa risker kan hjälpa revisorn att bedöma risker för väsentliga felaktigheter på påståendenivån, och när han eller hon utformar fortsatta granskningsåtgärder för att hantera de identifierade riskerna.

Identifiera och bedöma riskerna för väsentliga felaktigheter på rapportnivån

A195. Risk för väsentliga felaktigheter på rapportnivån hänför sig till risker som genomsyrar de finansiella rapporterna som helhet och kan påverka många påståenden. Den här typen av risker är inte nödvändigtvis risker som kan kopplas till särskilda påståenden på transaktionsslags-, konto- eller upplysningsnivåerna (t.ex. risk för att ledningen sätter sig över kontrollerna). De utgör snarare omständigheter som kan höja riskerna för väsentliga felaktigheter på påståendenivån. Revisorns utvärdering av huruvida identifierade risker allmänt skulle kunna påverka de finansiella rapporterna stödjer revisorns bedömning av risker för väsentliga felaktigheter på rapportnivån. I andra fall kan också ett antal påståenden identifieras som känsliga för denna risk, och kan därför påverka revisorns riskidentifiering och bedömning av riskerna för väsentliga felaktigheter på påståendenivån.

> **Exempel**:
>
> Företaget står inför rörelseförluster och likviditetsproblem och är beroende av finansiering som ännu inte har säkrats. Under sådana omständigheter kan revisorn fastställa att upprättande av finansiella rapporter enligt fortlevnadsprincipen ger upphov till en risk för väsentliga felaktigheter på rapportnivån. I den situationen kan ramverket för den finansiella rapporteringen behöva tillämpas med hjälp av en likvidationsvärdering, vilket på ett avgörande sätt skulle påverka alla påståenden.

A196. Revisorns identifiering och bedömning av risker för väsentliga felaktigheter på rapportnivån påverkas av revisorns förståelse av företagets system för intern kontroll, i synnerhet revisorns förståelse av kontrollmiljön, företagets riskbedömning samt företagets process för att övervaka systemet för intern kontroll, och

- utfallet av de hänförliga utvärderingar som krävs enligt punkterna 21(b), 22(b), 24(c) och 25(c), och
- eventuella brister i kontrollerna som identifieras enligt punkt 27.

Särskilt risker på rapportnivån kan uppkomma genom brister i kontrollmiljön eller från yttre händelser eller faktorer såsom en vikande konjunktur.

[50] ISA 330, punkt 5

A197. Risker för väsentliga felaktigheter till följd av oegentligheter kan vara särskilt relevanta när revisorn ska bedöma riskerna för väsentliga felaktigheter på rapportnivån.

> **Exempel**:
>
> Revisorn förstår av frågor till ledningen att företagets finansiella rapporter ska användas vid diskussioner med långivare för att säkra ytterligare finansiering för att upprätthålla rörelsekapitalet. Revisorn kan därmed dra slutsatsen att det föreligger en större känslighet för felaktigheter till följd av riskfaktorer för oegentligheter som påverkar de inneboende riskerna (dvs. att de finansiella rapporterna är känsliga för väsentliga felaktigheter på grund av risken för bedräglig finansiell rapportering, såsom för högt redovisade tillgångar och intäkter och för lågt redovisade skulder och kostnader, för att säkra att finansieringen kan erhållas).

A198. Revisorns förståelse, inklusive de tillhörande utvärderingarna, av kontrollmiljön och andra komponenter i systemet för intern kontroll kan leda till tvivel när det gäller revisorns förmåga att inhämta revisionsbevis på vilka han eller hon kan grunda sitt uttalande i revisors rapport eller vara orsak till att avgå från uppdraget, där detta är möjligt enligt tillämplig lag eller annan författning.

> **Exempel**:
>
> - Som ett resultat av att revisorn utvärderar företagets kontrollmiljö, har revisorn farhågor rörande företagsledningens hederlighet, vilka kan vara så allvarliga att revisorn drar slutsatsen att risken för att företagsledningen avsiktligen har lämnat felaktig information i de finansiella rapporterna är så hög att en revision inte kan utföras.
> - Som ett resultat av sin utvärdering av företagets informationssystem och kommunikation fastställer revisorn att betydande ändringar i IT-miljön har skötts illa, med liten översyn från ledning och styrelse. Revisorn kommer till slutsatsen att det finns anledning till betydande oro i fråga om skicket på och tillförlitligheten hos företagets räkenskapsmaterial. Under sådana omständigheter kan revisorn dra slutsatsen att det är osannolikt att tillräckliga och ändamålsenliga revisionsbevis kommer att finnas tillgängliga för att stödja ett omodifierat uttalande om de finansiella rapporterna.

A199. ISA 705 (omarbetad)[51] fastställer krav för och ger vägledning när revisorn ska avgöra om han eller hon behöver uttala sig med reservation eller avstå från att uttala sig eller, vilket kan krävas i vissa fall, om han eller hon ska avgå från uppdraget, där detta är möjligt enligt tillämplig lag eller annan författning.

Överväganden som särskilt gäller företag inom den offentliga sektorn

A200. För företag inom den offentliga sektorn kan identifieringen av risker på rapportnivån omfatta överväganden av frågor hänförliga till känslighet för det politiska klimatet, offentliga intressen och program.

---

[51] ISA 705 (omarbetad), *Modifierat uttalande i rapport från oberoende revisor*

Risker för väsentliga felaktigheter på påståendenivån (se punkt 28(b))

> **Bilaga 2** ger exempel inom området för inneboende riskfaktorer, på händelser eller omständigheter som kan tyda på att känsligheten för felaktigheter kan vara väsentlig.

A201. Risker för väsentliga felaktigheter som inte genomgripande påverkar de finansiella rapporterna utgör risker för väsentliga felaktigheter på påståendenivån.

Relevanta påståenden samt betydande transaktionsslag, konton och upplysningar (se punkt 29)

Varför relevanta påståenden samt betydande transaktionsslag, konton och upplysningar fastställs

A202. Att fastställa relevanta påståenden samt betydande transaktionsslag, konton och upplysningar utgör grunden för omfattningen av revisorns förståelse av företagets informationssystem som måste inhämtas enligt punkt 25(a). Denna förståelse kan även hjälpa revisorn att identifiera och bedöma riskerna för väsentliga felaktigheter (se A86).

Automatiserade verktyg och tekniker

A203. Revisorn kan använda automatiserade tekniker som hjälp för att identifiera betydande transaktionsslag, konton och upplysningar.

> **Exempel**:
>
> - En hel population av transaktioner kan analyseras med hjälp av automatiserade verktyg och tekniker för att förstå deras karaktär, källa, storlek och omfattning. Revisorn kan genom att tillämpa automatiserade tekniker till exempel identifiera att ett konto med nollsaldo vid periodens utgång består av ett stort antal kvittningstransaktioner och bokföringsposter som har bokförts under perioden, som visar att kontosaldot eller transaktionsslaget kan vara betydande (t.ex. ett avräkningskonto för löneutbetalningar). Samma avräkningskonto för löneutbetalningar kan också identifiera kostnadsersättningar till ledningen (och andra anställda), som skulle kunna utgöra en betydande upplysning eftersom dessa utbetalningar har gjort till närstående.
> - Revisorn kan genom att analysera flödena i en hel grupp intäktstransaktioner lättare identifiera ett betydande transaktionsslag som inte har identifierats tidigare.

Upplysningar som kan vara betydande

A204. Betydande upplysningar omfattar både kvantitativa och kvalitativa upplysningar för vilka det finns ett eller flera relevanta påståenden. Exempel på upplysningar som har kvalitativa aspekter och för vilka det kan finnas relevanta påståenden och som därmed kan betraktas som betydande av revisorn omfattar upplysningar om följande:

- likviditet och avtalsvillkor för skulder för ett företag med ekonomiska problem
- händelser eller omständigheter som har lett till att en nedskrivning redovisas
- huvudsakliga källor till osäkerhet i uppskattningar, däribland antaganden om framtiden

- karaktären på en ändring i redovisningsprincip och andra relevanta upplysningar som krävs i det tillämpliga ramverket för finansiell rapportering, där t.ex. nya rapporteringskrav väntas ha en betydande effekt på företagets finansiella ställning och resultat
- avtal om aktierelaterade ersättningar, däribland information om hur eventuella redovisade belopp fastställdes samt andra relevanta upplysningar
- närstående och transaktioner med närstående
- känslighetsanalys, innefattande effekterna av ändringar i antaganden som används i företagets värderingstekniker, som ska göra det möjligt för användarna att förstå den underliggande osäkerheten i beräkningen av ett redovisat belopp eller belopp om vilket upplysning lämnas.

Bedöma risker för väsentliga felaktigheter på påståendenivån

Bedöma inneboende risker (se punkt 31–33)

Bedöma sannolikheten för och storleken på felaktigheter (se punkt 31)

Varför revisorn bedömer sannolikheten för och storleken på felaktigheter

A205. Revisorn bedömer sannolikheten för och omfattningen av felaktigheterna för identifierade risker för väsentliga felaktigheter eftersom kombinationen av sannolikheten för att en felaktighet uppstår och storleken på den möjliga felaktigheten om den skulle uppkomma avgör var i spektrumet av inneboende risker som den identifierade risken bedöms återfinnas, vilket ligger till grund för revisorns utformning av fortsatta granskningsåtgärder för att hantera risken.

A206. Att bedöma den inneboende risken för väsentliga felaktigheter hjälper också revisorn att fastställa betydande risker. Revisorn fastställer betydande risker eftersom det krävs specifika motåtgärder för betydande risker enligt ISA 330 och andra ISA-standarder.

A207. Inneboende riskfaktorer påverkar revisorns bedömning av sannolikheten för och storleken på identifierade risker för väsentliga felaktigheter på påståendenivån. I ju högre grad ett transaktionsslag, ett konto eller en upplysning är känslig för väsentliga felaktigheter, desto högre är sannolikt bedömningen av inneboende risk. Att bedöma i vilken grad inneboende riskfaktorer påverkar hur känsligt ett påstående är för felaktigheter hjälper revisorn att på ett korrekt sätt avgöra inneboende risker för väsentliga felaktigheter på påståendenivån och utforma en mer precis motåtgärd för sådana risker.

Spektrum av inneboende risker

A208. När revisorn bedömer den inneboende risken använder han eller hon sitt professionella omdöme för att fastställa betydelsen av kombinationen av sannolikheten för och storleken på en felaktighet.

A209. Den bedömda inneboende risken avseende en särskild risk för väsentliga felaktigheter på påståendenivån utgör en bedömning inom ett spann, från lägre till högre, inom spektrumet av inneboende risker. Bedömningen om var i spannet den inneboende risken ligger kan variera beroende på företagets karaktär, storlek och komplexitet, och beaktar den bedömda sannolikheten för och storleken på felaktigheterna och de inneboende riskfaktorerna.

A210. När revisorn överväger sannolikheten för felaktigheter beaktar han eller hon möjligheten att felaktigheter kan uppkomma baserat på utvärderingen av de inneboende riskfaktorerna.

A211. När revisorn överväger storleken på felaktigheterna tar han eller hon i beaktande de kvalitativa och kvantitativa aspekterna på de möjliga felaktigheterna (dvs. felaktigheter i påståenden avseende transaktionsslag, konton eller upplysningar kan bedömas vara väsentliga på grund av storlek, art eller omständigheter).

A212. Revisorn använder betydelsen av kombinationen av sannolikheten för och storleken på en väsentlig felaktighet när han eller hon avgör var i spektrumet av inneboende risker (dvs. intervallet) som den inneboende risken bedöms ligga. Ju högre kombination av sannolikhet och storlek, desto högre bedömning av den inneboende risken, och ju lägre kombination av sannolikhet och storlek, desto lägre bedömning av den inneboende risken.

A213. För att en risk ska bedömas som högre i spektrumet av inneboende risker krävs inte att både storleken och sannolikheten behöver bedömas som höga. Det är snarare kombinationen av storleken på och sannolikheten för väsentliga felaktigheter i spektrumet av inneboende risker som avgör om den bedömda inneboende risken är högre eller lägre i spektrumet av inneboende risker. En högre inneboende risk kan också uppkomma genom olika kombinationer av sannolikhet och storlek. En högre bedömning av inneboende risker skulle till exempel kunna komma sig av en lägre sannolikhet men en mycket hög storlek.

A214. För att kunna utveckla lämpliga strategier för att svara på risker för väsentliga felaktigheter kan revisorn dela in risker för väsentliga felaktigheter inom kategorier längs spektrumet av inneboende risker, baserat på sin bedömning av de inneboende riskerna. Dessa kategorier kan beskrivas på olika sätt. Oavsett vilken metod som används för kategorisering, är revisorns bedömning av inneboende risker ändamålsenlig när utformningen och genomförandet av fortsatta granskningsåtgärder för att hantera identifierade risker för väsentliga felaktigheter på påståendenivån är lämpligt svarande mot bedömningen av de inneboende riskerna och skälen till den bedömningen.

Övergripande risker för väsentliga felaktigheter på påståendenivån (se punkt 31(b))

A215. När revisorn bedömer risker för väsentliga felaktigheter på påståendenivån kan han eller hon dra slutsatsen att vissa av riskerna för väsentliga felaktigheter genomgripande påverkar de finansiella rapporterna som helhet och potentiellt påverkar många påståenden. Då kan revisorn uppdatera sin identifiering av väsentliga felaktigheter på rapportnivån.

A216. I de fall där risker för väsentliga felaktigheter identifieras som risker på rapportnivån till följd av sin genomgripande påverkan på ett antal påståenden, och kan kopplas till specifika påståenden, måste revisorn ta de riskerna i beaktande när han eller hon bedömer den inneboende risken för väsentliga felaktigheter på påståendenivån.

Överväganden som särskilt gäller företag inom den offentliga sektorn

A217. När revisorer inom den offentliga sektorn använder sitt professionella omdöme gällande risken för väsentliga felaktigheter kan de beakta komplexiteten i författningar och direktiv, och riskerna för överträdelser av myndigheternas bestämmelser.

Betydande risk (se punkt 32)

Varför betydande risker fastställs och vad det innebär för revisionen

A218. Fastställandet av betydande risker ger revisorn möjlighet att rikta större uppmärksamhet mot de risker som ligger i den övre delen av spektrumet av inneboende risker, genom att utföra vissa obligatoriska motåtgärder, däribland följande:

- Kontroller som hanterar betydande risker måste identifieras i enlighet med punkt 26(a)(i), med krav på att utvärdera om kontrollen har utformats på ett ändamålsenligt sätt och införts i enlighet med punkt 26(d).
- ISA 330 kräver att kontroller som hanterar betydande risker ska prövas under den aktuella perioden (när revisorn avser att förlita sig på att sådana kontroller fungerar) och substansgranskningsåtgärder ska planeras och genomföras som är specifikt avsedda som svar på den identifierade betydande risken.[52]
- ISA 330 kräver att revisorn inhämtar mer avgörande revisionsbevis ju högre revisorns bedömning av risken är.[53]
- ISA 260 (omarbetad) kräver kommunikation med styrelsen om de betydande risker som identifieras av revisorn.[54]
- ISA 701 kräver att revisorn beaktar betydande risker när han eller hon avgör de frågor som krävde revisorns särskilda uppmärksamhet, vilket är frågor som kan utgöra särskilt betydelsefulla områden.[55]
- En genomgång av revisionsdokumentationen vid rätt tidpunkt av den ansvariga revisorn vid lämpliga stadier under revisionen medger att viktiga frågor, inklusive betydande risker, kan lösas i rätt tid på ett sätt som den ansvariga revisorn finner nöjaktigt senast per datumet för revisionsberättelsen.[56]
- ISA 600 kräver större engagemang från koncernens ansvariga revisor om den betydande risken avser en enhet i en koncernrevision och att koncernens uppdragsteam ska styra det behövliga arbete som enhetsrevison utför på enheten.[57]

Fastställa betydande risker

A219. När revisorn fastställer betydande risker kan han eller hon först identifiera de bedömda risker för väsentliga felaktigheter som har bedömts som högre på spektrumet av inneboende risker för att utgöra grunden till att överväga vilka risker som kan ligga nära den översta delen. Vad som är nära den översta delen av spektrumet av inneboende risker skiljer sig från ett företag till ett annat, och är

---

52 ISA 330, punkterna 15 och 21

53 ISA 330, punkt 7(b)

54 ISA 260 (omarbetad), punkt 15

55 ISA 701, *Kommunikation om särskilt betydelsefulla områden i rapport från oberoende revisor*, punkt 9

56 ISA 220, punkterna 17 och A19

57 ISA 600, punkterna 30 och 31

inte nödvändigtvis samma för ett företag från period till period. Det kan bero på karaktären på och omständigheterna för det företag för vilket risken bedöms.

A220. Fastställandet av vilka av de bedömda riskerna för väsentliga felaktigheter som är nära den översta delen av spektrumet av inneboende risker, och som därmed utgör betydande risker, är en fråga om professionellt omdöme, såvida inte risken är av en typ som har specificerats för att behandlas som en betydande risk enligt kraven i andra standarder. ISA 240 fastställer ytterligare krav och ger vägledning om hur risker för väsentliga felaktigheter som beror på oegentligheter skall identifieras och behandlas.[58]

Exempel:

- Kontanter hos en detaljhandlare på en stormarknad skulle vanligtvis bedömas som om det fanns en hög sannolikhet för möjliga felaktigheter (på grund av risken för att kontanterna stjäls), men beloppen är normalt sett mycket låga (på grund av de låga nivåerna av kontanter som hanteras i butikerna). Kombinationen av dessa två faktorer på spektrumet av inneboende risker resulterar sannolikt inte i att förekomsten av kontanter fastställs som en betydande risk.
- Ett företag deltar i förhandlingar om att sälja ett affärssegment. Revisorn överväger effekten på nedskrivningen av goodwill, och kan fastställa att det finns en större sannolikhet för möjliga felaktigheter och högre belopp på grund av påverkan av inneboende riskfaktorer avseende subjektivitet, osäkerhet och känslighet för partiskhet i ledningen eller andra riskfaktorer för oegentligheter. Det kan leda till att behovet av nedskrivning av goodwill anses vara en betydande risk.

A221. Revisorn beaktar också de relativa effekterna av inneboende riskfaktorer när han eller hon bedömer de inneboende riskerna. Ju lägre effekten av inneboende riskfaktorer, desto lägre blir sannolikt den bedömda risken. Risker för väsentliga felaktigheter som kan bedömas som att de har en högre inneboende risk och därmed kan anses utgöra en betydande risk kan föreligga vid följande omständigheter:

- transaktioner för vilka det finns flera olika godtagbara sätt att redovisa så att subjektivitet är inblandad
- uppskattningar i redovisningen som innefattar ett stort mått av osäkerhet eller komplexa modeller
- komplexitet i insamling och bearbetning av data som underlag för kontosaldon
- konton eller kvantitativa upplysningar som baseras på komplexa beräkningar
- redovisningsprinciper som kan vara föremål för olika tolkningar
- förändringar i företagets verksamhet som innebär ändringar av redovisningen, t.ex. sammanslagningar och förvärv.

[58] ISA 240, punkterna 26–28

Risker för vilka inte enbart substansgranskningar utgör tillräckliga och ändamålsenliga revisionsbevis (se punkt 33)

Varför risker för vilka enbart substansgranskningar inte utgör tillräckliga och ändamålsenliga revisionsbevis måste identifieras

A222. På grund av karaktären på en risk för väsentliga felaktigheter, och de kontrollaktiviteter som hanterar den risken, är under vissa omständigheter det enda sättet att inhämta tillräckliga och ändamålsenliga revisionsbevis att granska kontrollernas funktion. Följaktligen finns det ett krav på revisorn att identifiera sådana risker på grund av betydelsen för utformningen och genomförandet av fortsatta granskningsåtgärder enligt ISA 330 för att hantera risker för väsentliga felaktigheter på påståendenivån.

A223. Punkt 26(a)(iii) kräver också att revisorn identifierar kontroller som hanterar risker där enbart substansgranskning inte kan inhämta tillräckliga och ändamålsenliga revisionsbevis eftersom revisorn enligt ISA 330[59] måste utforma och genomföra tester av sådana kontroller.

Att fastställa för vilka risker enbart substansgranskning inte utgör tillräckliga och ändamålsenliga revisionsbevis

A224. När rutinmässiga affärstransaktioner är föremål för en i hög grad automatiserad bearbetning med endast liten manuell hantering eller ingen manuell hantering alls, kanske det inte går att enbart utföra substansgranskningar för att hantera risken. Detta kan vara fallet i situationer där en betydande del av ett företags information initieras, registreras, bearbetas eller rapporteras endast i elektronisk form i ett informationssystem som inbegriper en hög grad av integrationen mellan de olika IT-applikationerna. I sådana fall gäller följande:

- Revisionsbevis kanske enbart finns i elektronisk form och deras tillräcklighet och ändamålsenlighet beror vanligtvis på hur effektiva kontrollerna av riktighet och fullständighet är.
- Om lämpliga kontroller inte fungerar kan det hända att information initieras felaktigt eller ändras, utan att detta upptäcks.

> **Exempel**:
>
> Det är vanligtvis inte möjligt att inhämta tillräckliga och ändamålsenliga revisionsbevis hänförliga till intäkter för ett telekommunikationsföretag enbart baserat på substansgranskning. Det beror på att bevisen för samtals- eller dataaktivitet inte existerar i en form som är observerbar. I stället genomförs vanligen omfattande granskning av kontroller för att fastställa att inledandet och avslutandet av samtal samt dataaktivitet har dokumenterats på ett korrekt sätt (t.ex. hur många minuter ett samtal pågår eller volymerna av en nedladdning) och redovisats korrekt i företagets faktureringssystem.

[59] ISA 330, punkt 8

A225. ISA 540 (omarbetad) ger vidare vägledning avseende uppskattningar i redovisningen avseende risker för vilka enbart substansgranskning inte ger tillräckliga och ändamålsenliga revisionsbevis.[60] Vad avser uppskattningar i redovisningen kanske detta inte begränsas till automatiserad bearbetning, utan kan också gå att tillämpa på komplexa modeller.

Bedöma kontrollrisken (se punkt 34)

A226. Revisorns planer på att testa kontrollernas funktion grundar sig på förväntningen att kontrollerna fungerar, och detta utgör grunden för revisorns bedömning av kontrollrisken. Den initiala förväntan på kontrollernas funktion grundar sig på revisorns utvärdering i kontrollaktivitetskomponenten av hur de identifierade kontrollerna har utformats och införts. Så snart revisorn har granskat kontrollernas funktion i enlighet med ISA 330 kommer han eller hon att kunna bekräfta sin initiala förväntan avseende kontrollernas funktion. Om kontrollerna inte fungerar så väl som revisorn hade förväntat sig, måste revisorn revidera bedömningen av kontrollrisken enligt punkt 37.

A227. Revisorns bedömning av kontrollrisken kan genomföras på olika sätt beroende på vilka revisionstekniker eller -metoder han eller hon föredrar och kan uttryckas på olika sätt.

A228. Om revisorn planerar att granska kontrollernas funktion kan det vara nödvändigt att granska en kombination av kontroller för att bekräfta revisorns förväntningar på att kontrollerna fungerar. Revisorn kan planera att granska både direkta och indirekta kontroller, inklusive allmänna IT-kontroller, och i sådana fall beakta den kombinerade förväntade effekten av kontrollerna när han eller hon bedömer kontrollrisken. I den mån som den kontroll som ska granskas inte till fullo hanterar den bedömda inneboende risken fastställer revisorn påverkan på utformningen av ytterligare granskningsåtgärder för att minska revisionsrisken till en godtagbart låg nivå.

A229. När revisorn planerar att granska funktionen hos en automatiserad kontroll kan han eller hon också planera att granska funktionen hos de relevanta allmänna IT-kontroller som utgör en förutsättning för den fortsatta funktionen för den automatiserade kontrollen att hantera de IT-relaterade riskerna, samt utgöra grunden till revisorns förväntan att den automatiserade kontrollen fungerade under hela perioden. När revisorn förväntar sig att relaterade generella IT-kontroller inte fungerar kan denna förväntan påverka revisorns bedömning av kontrollrisken på påståendenivån och revisorns fortsatta granskningsåtgärder kan behöva omfatta substansgranskning för att hantera de tillämpliga IT-relaterade riskerna. Vidare vägledning om de åtgärder som revisorn kan vidta i dessa fall återfinns i ISA 330.[61]

Utvärdera revisionsbevisen inhämtade från riskbedömningen (se punkt 35)

Varför revisorn utvärderar de revisionsbevis som inhämtas från riskbedömningen

A230. Revisionsbevis inhämtade från riskbedömningen är grunden för identifieringen och bedömningen av riskerna för väsentliga felaktigheter. Detta lägger grunden till revisorns utformning av art, tidpunkter och omfattning av fortsatta granskningsåtgärder som hanterar de hänförliga bedömda riskerna för väsentliga felaktigheter, på påståendenivån, enligt ISA 330. Följaktligen utgör de revisionsbevis som

[60] ISA 540 (omarbetad), punkterna A87–A89

[61] ISA 330, punkterna A29–A30

har inhämtats från riskbedömningen en grund för att identifiera och bedöma risker för väsentliga felaktigheter, vare sig dessa beror på oegentligheter eller misstag, på rapport- och påståendenivåerna.

Utvärderingen av revisionsbevisen

A231. Revisionsbevis från riskbedömningen består både av information som stödjer och bekräftar ledningens påståenden, och all information som motsäger sådana påståenden.[62]

En professionellt skeptisk inställning

A232. Vid utvärderingen av revisionsbevisen från riskbedömningen överväger revisorn om en tillräcklig förståelse av företaget och dess miljö, det tillämpliga ramverket för finansiell rapportering och företagets system för intern kontroll har uppnåtts för att kunna identifiera riskerna för väsentliga felaktigheter, samt om det finns några bevis som är motsägelsefulla, vilket kan tyda på en risk för väsentliga felaktigheter.

Transaktionsslag, konton och upplysningar som inte är betydande, men som är väsentliga (se punkt 36)

A233. Enligt förklaring i ISA 320[63] övervägs väsentlighet och revisionsrisk när riskerna för väsentliga felaktigheter i transaktionsslag, konton och upplysningar identifieras och bedöms. Revisorns fastställande av väsentlighet är en fråga om professionell bedömning och påverkas av revisorns uppfattning om de behov av finansiell information som användare av de finansiella rapporterna har.[64] För denna standard och punkt 18 i ISA 330 är transaktionsslag, konton eller upplysningar väsentliga om utelämnad, felaktig eller otydlig information om dem rimligen kan förväntas påverka användarnas ekonomiska beslut fattade utifrån de finansiella rapporterna som helhet.

A234. Det kan finnas transaktionsslag, konton och upplysningar som är väsentliga men som inte har fastställts som betydande transaktionsslag, konton eller upplysningar (dvs. revisorns har inte identifierat några relevanta påståenden).

> **Exempel**:
>
> Företaget kan ha en upplysning om ersättningar till högsta ledningen för vilken revisorn inte har identifierat någon risk för väsentliga felaktigheter. Däremot kan revisorn fastställa att denna upplysning är väsentlig baserat på övervägandena i punkt A233.

A235. Granskningsåtgärder för att hantera transaktionsslag, konton eller upplysningar som är väsentliga men som inte bedöms vara betydande, behandlas i ISA 330.[65] När ett transaktionsslag, ett konto eller en upplysning anses vara betydande enligt kraven i punkt 29 är även transaktionsslaget, kontot eller upplysningen väsentlig enligt punkt 18 i ISA 330.

---

62 ISA 500, punkt A1

63 ISA 320, punkt A1

64 ISA 320, punkt 4

65 ISA 330, punkt 18

Ändring av riskbedömning (se punkt 37)

A236. Under revisionen kan revisorn få tillgång till ny eller annan information som skiljer sig betydligt från den information på vilken riskbedömningen grundades.

> **Exempel**:
>
> Riskbedömningen kan vara grundad på en förväntning om att vissa kontroller fungerar tillfredsställande. När dessa kontroller granskas kan revisorn få fram revisionsbevis som visar att de inte fungerade tillfredsställande vid relevanta tidpunkter under revisionen. På samma sätt kan revisorn i samband med substansgranskning upptäcka felaktiga belopp eller större förekomster av felaktigheter än vad som överensstämmer med revisorns riskbedömningar. Under sådana omständigheter kan det hända att riskbedömningen inte korrekt avspeglar de verkliga förhållandena i företaget och det kan hända att de planerade fortsatta granskningsåtgärderna inte på ett tillfredsställande sätt kan upptäcka väsentliga felaktigheter. Punkterna 16 och 17 i ISA 330 ger ytterligare vägledning om att utvärdera kontrollers funktion.

Dokumentation (se punkt 38)

A237. Vid återkommande revisioner kan viss dokumentation föras över till framtida perioder och om nödvändigt uppdateras för att avspegla förändringar i företagets verksamhet eller processer.

A238. ISA 230 noterar bland annat att även om det inte bara finns ett enda sätt att dokumentera hur revisorn utövar en professionellt skeptisk inställning, kan revisionsdokumentationen ändå visa att revisorn har haft en professionellt skeptisk inställning.[66] När till exempel revisionsbevisen inhämtade genom arbetet med riskbedömningen omfattar bevis som både understödjer och motsäger ledningens påståenden kan dokumentationen inkludera hur revisorn värderade bevisen, inklusive de professionella bedömningar som gjordes av huruvida revisionsbevisen ger en ändamålsenlig grund för revisorns identifiering och bedömning av riskerna för väsentliga felaktigheter. Exempel på andra krav i denna standard där dokumentationen kan ge bevis på att revisorn utövat en professionellt skeptisk inställning omfattar följande:

- Punkt 13, som kräver att revisorn ska utforma och genomföra sin riskbedömning på ett sätt som inte är partiskt för att inhämta revisionsbevis som kan stödja förekomsten av risker eller mot att exkludera revisionsbevis som kan motsäga förekomsten av risker.
- Punkt 17, som kräver en diskussion bland nyckelpersoner i uppdragsteamet om tillämpningen av det tillämpliga ramverket för finansiell rapportering och hur känsliga företagets finansiella rapporter är för väsentliga felaktigheter.
- Punkterna 19(b) och 20, som kräver att revisorn skaffar sig en förståelse av anledningarna till eventuella förändringar i företagets redovisningsprinciper och bedömer om företagets redovisningsprinciper är lämpliga och förenliga med det tillämpliga ramverket för finansiell rapportering.

[66] ISA 230, punkt A7

- Punkterna 21(b), 22(b), 23(b), 24(c), 25(c), 26(d) och 27, som kräver att revisorn bedömer, utifrån den nödvändiga förståelse som han eller hon har inhämtat, om komponenterna i företagets system för intern kontroll är lämpliga mot bakgrund av företagets omständigheter med beaktande av företagets karaktär och komplexitet, samt att han eller hon fastställer huruvida en eller fler brister i kontrollerna har identifierats.
- Punkt 35, som kräver att revisorn tar hänsyn till alla revisionsbevis som har inhämtats från riskbedömningen, vare sig de understödjer eller motsäger påståenden från ledningen, samt att han eller hon utvärderar huruvida revisionsbevisen inhämtade från riskbedömningen erbjuder en lämplig grund för identifieringen och bedömningen av riskerna för väsentliga felaktigheter, och
- Punkt 36, som kräver att revisorn i tillämpliga fall bedömer om revisorns slutsats att det inte finns några risker för väsentliga felaktigheter för ett väsentligt transaktionsslag, ett konto eller en upplysning fortfarande gäller.

Skalbarhet

A239. Revisorn får använda sitt professionella omdöme för att avgöra på vilket sätt kraven i punkt 38 ska dokumenteras.

A240. Mer detaljerad dokumentation, som är tillräcklig för att göra det möjligt för en erfaren revisor, som inte har någon tidigare erfarenhet av revisionen, att förstå art, tidpunkter och omfattning av de granskningsåtgärder som har genomförts, kan krävas för att visa logiken bakom gjorda svåra bedömningar.

A241. För revisionerna av mindre komplexa företag kan formen på och omfattningen av dokumentation vara enkel och relativt kortfattad. Formen på och omfattningen av revisorns dokumentation påverkas av arten, storleken och komplexiteten på företaget och dess system för intern kontroll, tillgången på information från företaget samt den granskningsmetod och -teknik som tillämpas under revisionen. Det är inte nödvändigt att dokumentera hela revisorns förståelse av företaget och angränsande frågor. Viktiga delar[67] av den förståelse som revisorn dokumenterar kan inbegripa sådana på vilken revisorn har grundat sin bedömning av risker för väsentliga felaktigheter. Revisorn behöver däremot inte dokumentera alla inneboende riskfaktorer som beaktades när han eller hon identifierade och bedömde riskerna för väsentliga felaktigheter på påståendenivån.

> **Exempel**:
>
> Vid revisioner av mindre komplexa företag kan dokumentationen av revisionen införlivas i revisorns dokumentation av den övergripande strategin och granskningsplanen.[68] På liknande sätt kan t.ex. resultaten av riskbedömningen dokumenteras separat eller dokumenteras som en del av revisorns dokumentation av fortsatta granskningsåtgärder.[69]

---

67 ISA 230, punkt 8

68 ISA 300, *Planering av revision av finansiella rapporter*, punkterna 7, 9 och A11

69 ISA 330, punkt 28

Bilaga 1

(Se punkt A61–A67)

Överväganden för att förstå företaget och dess affärsmodell

Denna bilaga beskriver målet med och omfattningen av företagets affärsmodell och ger exempel på omständigheter som revisorn kan beakta för att förstå aktiviteter i företaget som kanske ingår i affärsmodellen. Revisorns förståelse av företagets affärsmodell, och hur den påverkas av dess affärsstrategi och affärsmål, kan hjälpa revisorn att identifiera affärsrisker som kan påverka de finansiella rapporterna. Dessutom kan det hjälpa revisorn att identifiera risken för väsentliga felaktigheter.

Mål med och omfattning av ett företags affärsmodell

1. Ett företags affärsmodell beskriver hur ett företag betraktar t.ex. sin organisationsstruktur eller omfattningen av sina aktiviteter, verksamhetsgrenar (inklusive konkurrenter och kunder), processer, tillväxtmöjligheter, globalisering, krav enligt lagar och andra författningar samt teknik. Företagets affärsmodell beskriver hur företaget skapar, bibehåller och tar vara på finansiellt eller bredare värde, för sina intressenter.

2. Strategier är de sätt på vilka ledningen planerar att uppnå företagets mål, inklusive hur företaget planerar att hantera de risker och möjligheter som det ställs inför. Ett företags strategier ändras över tid av ledningen, för att svara mot förändringar i företagets mål samt i den interna och externa miljö i vilka verksamheten bedrivs.

3. En beskrivning av en affärsmodell omfattar vanligtvis följande:

    - Omfattningen av företagets aktiviteter och varför de bedrivs.
    - Företagets struktur och verksamhetens omfattning.
    - Marknaderna eller de geografiska eller demografiska områdena, samt delar av värdekedjan, där företaget bedriver verksamhet, hur det samverkar med dessa marknader eller områden (huvudsakliga produkter, kundsegment och distributionsmetoder) samt vilka företagets konkurrensfördelar och -nackdelar är.
    - Företagets verksamhets- eller rörelseprocesser (t.ex. processer för investeringar, finansieringsprocesser eller löpande processer) som används för att bedriva verksamheten, med fokus på de delar av affärsprocesserna som är viktiga för att skapa, bibehålla och ta vara på värde.
    - Resurserna (t.ex. finansiella resurser, personal, immateriella, miljömässiga och tekniska resurser) samt andra resurser och relationer (t.ex. kunder, konkurrenter, leverantörer och anställda) som är nödvändiga eller viktiga för företagets framgångar.
    - Hur företagets affärsmodell integrerar användning av IT i sina kontakter med kunder, leverantörer, långivare och andra intressenter genom IT-gränssnitt och andra tekniker.

4. En affärsrisk kan få omedelbara konsekvenser för risken för väsentliga felaktigheter när det gäller transaktionsslag, konton och upplysningar på påstående- eller rapportnivån. En affärsrisk som härrör från en betydande nedgång i marknadsvärdena på fastighetsmarknaden kan t.ex. öka risken för

väsentliga felaktigheter hänförliga till värderingspåståendet för en långivare av medelfristiga fastighetslån. Samma risk, framför allt i kombination med en svår lågkonjunktur som på samma gång ökar den underliggande risken för kreditförluster under lånens livslängd, kan emellertid också få konsekvenser på längre sikt. Den nettoexponering för kreditförluster som blir resultatet kan kasta betydande tvivel över företagets förmåga att fortsätta verksamheten. Om så är fallet skulle det kunna ha betydelse för ledningens, och revisorns, slutsats om företagets tillämpning av fortlevnadsprincipen vid upprättandet av de finansiella rapporterna, och fastställandet av om det föreligger en betydande osäkerhet. Om en affärsrisk kan leda till en risk för väsentliga felaktigheter beaktas därför mot bakgrund av företagets situation. Exempel på händelser och förhållanden som kan ge upphov till risk för väsentliga felaktigheter återfinns i **Bilaga 2**.

Företagets aktiviteter

5. Exempel på omständigheter som revisorn kan överväga när han eller hon gör sig en bild av företagets verksamhet (som ingår i företagets affärsmodell) inkluderar följande:

   (a) Affärsverksamhet, t.ex.:

   - karaktären på inkomstkällorna, varor eller tjänster, och marknaderna, bland annat elektronisk handel såsom internetförsäljning och marknadsföringsaktiviteter
   - hur verksamheten bedrivs (t.ex. produktionsstadier och produktionsmetoder eller aktiviteter som är utsatta för miljörisker)
   - allianser, samriskföretag och till andra utlagda aktiviteter
   - geografisk spridning och branschsegmentering
   - lokalisering av produktionsanläggningar, lagerlokaler och kontor samt varulagrens lokalisering och kvantiteter
   - viktiga kunder och viktiga leverantörer av varor och tjänster, anställningsformer (däribland förekomsten av kollektivavtal, pensioner och andra förmåner efter avslutad anställning, aktie- och bonusbaserade incitamentsprogram samt offentlig reglering av anställningsfrågor)
   - aktivitet inom och utgifter för forskning och utveckling
   - transaktioner med närstående.

   (b) Investeringar och investeringsaktiviteter, t.ex.:

   - planerade eller nyligen gjorda förvärv eller avyttringar
   - investeringar i och avyttringar av värdepapper och lån
   - investeringar i anläggningstillgångar
   - investeringar i icke konsoliderade företag, bland annat partnersamarbeten utan bestämmande inflytande, samriskföretag och företag för särskilda ändamål utan bestämmande inflytande.

(c) Finansiering och finansieringsaktiviteter, t.ex.:

- ägarstruktur i större dotterföretag och intresseföretag, både konsoliderade och icke konsoliderade strukturer
- skuldstruktur och tillhörande villkor, inklusive finansieringsarrangemang utanför balansräkningen och leasingavtal
- verkliga ägare (t.ex. lokala och utländska och dessas renommé och erfarenhet) och närstående parter
- användning av derivatinstrument.

Karaktären på ”företag för särskilda ändamål”

6. Ett företag för särskilt ändamål (kallas ibland ett ”specialfordon”) är ett företag som i allmänhet bildas för ett smalt och väldefinierat syfte, t.ex. för att genomföra leasing eller värdepapperisering av finansiella tillgångar, eller för att utföra forsknings- och utvecklingsverksamhet. Det kan ha formen av ett bolag, en stiftelse, ett handelsbolag eller ett enkelt bolag. Företaget för vars räkning företaget för särskilt ändamål har skapats kan ofta överföra tillgångar till det senare (t.ex. som en del av en transaktion för att ta bort finansiella tillgångar från balansräkningen), skaffa sig rätten att använda det senare företagets tillgångar eller utföra tjänster åt det senare företaget, samtidigt som andra parter kan finansiera det senare företaget. Som ISA 550 anger kan ett företag för särskilt ändamål under vissa omständigheter vara en närstående part till företaget.[70]

7. Ramverk för finansiell rapportering anger ofta detaljerade villkor som kan anses innebära bestämmande inflytande eller omständigheter under vilka en konsolidering av företaget för särskilt ändamål bör övervägas. Tolkningen av kraven i sådana ramverk kräver ofta detaljerade kunskaper om de relevanta avtal som rör företaget för särskilt ändamål.

[70] ISA 550, punkt A7

Bilaga 2

(Se punkt 12(f), 19(c), A7–A8, A85–A89)

Förstå inneboende riskfaktorer

Denna bilaga ger ytterligare förklaringar av de inneboende riskfaktorerna och omständigheter som revisorn kan beakta för att förstå och använda de inneboende riskfaktorerna när han eller hon identifierar och bedömer riskerna för väsentliga felaktigheter på påståendenivån.

De inneboende riskfaktorerna

1. Inneboende riskfaktorer är egenskaper hos händelser eller förhållanden som påverkar hur känsligt ett påstående om ett transaktionsslag, ett konto eller en upplysning är för felaktigheter, vare sig dessa beror på oegentligheter eller misstag, före beaktandet av kontroller. Sådana faktorer kan vara kvalitativa eller kvantitativa, och omfattar komplexitet, subjektivitet, förändring, osäkerhet eller känslighet för felaktigheter till följd av bristande objektivitet hos företagsledningen eller andra riskfaktorer avseende oegentligheter[71] i den mån de påverkar den inneboende risken. När revisorn bildar sig en uppfattning om företaget och dess miljö samt det tillämpliga ramverket för finansiell rapportering och företagets redovisningsprinciper, enligt punkterna 19(a)–(b) förstår revisorn också hur de inneboende riskfaktorerna påverkar känsligheten i påståenden för felaktigheter vid upprättandet av de finansiella rapporterna.

2. Inneboende riskfaktorer avseende framtagandet av information som krävs enligt det tillämpliga ramverket för finansiell rapportering (kallas i detta avsnitt ”nödvändig information”) inkluderar följande:

   - *Komplexitet* uppkommer antingen från informationens karaktär eller på det sätt som den nödvändiga informationen tas fram, inklusive när det på grund av informationens karaktär är svårt att ta fram den. Komplexitet kan t.ex. uppkomma
     - vid beräkningen av avsättning för leverantörsrabatter, eftersom det kan vara nödvändigt att beakta olika kommersiella villkor hos många olika leverantörer, eller många sammanhängande kommersiella villkor som alla är relevanta för att beräkna de upplupna rabatter leverantörerna är berättigade till, eller
     - när det finns många potentiella datakällor, med olika egenskaper som används för att göra en uppskattning i redovisningen omfattar bearbetningen av dessa data många sammanlänkade steg, och därmed ligger det i sakens natur att informationen är svårare att identifiera, samla in, få åtkomst till, förstå eller bearbeta.
   - *Subjektivitet*—uppkommer från inneboende begränsningar i möjligheten att ta fram nödvändig information på ett objektivt sätt, på grund av begränsningar i tillgång på kunskap eller information, på så sätt att ledningen kan behöva göra ett val eller en subjektiv bedömning av den lämpliga metoden att använda och vilken resulterande information som bör tas med i de finansiella rapporterna. På grund av de olika metoderna för att ta fram den nödvändiga

[71] ISA 240, punkterna A24–A27

informationen skulle man kunna få olika resultat från en korrekt tillämpning av kraven i det tillämpliga ramverket för finansiell rapportering. När begränsningarna av kunskap eller data ökar kommer även subjektiviteten i bedömningarna som skulle kunna göras av rimligt insatta och oberoende personer, och mångfalden i de möjliga utfallen av dessa bedömningar, att öka.

- *Förändring*—är resultatet av händelser eller omständigheter som, över tid, påverkar företagets verksamhet eller ekonomiska, redovisningsmässiga, tillsynsmässiga, branschrelaterade eller andra aspekter på den miljö där företaget bedriver verksamhet, när effekterna av de händelserna eller omständigheterna återspeglas i den nödvändiga informationen. Sådana händelser eller omständigheter kan uppkomma under, eller mellan, finansiella rapporttidpunkter. Förändring kan t.ex. komma sig av utveckling av kraven i det tillämpliga ramverket för finansiell rapportering, eller i företaget och dess affärsmodell, eller i den miljö där verksamheten bedrivs. Sådana förändringar kan påverka ledningens antaganden och bedömningar, inklusive hur de är relaterade till ledningens val av redovisningsprinciper eller hur uppskattningar i redovisningen görs eller hur hänförliga upplysningar fastställs.
- *Osäkerhet*—uppkommer när den nödvändiga informationen inte kan tas fram enbart baserat på tillräckligt precis och omfattande data som går att verifiera genom direkta observationer. I sådana fall kan det krävas att man tillämpar en metod som använder den tillgängliga kunskapen utifrån tillräckligt precisa och omfattande observerbara data, i den mån sådana finns tillgängliga, samt rimliga antaganden stödda av de mest lämpliga data som finns tillgängliga, när observerbara data inte finns. Begränsningar i tillgången på kunskap eller data, som inte ligger inom ledningens kontroll (med förbehåll för kostnadsbegränsningar där det är tillämpligt) är källor till osäkerhet och deras effekt på framtagandet av den nödvändiga informationen kan inte elimineras. Osäkerhet i uppskattningarna uppstår t.ex. när det nödvändiga monetära beloppet inte kan fastställas med precision och utfallet av uppskattningen inte är känt före det datum när de finansiella rapporterna färdigställs.
- *Känslighet för felaktigheter till följd av bristande objektivitet hos företagsledningen eller andra riskfaktorer avseende oegentligheter i den mån de påverkar den inneboende risken*—känslighet för bristande objektivitet hos företagsledningen uppstår genom omständigheter som skapar en känslighet för ett avsiktligt eller oavsiktligt misslyckande från ledningen att förbli neutral när informationen tas fram. Bristande objektivitet hos ledningen är ofta förknippat med vissa omständigheter som har potential att ge upphov till att ledningen inte upprätthåller neutraliteten när den gör bedömningar (tecken på potentiell bristande objektivitet hos ledningen), vilket skulle kunna leda till väsentliga felaktigheter i informationen som, skulle vara bedräglig om den var avsiktlig. Sådana tecken inkluderar incitament eller påtryckningar i den mån som de påverkar inneboende risker (t.ex. som ett resultat av motivationen att uppnå ett önskat resultat, såsom ett önskat resultatmål eller en soliditet) och möjligheter att inte upprätthålla neutralitet. Faktorer relevanta för känsligheten för felaktigheter till följd av oegentligheter i form av bedräglig finansiell rapportering eller förskingring av tillgångar beskrivs i punkterna A1 till A5 i ISA 240.

3. När komplexiteten är en inneboende riskfaktor kan det finnas ett inbyggt behov av mer komplexa processer vid framtagandet av informationen, och sådana processer kan till sin natur vara svårare

att tillämpa. Detta kan leda till att tillämpningen kräver specialkompetens eller specialkunskaper och kan kräva att man använder sig av en specialist anlitad av företagsledningen.

4. När ledningens bedömning är mer subjektiv kan känsligheten för felaktigheter på grund av bristande objektivitet hos ledningen, vare sig den är oavsiktlig eller avsiktlig, också öka. Det kan t.ex. inbegripa betydande bedömningar från ledningen för att göra uppskattningar i redovisningen som har identifierats som att de är behäftade med en stor osäkerhet, och slutsatser gällande metoder, data och antaganden kan återspegla en oavsiktlig eller avsiktlig bristande objektivitet hos ledningen.

Exempel på händelser och förhållanden som kan ge upphov till förekomsten av risker för väsentliga felaktigheter

5. Nedan finns exempel på händelser (inklusive transaktioner) och förhållanden som kan tyda på att det finns risker för väsentliga felaktigheter i de finansiella rapporterna, på rapportnivån eller påståendenivån. Exemplen som ges för inneboende riskfaktorer täcker en rad olika händelser och omständigheter. Alla dessa händelser och omständigheter är dock inte relevanta för varje revisionsuppdrag och förteckningen över exempel är inte nödvändigtvis uttömmande. Händelserna och omständigheterna har kategoriserats utifrån den inneboende riskfaktor som kan ha den största effekten under omständigheterna. Viktigt att notera är att på grund av det inbördes sambandet mellan de inneboende riskfaktorerna kan exemplen på händelser och omständigheter sannolikt vara föremål för, eller påverkas av, andra inneboende riskfaktorer i olika grad.

Relevanta inneboende riskfaktorer:	Exempel på händelser eller förhållanden som kan vara tecken på förekomsten av risker för väsentliga felaktigheter på påståendenivån:
Komplexitet	Regelverk: • Verksamheter som är föremål för en mycket komplex reglering. Affärsmodell: • Förekomsten av komplexa allianser och samriskföretag. Tillämpligt ramverk för finansiell rapportering: • Värderingar i redovisningen som inbegriper komplexa processer. Transaktioner: • Användning av finansiering utanför balansräkningen, företag för särskilt ändamål och andra komplexa finansieringsavtal.
Subjektivitet	Tillämpligt ramverk för finansiell rapportering: • En lång rad möjliga värderingskriterier för en uppskattning i redovisningen. T.ex. ledningens redovisning av avskrivningar eller byggnationsintäkter och -kostnader.

Relevanta inneboende riskfaktorer:	Exempel på händelser eller förhållanden som kan vara tecken på förekomsten av risker för väsentliga felaktigheter på påståendenivån:
	• Ledningens val av en värderingsteknik eller -modell för en anläggningstillgång, såsom förvaltningsfastigheter.
Förändring	Ekonomiska förhållanden: • Verksamheter i ekonomiskt instabila regioner, t.ex. länder med betydande valutadevalvering eller ekonomier med hög inflation. Marknader: • Verksamheter som är exponerade för volatila marknader, t.ex. handel med terminskontrakt. Förlust av kunder: • Frågor som rör fortsatt drift och likviditet, däribland förlust av betydelsefulla kunder. Branschmodell: • Förändringar i den bransch där företaget verkar. Affärsmodell: • Förändringar i varuförsörjningskedjan. • Utveckling eller tillhandahållande av nya varor eller tjänster, eller utvidgning till nya affärsområden. Geografi: • Expansion till nya platser. Företagsstruktur. • Förändringar i företaget såsom stora förvärv eller omorganisationer eller andra ovanliga händelser. • Företag eller affärssegment som troligtvis kommer att säljas. Personalkompetens: • Förändringar bland nyckelpersoner, däribland att personer i företagsledningen slutar. IT: • Förändringar i IT-miljön. • Installation av betydelsefulla nya IT-system för finansiell rapportering. Tillämpligt ramverk för finansiell rapportering:

Relevanta inneboende riskfaktorer:	Exempel på händelser eller förhållanden som kan vara tecken på förekomsten av risker för väsentliga felaktigheter på påståendenivån:
	• Tillämpning av nya redovisningsuttalanden. Kapital: • Nya begränsningar i fråga om tillgängligheten på kapital och krediter. Regelverk: • Påbörjande av utredningar från tillsynsorgan eller statliga organ av företagets verksamheter eller ekonomiska resultat. • Påverkan från ny lagstiftning hänförlig till miljöskydd.
Osäkerhet	Rapportering: • Händelser eller transaktioner som inbegriper en betydande grad av osäkerhet i värderingen, inklusive uppskattningar i redovisningen samt tillhörande upplysningar. • Icke avgjorda rättstvister och ansvarsförbindelser, t.ex. säljgarantier, ekonomiska garantier och miljöskulder.
Känslighet för felaktigheter till följd av bristande objektivitet hos företagsledningen eller andra riskfaktorer avseende oegentligheter i den mån de påverkar den inneboende risken	Rapportering: • Möjligheter för företagsledning och anställda att bedriva bedräglig finansiell rapportering, inklusive att utesluta, eller dölja, väsentlig information i upplysningarna. Transaktioner: • Betydande transaktioner med närstående parter. • Betydande antal av icke rutinmässiga eller icke-systematiska transaktioner, inklusive koncerninterna transaktioner och stora intäktstransaktioner vid räkenskapsperiodens slut. • Transaktioner som bokförs på grundval av företagsledningens avsikter, t.ex. refinansiering av skulder, tillgångar som ska säljas och klassificering av värdepapper.

Andra händelser eller förhållanden som kan tyda på risker för väsentliga felaktigheter på rapportnivån:

- Avsaknad av personal med rätt kompetens inom redovisning och finansiell rapportering.
- Brister i kontrollerna – i synnerhet i kontrollmiljön, riskbedömningsprocessen och processen för övervakning, och i synnerhet de brister som ledningen inte vidtar åtgärder mot.
- Tidigare felaktigheter, en historia av misstag eller ett betydande antal justeringar vid räkenskapsperiodens slut.

Bilaga 3

(Se punkt 12(m), 21–26, A90–A181)

Att förstå företagets system för intern kontroll

1. Företagets system för intern kontroll kan återspeglas i handböcker för riktlinjer och rutiner, system och blanketter och den information som finns inbäddad i dessa, och utförs av företagets personal. Företagets system för intern kontroll införs av ledningen, styrelsen och annan personal utifrån företagets struktur. Företagets system för intern kontroll kan tillämpas, grundat på beslut från ledning, styrelse eller annan personal och inom ramen för lagar och andra författningar, på företagets verksamhetsmodell, strukturen för den juridiska personen, eller en kombination av dessa.

2. I den här bilagan förklaras den interna kontrollens komponenter, samt dess begränsningar, som de beskrivs i punkterna 12(m), 21–26, and A90–A181, som de hänför sig till revision av finansiella rapporter.

3. Företagets system för intern kontroll innefattar aspekter som är hänförliga till företagets mål för den finansiella rapporteringen men det kan också innefatta aspekter som avser dess verksamhets- eller efterlevnadsmål, när sådana aspekter är relevanta för den finansiella rapporteringen.

> **Exempel**:
>
> Kontroller över efterlevnad av lagar och andra författningar kan också vara relevanta för den finansiella rapporteringen när sådana kontroller är relevanta när företaget tar fram upplysningar om eventualförpliktelser i de finansiella rapporterna.

Komponenterna i företagets system för intern kontroll

Kontrollmiljön

4. I kontrollmiljön ingår styr- och ledningsfunktioner samt styrelsens och företagsledningens inställning, medvetenhet och åtgärder beträffande företagets system för intern kontroll och dess betydelse i företaget. Kontrollmiljön anger tonen i en organisation, påverkar medarbetarnas medvetenhet om kontroller och lägger generellt grunden till driften av de andra komponenterna i företagets system för intern kontroll.

5. Ett företags kontrollmedvetande påverkas av styrelsen, eftersom en av styrelsens uppgifter är att uppväga det tryck på företagsledningen i fråga om finansiell rapportering, som kan uppstå till följd av krav från marknaden eller ersättningssystem. Hur väl styrelsens medverkan påverkar effektiviteten i utformningen av kontrollmiljön påverkas således av frågor som

   - dess oberoende från företagsledningen och dess förmåga att utvärdera företagsledningens åtgärder
   - huruvida styrelsen förstår företagets affärstransaktioner

- i vilken omfattning den bedömer huruvida de finansiella rapporterna har upprättats enligt det tillämpliga ramverket för finansiell rapportering, däribland huruvida de finansiella rapporterna innehåller adekvata upplysningar.

6. Kontrollmiljön består av följande delar:

(a) *Hur ledningen utövar sitt ansvar, såsom att skapa och upprätthålla företagets kultur och betona vikten av hederlighet och etiska värderingar.* Kontroller kan inte kompensera brist på hederlighet och etiska värderingar hos de människor som utvecklar, administrerar och övervakar dem. Hederlighet och etiskt agerande är resultatet av företagets etiska normer och normer för agerande eller uppförandekoder, hur de kommuniceras (t.ex. genom riktlinjer), och hur de följs upp i praktiken (t.ex. genom ledningens agerande för att eliminera eller minska motiv eller frestelser som kan förmå anställda att agera ohederligt, olagligt eller oetiskt). I kommunikationen av företagets riktlinjer i fråga om hederlighet och etiska värderingar kan ingå att kommunicera normer för agerande till personalen genom riktlinjer och uppförandekoder samt genom att föregå med gott exempel.

(b) *När styrelsen är separat från ledningen, hur styrelsen visar sitt oberoende gentemot ledningen och utövar tillsyn över företagets system för intern kontroll.* Ett företags kontrollmedvetande påverkas av styrelsen. Överväganden kan omfatta huruvida det finns tillräckligt många personer som är oberoende i förhållande till ledningen och objektiva i sina utvärderingar och sitt beslutsfattande och hur styrelsen identifierar och godtar ansvar för översynen och huruvida styrelsen behåller ansvaret för översynen av ledningens utformning, införande och hantering av företagets system för intern kontroll. Betydelsen av styrelsens ansvar framgår av regelsystem samt av andra lagar och andra författningar eller vägledning som tagits fram åt styrelsen. Bland övriga ansvarsområden för styrelsen ingår tillsyn över utformningen och driften av anmälningsrutiner, s.k. ”whistle blower”-rutiner.

(c) *Hur företaget tilldelar befogenhet och ansvar för att uppnå sina mål.* Det kan omfatta överväganden av

- viktiga befogenhets- och ansvarsområden samt ändamålsenliga rapporteringsvägar
- riktlinjer som avser lämplig affärssed, kunskap och erfarenhet hos nyckelpersoner samt de resurser som ges när arbetsuppgifterna ska genomföras, och
- riktlinjer och kommunikation i syfte att se till att all personal förstår företagets mål, vet hur deras personliga handlingar samverkar med och bidrar till dessa mål samt inser hur och för vad de får ansvar.

(d) *Hur företaget lockar till sig, utvecklar och behåller kompetenta medarbetare i enlighet med sina mål.* Det omfattar hur företaget säkerställer att medarbetarna besitter den kunskap och skicklighet som krävs för att utföra de arbetsuppgifter som ingår i den enskilda personens jobb, så som

- normer för rekrytering av de mest kvalificerade personerna – med betoning på utbildning, tidigare erfarenheter, tidigare prestationer samt bevis på hederlighet och etiskt agerande.

- utbildningsriktlinjer som kommunicerar framtida roller och ansvar, som bland annat inbegriper kurser och seminarier som visar vilka nivåer på prestationer och agerande företaget förväntar sig
- regelbundna prestationsbedömningar som leder till befordringar visar att företaget satsar på att befordra kvalificerad personal till nivåer med större ansvar.

(e) *Hur företaget håller olika personer ansvariga för deras ansvarsområden för att nå målen med företagets system för intern kontroll.* Det kan till exempel uppnås genom

- mekanismer för att kommunicera och hålla olika personer ansvariga för att utöva kontrollansvar och för att införa rättelseåtgärder efter behov
- etablera resultatmått, stimulans och belöningar till de personer som är ansvariga för företagets system för intern kontroll, inklusive hur måtten utvärderas och behåller sin relevans
- hur press förknippad med uppnåendet av kontrollmål påverkar de enskilda personernas ansvar och resultatmått, och
- hur personerna blir föremål för disciplinära åtgärder efter behov.

Tillämpligheten av de ovanstående frågorna kommer att skilja sig åt mellan olika företag beroende på storlek, komplexitet i dess struktur och karaktären på dess aktiviteter.

Företagets riskbedömningsprocess

7. Företagets riskbedömningsprocess är en iterativ process för att identifiera och analysera risker för att nå företagets mål, och utgör grunden för hur företagsledningen eller styrelsen avgör vilka risker som ska hanteras.

8. När det gäller finansiell rapportering inbegriper företagets riskbedömningsprocess det sätt på vilket företagsledningen identifierar risker som är relevanta för utarbetandet av finansiella rapporter enligt företagets tillämpliga ramverk för finansiell rapportering, uppskattar hur betydande de är, bedömer sannolikheten för att de ska inträffa och beslutar om åtgärder för att hantera dem och resultatet av detta. Företagets riskbedömningsprocess kan t.ex. ta upp frågan hur företaget beaktar risken för att det finns oredovisade transaktioner eller hur företaget identifierar och analyserar betydande uppskattningar som har redovisats i de finansiella rapporterna.

9. Risker som är relevanta för en tillförlitlig finansiell rapportering inbegriper externa och interna händelser, transaktioner eller förhållanden som kan inträffa och få en negativ inverkan på företagets möjlighet att initiera, registrera, bearbeta och rapportera finansiell information som överensstämmer med företagsledningens påståenden i de finansiella rapporterna. Företagsledningen kan initiera planer, program eller åtgärder för att hantera särskilda risker eller besluta att påta sig en risk, av kostnadsskäl eller andra skäl. Risker kan uppstå eller förändras till följd av omständigheter såsom följande:

- *Förändringar i den operativa miljön.* Förändringar i regelverket, i den ekonomiska eller operativa miljön kan medföra förändringar i tryck från konkurrenter och betydande olika risker.

- *Ny personal.* Ny personal kan ha annat fokus eller annan förståelse av företagets system för intern kontroll.
- *Nytt eller ändrat informationssystem.* Betydande och snabba ändringar i informationssystemet kan förändra den risk som hänför sig till företagets system för intern kontroll.
- *Snabb tillväxt.* Betydande och snabbt expanderande verksamheter kan utsätta kontrollerna för påfrestningar och öka risken för att kontrollerna inte fungerar.
- *Ny teknik.* Att införa ny teknik i produktionsprocesser eller informationssystemet kan förändra den risk som företagets system för intern kontroll utformats för.
- *Nya affärsmodeller, produkter eller aktiviteter.* Att gå in i nya affärsområden eller affärstransaktioner som ett företag har begränsad erfarenhet av kan medföra nya risker avseende företagets system för intern kontroll.
- *Omstruktureringar av företag.* Omstruktureringar kan medföra personalminskningar och förändringar av övervakning och arbetsfördelning vilket kan ändra risken avseende företagets system för intern kontroll.
- *Expansion av utlandsverksamheter.* Expansion eller förvärv av utlandsverksamheter medför nya och ofta unika risker som kan påverka den interna kontrollen, t.ex. fler eller ändrade risker i samband med valutatransaktioner.
- *Nya redovisningsuttalanden.* Införande av nya redovisningsprinciper eller byte av redovisningsprinciper kan påverka risker i samband med att finansiella rapporter upprättas.
- *Användning av IT*. Risker avseende att
    - upprätthålla integriteten i data och informationsbearbetning
    - risker gällande företagets affärsstrategi som uppkommer om företagets IT-strategi inte på ett effektivt sätt stödjer företagets affärsstrategi, eller
    - förändringar av eller avbrott i företagets IT-miljö eller omsättning på IT-personal eller när företaget inte gör nödvändiga uppdateringar av IT-miljön eller sådana uppdateringar inte görs i rätt tid.

Företagets process för att övervaka systemet för intern kontroll

10. Företagets process för att övervaka systemet för intern kontroll är en fortlöpande process för att utvärdera ändamålsenligheten i företagets system för intern kontroll, samt att vidta nödvändiga åtgärder utan onödigt dröjsmål. Företagets process för att övervaka företagets system för intern kontroll kan bestå av löpande aktiviteter, separata utvärderingar (som genomförs regelbundet) eller en kombination av de båda. Löpande övervakningsaktiviteter byggs ofta in i ett företags ordinarie återkommande aktiviteter och kan inbegripa regelmässiga lednings- och tillsynsaktiviteter. Företagets process varierar sannolikt i omfattning och frekvens beroende på företagets bedömning av risken.

11. Målen med och omfattningen av funktioner för internrevision omfattar vanligtvis aktiviteter utformade för att utvärdera eller övervaka ändamålsenligheten i företagets system för intern kontroll.[72] Företagets process för att övervaka företagets system för intern kontroll kan inbegripa sådana aktiviteter som företagsledningens genomgång av huruvida bankavstämningar görs utan onödigt dröjsmål, internrevisorernas bedömning av om försäljningspersonalen följer företagets riktlinjer för villkor i försäljningsavtal samt en juridisk avdelnings tillsyn av hur företagets etiska riktlinjer eller riktlinjer för affärsmetoder följs. Övervakning sker också för att säkerställa att kontrollerna fortsätter att fungera över tiden. Om t.ex. ingen övervakning görs av att bankavstämningar sker på ett riktigt sätt och utan onödigt dröjsmål är det troligt att personalen slutar att göra dem.

12. Kontroller hänförliga till företagets process för att övervaka företagets system för intern kontroll, inklusive dem som övervakar underliggande automatiserade kontroller, kan vara automatiserade eller manuella, eller en kombination av båda. Ett företag kan till exempel använda automatiserade övervakningskontroller över åtkomst till viss teknik i kombination med automatiserade rapporter om ovanliga aktiviteter till ledningen, som manuellt undersöker identifierade avvikande poster.

13. När man skiljer mellan en övervakningsaktivitet och en kontroll hänförlig till informationssystemet beaktas de underliggande detaljerna i aktiviteten, särskilt när aktiviteten inbegriper någon form av tillsynsgranskning. Tillsynsgranskningar klassificeras inte automatiskt som övervakningsaktiviteter och det kan vara en bedömningsfråga om en granskning klassificeras som en kontroll hänförlig till informationssystemet eller en övervakningsaktivitet. Avsikten med en månatlig kontroll av fullständigheten kan till exempel vara att upptäcka och rätta till fel, medan syftet med en övervakningsaktivitet är att ta reda på varför felen uppkommer och ge ledningen ansvaret för att korrigera processen för att förhindra framtida fel. Enkelt uttryckt, en kontroll hänförlig till informationssystemet svarar på en specifik risk, medan en övervakningsaktivitet bedömer om kontrollerna inom var och en av de fem komponenterna i företagets system för intern kontroll fungerar som det är tänkt.

14. Övervakningsaktiviteter kan innefatta att använda sådan information från kommunikation med externa parter som kan tyda på problem eller belysa områden som behöver förbättras. Kunderna bekräftar indirekt fakturauppgifter genom att betala sina fakturor eller klaga på debiteringar. Tillsynsmyndigheter kan dessutom kommunicera med företaget i frågor som påverkar företagets system för intern kontroll, t.ex. kommunikation från granskning som görs av banktillsynsorgan. Företagsledningen kan vid utförandet av övervakningsaktiviteter dessutom beakta eventuell kommunikation om intern kontroll från externa revisorer.

Informationssystem och kommunikation

15. Det informationssystem som är relevant för upprättandet av de finansiella rapporterna består av aktiviteter och riktlinjer samt redovisning med underlag, utformade och fastställda för att

    - initiera, registrera och bearbeta transaktioner i företaget (samt att inhämta, bearbeta och ge information om händelser och förhållanden utöver transaktionerna) samt uppfylla redovisningsskyldigheten för tillhörande tillgångar, skulder och eget kapital

[72] ISA 610 (omarbetad 2013) Bilaga 4 i denna standard ger ytterligare vägledning avseende internrevision.

- rätta till transaktioner som har bearbetats felaktigt, t.ex. automatiska bevakningsfiler och rutiner för att reglera bevakningsposter utan onödigt dröjsmål
- bearbeta och redogöra för situationer då system har åsidosatts eller kontroller har kringgåtts
- införliva information från bearbetning av transaktioner i huvudboken (t.ex. överföring av ackumulerade transaktioner från en reskontra)
- samla in och bearbeta information, som är relevant för upprättandet av de finansiella rapporterna, om händelser och förhållanden utöver transaktioner, t.ex. avskrivning av tillgångar och förändringar i återvinningsvärdet av tillgångar, och
- säkerställa att den information som måste lämnas enligt det tillämpliga ramverket för finansiell rapportering samlas in, förtecknas, bearbetas, sammanfattas och rapporteras på rätt sätt i de finansiella rapporterna.

16. Ett företags affärsprocesser omfattar aktiviteter som syftar till att
    - utveckla, köpa, producera, sälja och distribuera ett företags varor och tjänster
    - säkerställa att lagar och andra författningar följs, och
    - registrera information, däribland information som rör redovisning och finansiell rapportering.

    Affärsprocesser leder fram till transaktioner som bokförs, bearbetas och redovisas i informationssystemet.

17. Kvaliteten på informationen påverkar företagsledningens möjlighet att fatta riktiga beslut om ledning och kontroll av företagets verksamheter och att upprätta tillförlitliga finansiella rapporter.

18. Kommunikation, som inbegriper att ge en förståelse av enskilda roller och ansvar som hänför sig till företagets system för intern kontroll kan ske i form av policydokument, handböcker för redovisning och finansiell rapportering samt promemorior. Kommunikation kan också ske elektroniskt, muntligt eller genom företagsledningens åtgärder.

19. I företagets interna kommunikation av roller och ansvar beträffande den finansiella rapporteringen och betydelsefulla frågor som rör den finansiella rapporteringen ingår att förmedla en förståelse av de individuella roller och ansvarsområden som rör den interna kontrollen över den finansiella rapporteringen. Detta kan inbegripa frågor som i vilken omfattning medarbetarna förstår hur deras aktiviteter i informationssystemet hänger samman med andras arbete och på vilket sätt avvikelser ska rapporteras till lämplig högre nivå i företaget.

Kontrollaktiviteter

20. Kontrollerna i kontrollaktivitetskomponenten identifieras enligt punkt 26. Sådana kontroller omfattar informationsbearbetningskontroller och allmänna IT-kontroller, varav båda kan vara av manuell eller automatiserad art. Ju större omfattningen är av automatiserade kontroller, eller kontroller som inbegriper automatiserade aspekter, som ledningen använder och förlitar sig på med avseende på sin finansiella rapportering, desto viktigare kan det bli för företaget att införa allmänna IT-kontroller som säkerställer att de automatiserade aspekterna av informationsbearbetningskontrollerna löpande fungerar. Kontroller i kontrollaktivitetskomponenten kan avse följande:

- *Auktorisation och godkännanden*. En auktorisation bekräftar att en transaktion är giltig (dvs. den representerar en faktisk ekonomisk händelse eller faller inom ramen för ett företags riktlinjer). En auktorisation har vanligtvis formen av ett godkännande från en högre nivå i ledningen eller av en verifiering samt ett fastställande av att transaktionen är giltig. En chef kan till exempel godkänna en kostnadsrapport efter att ha granskat om kostnaderna verkar rimliga och inom ramen för riktlinjerna. Ett exempel på ett automatiserat godkännande är när en kostnad per enhet på en faktura automatiskt jämförs med motsvarande kostnaden per enhet på köpordern inom en på förhand etablerad toleransnivå. Fakturor inom ramen för toleransnivån godkänns automatiskt för betalning. De fakturor som faller utanför toleransnivån flaggas för ytterligare utredning.
- *Avstämningar* – Avstämningar jämför två eller fler dataelement. Om några skillnader identifieras vidtas åtgärder för att ta reda på vari skillnaden består. Avstämningar avser vanligtvis fullständigheten eller riktigheten i hur transaktionerna bearbetas.
- *Verifieringar* – Verifieringar jämför två eller fler poster med varandra eller jämför en post med en riktlinje, och medför sannolikt en uppföljningsåtgärd när de två posterna inte stämmer överens eller posten inte följer riktlinjerna. Verifieringar avser vanligtvis fullständigheten, riktigheten eller giltigheten i hur transaktionerna har bearbetats.
- *Fysiska eller logiska kontroller, inklusive dem som hanterar tillgångarnas säkerhet mot obehörig åtkomst, obehörigt förvärv, obehörig användning eller avyttring.* Kontroller som inbegriper
    - den fysiska säkerheten för tillgångar, däribland tillräckligt skydd såsom säkra lokaler som hindrar åtkomst till tillgångar och bokföringsmaterial
    - godkännande av åtkomst till datorprogram och datafiler (dvs. logisk åtkomst)
    - regelbunden räkning och jämförelse med belopp som framgår av kontrollposter (t.ex. jämförelse av resultatet av inventeringar av likvida medel, värdepapper och varulager med räkenskapsmaterialet).

  I vilken omfattning de fysiska kontroller som ska förhindra stöld av tillgångar är relevanta för att de finansiella rapporterna upprättas på ett tillförlitligt sätt beror på omständigheter såsom om tillgångar är begärliga eller lätt kan förskingras.
- *Arbetsfördelning.* Ge olika personer ansvar för att godkänna transaktioner, bokföra transaktioner och förvara tillgångar. Syftet med arbetsfördelning är att minska möjligheten för en person att ha en sådan ställning att han eller hon både kan begå och dölja misstag eller oegentligheter inom ramen för sina ordinarie arbetsuppgifter.

  En chef som godkänner försäljning på kredit ansvarar till exempel inte för redovisningen av kundfordringar eller för att hantera inbetalningar. Om en person kan utföra alla dessa aktiviteter skulle personen till exempel kunna skapa en fiktiv försäljning som inte skulle bli upptäckt. På ett liknande sätt ska säljare inte ha möjlighet att modifiera produktprisfiler eller provisionsnivåer.

Ibland är inte en arbetsfördelning praktiskt genomförbar, kostnadseffektiv eller möjlig. Små och mindre komplexa företag kanske till exempel saknar tillräckliga resurser för att uppnå en idealisk arbetsfördelning och kostnaden för att anställa ytterligare personal kan vara oöverkomlig. I de lägena kan ledningen införa alternativa kontroller. Om säljaren i exemplet ovan kan modifiera produktprisfiler kan en kontrollaktivitet för att upptäcka felaktigheter inrättas så att personal som inte har någon relation till säljaren i fråga regelbundet granskar om och under vilka omständigheter säljaren har ändrat priserna.

21. Vissa kontroller kan vara beroende av förekomsten av tillsynskontroller som har införts av företagsledningen eller styrelsen. T.ex. kan attestkontroller delegeras enligt fastställda riktlinjer såsom investeringskriterier som har fastställts av styrelsen. Alternativt kan icke rutinmässiga transaktioner, såsom stora förvärv eller avyttringar, kräva särskilt godkännande från hög nivå, däribland av aktieägarna i vissa fall.

Begränsningar i intern kontroll

22. Företagets system för intern kontroll, oavsett hur effektiv den är, kan endast ge rimlig säkerhet om hur väl företag når sina mål med avseende på finansiell rapportering. Sannolikheten för att de ska uppnås påverkas av inneboende begränsningar i den interna kontrollen. I dessa ingår det faktum att människor kan göra felaktiga bedömningar när de fattar beslut och att systemet för intern kontroll kan sluta att fungera på grund av den mänskliga faktorn. Fel kan t.ex. förekomma i utformningen av eller vid en ändring av en kontroll. På samma sätt kan det hända att en kontroll inte fungerar, t.ex. om den information som har tagits fram särskilt för företagets system för intern kontroll (t.ex. en avvikelserapport) inte används på avsett sätt på grund av att den person som ska gå igenom informationen inte förstår dess syfte eller inte vidtar lämpliga åtgärder.

23. Kontroller kan dessutom kringgås om två personer eller fler kommer överens om detta i maskopi med varandra eller om företagsledningen på ett otillbörligt sätt beslutar att sätta sig över kontrollerna. Företagsledningen kan t.ex. teckna sidoavtal med kunder, som ändrar villkoren i företagets standardiserade försäljningsavtal vilket kan leda till felaktig intäktsredovisning. Kontroller i en IT-applikation som har utformats för att identifiera och rapportera transaktioner som överstiger vissa kreditgränser kan också åsidosättas eller stängas av.

24. När företagsledningen utformar och inför kontroller kan den dessutom göra bedömningar av arten på och omfattningen av de kontroller som den väljer att införa samt arten på och omfattningen av de risker som den väljer att påta sig.

Bilaga 4

(Se punkterna 14(a), 24(a)(ii), A25–A28, A118)

Överväganden för att förstå företagets internrevisionsfunktion

Denna bilaga innehåller ytterligare överväganden avseende att förstå företagets internrevisionsfunktion när det finns en sådan funktion.

Internrevisionsfunktionens mål och omfattning

1. Internrevisionsfunktionens mål och omfattning, och arten på dess uppgifter och ställning inom organisationen, däribland funktionens befogenheter och ansvar, varierar kraftigt och beror på företagets storlek, komplexitet och struktur samt behoven hos företagsledningen och, i tillämpliga fall, styrelsen. Dessa förhållanden kan beskrivas i internrevisionens stadgar eller direktiv.

2. Internrevisionsfunktionens ansvar kan innefatta att utföra åtgärder och bedöma resultaten för att ge företagsledningen och styrelsen bekräftelse att utformningen av och ändamålsenligheten i riskhantering, företagets system för intern kontroll och styrningsprocesser är tillfredsställande. Om så är fallet kan internrevisionsfunktionen spela en viktig roll i företagets process för att övervaka företagets system för intern kontroll. Men internrevisionsfunktionens ansvar kan vara fokuserat på bedömning av verksamhetens ekonomi, effektivitet och ändamålsenlighet, och i detta fall kan internrevisionens arbete sakna direkt koppling till företagets finansiella rapportering.

Frågor till internrevisionsfunktionen

3. Om ett företag har en internrevisionsfunktion kan frågor till lämpliga personer inom funktionen ge information som är till nytta när revisorn skaffar sig en förståelse av företaget och dess miljö, det tillämpliga ramverket för finansiell rapportering och företagets system för intern kontroll, samt i att identifiera och bedöma riskerna för väsentliga felaktigheter på rapport- och påståendenivåerna. När internrevisionsfunktionen utför sitt arbete har den sannolikt fått kunskap om företagets verksamhet och affärsrisker och kan ha gjort iakttagelser baserat på sitt arbete, t.ex. identifierat kontrollbrister eller -risker som kan vara värdefull information för revisorns förståelse av företaget och dess miljö, det tillämpliga ramverket för finansiell rapportering, företagets system för intern kontroll, revisorns riskbedömning eller andra aspekter på revisionen. Frågorna ställs därför oavsett om revisorn räknar med att använda internrevisionsfunktionens arbete för att ändra karaktären på eller tidpunkten för, eller minska omfattningen av, de granskningsåtgärder som ska utföras eller inte.[73] Frågor som är särskilt relevanta kan handla om förhållanden som internrevisionsfunktionen har tagit upp med styrelsen och utfallet av funktionens egen riskbedömning.

4. Om det, baserat på svaren på revisorns frågor, verkar finnas iakttagelser som kan vara relevanta för företagets finansiella rapportering och revisionen av de finansiella rapporterna kan revisorn bedöma det som lämpligt att läsa relevanta rapporter från internrevisionsfunktionen. Exempel på rapporter från internrevisionsfunktionen som kan vara relevanta innefattar funktionens strategi- och

[73] De relevanta kraven återfinns i ISA 610 (omarbetad 2013).

planeringsdokument och rapporter som har upprättats åt företagsledningen eller styrelsen och som beskriver iakttagelserna från internrevisionsfunktionens granskningar.

5. Dessutom gäller, enligt ISA 240[74], att om internrevisionsfunktionen informerar revisorn om eventuella faktiska, misstänkta eller påstådda oegentligheter, ska revisorn beakta detta i sin identifiering av risk för väsentliga felaktigheter på grund av oegentligheter.

6. Lämpliga personer inom internrevisionsfunktionen till vilka frågor ställs är sådana som, enligt revisorns bedömning, har rätt kunskap, erfarenhet och befogenhet, t.ex. chefen för internrevisionen eller, beroende på omständigheterna, andra anställda inom funktionen. Revisorn kan också bedöma det lämpligt att ha återkommande möten med dessa personer.

Bedömning av internrevisionsfunktionen för att förstå kontrollmiljön

7. För att förstå kontrollmiljön kan revisorn också bedöma hur företagsledningen har hanterat internrevisionsfunktionens iakttagelser och rekommendationer i fråga om identifierade kontrollbrister som är relevanta för upprättandet av de finansiella rapporterna, däribland om och hur åtgärder som en följd härav har genomförts och om de därefter har utvärderats av internrevisionen.

Att förstå den roll som interrevisionsfunktionen spelar i företagets process för att övervaka systemet för intern kontroll

8. Om karaktären på internrevisionsfunktionens ansvarsområden och bestyrkandeverksamhet har koppling till företagets finansiella rapportering kan revisorn också använda internrevisionens arbete för att ändra art, tidpunkter och omfattning av de granskningsåtgärder som ska utföras direkt av revisorn för att inhämta revisionsbevis. Revisorer har troligen mer nytta av ett företags internrevisionsfunktions arbete när det, t.ex. utifrån erfarenheter från föregående revisioner eller revisorns riskbedömning, verkar som om företaget har en internrevisionsfunktion med tillräckliga och lämpliga resurser i förhållande till komplexiteten i företaget och arten på verksamheten samt som rapporterar direkt till styrelsen.

9. Om, utifrån revisorns preliminära förståelse av internrevisionen, han eller hon räknar med att använda internrevisionsfunktionens arbete för att ändra art, tidpunkter och omfattning av de granskningsåtgärder som ska utföras gäller ISA 610 (omarbetad 2013).

10. Enligt vad som närmare diskuteras i ISA 610 (omarbetad 2013) skiljer sig internrevisionsfunktionens aktiviteter från andra övervakningskontroller som kan vara relevanta för finansiell rapportering, t.ex. sådana genomgångar av företagets interna rapportering som är avsedda att bidra till att företaget förhindrar eller identifierar felaktigheter.

11. Att tidigt under uppdraget inleda en kommunikation med lämpliga personer inom ett företags internrevisionsfunktion och upprätthålla den kommunikationen under hela uppdraget kan bidra till en effektiv informationsdelning. Det skapar en miljö där revisorn kan hållas informerad om betydelsefulla förhållanden som internrevisionsfunktionen uppmärksammar, i de fall sådana förhållanden kan påverka revisorns arbete. ISA 200 diskuterar vikten av att revisorn planerar och utför revisionen med

[74] ISA 240, punkt 19

en professionellt skeptisk inställning[75], vilket innefattar att vara uppmärksam på information som ifrågasätter tillförlitligheten hos dokument och svar på frågor som ska användas som revisionsbevis. Därför kan kommunikation med internrevisionsfunktionen under hela uppdraget ge internrevisorer möjlighet att uppmärksamma revisorn på sådan information. Revisorn kan då ta hänsyn till den informationen i sin identifiering och bedömning av riskerna för väsentliga felaktigheter.

[75] ISA 200, punkt 7

Bilaga 5

(Se punkt 25(a), 26(b)–(c), A94, A166–A172)

Överväganden för att förstå informationstekniken (IT)

Denna bilaga innehåller ytterligare frågor som revisorn kan överväga för att förstå företagets användning av IT i sitt system för intern kontroll.

Att förstå företagets användning av informationsteknik i komponenterna i företagets system för intern kontroll

1. Ett företags system för intern kontroll innehåller manuella delar och automatiserade delar (dvs. manuella och automatiserade kontroller och andra resurser som används i företagets system för intern kontroll). Ett företags blandning av manuella och automatiserade delar varierar med arten på och komplexiteten i företagets IT-användning. Ett företags användning av IT påverkar hur information som är relevant för upprättandet av de finansiella rapporterna i enlighet med det tillämpliga ramverket för finansiell rapportering bearbetas, lagras och kommuniceras, och påverkar därmed hur företagets system för intern kontroll utformas och används. Varje enskild komponent i företagets system för intern kontroll kan använda IT i någon mån.

   Vanligtvis gagnar IT ett företags system för intern kontroll på följande sätt:

   - Företaget kan konsekvent tillämpa fördefinierade affärsregler och utföra komplexa beräkningar när stora mängder transaktioner eller data bearbetas.
   - Informationen kan tas fram snabbare, blir mer tillgänglig och riktig.
   - Ytterligare analys av informationen underlättas.
   - Det blir enklare att övervaka företagets aktiviteter samt dess riktlinjer och rutiner.
   - Risken för att kontroller kringgås minskar.
   - Genom att införa säkerhetskontroller i IT-applikationer, databaser och operativsystem ökar möjligheten att skapa en effektiv uppdelning av arbetsuppgifter.

2. De manuella eller automatiserade delarnas egenskaper har betydelse för revisorns identifiering och bedömning av riskerna för väsentliga felaktigheter och de fortsatta granskningsåtgärder som bygger på dessa. Automatiserade kontroller kan vara mer tillförlitliga än manuella kontroller, eftersom de inte kan kringgås, ignoreras eller åsidosättas, och risken är också mindre för att det uppstår enkla fel och misstag. Automatiserade kontroller kan vara mer effektiva än manuella kontroller under följande omständigheter:

   - Många återkommande transaktioner, eller i situationer när förväntade eller förutsägbara fel kan förhindras, eller upptäckas och rättas genom automatisering.
   - Kontroller där särskilda sätt att utföra kontrollen kan utformas och automatiseras på ett korrekt sätt.

Förstå företagets användning av informationsteknik i informationssystemet (se punkt 25(a))

3. Företagets informationssystem kan omfatta användningen av manuella och automatiserade delar, vilket också påverkar hur transaktioner initieras, registreras, bearbetas och redovisas. I synnerhet kan efterlevnaden av processer för att initiera, registrera, bearbeta och rapportera transaktioner upprätthållas genom de IT-applikationer som används av företaget samt hur företaget har konfigurerat dessa applikationer. Dessutom kan digital information ersätta eller komplettera redovisningen i form av pappersdokument.

4. För att skaffa sig en förståelse av IT-miljön relevant för transaktionsflödena och informationsbearbetningen i informationssystemet samlar revisorn in information om arten på och egenskaperna hos de IT-applikationer som används, liksom stödjande IT-infrastruktur och IT. Följande tabell innehåller exempel på frågor som revisorn kan överväga när han eller hon skaffar sig förståelse av IT-miljön och inbegriper exempel på typiska kännetecken för IT-miljöer baserat på komplexiteten i de IT-applikationer som används i företagets informationssystem. Sådana kännetecken pekar emellertid bara ut riktningen och kan variera beroende på arten på de specifika IT-program som används av ett företag.

	Exempel på typiska kännetecken för:		
	Icke-komplex kommersiell programvara	Medelstor och relativt komplex kommersiell programvara eller IT-applikationer	Stora eller komplexa IT-applikationer (t.ex. affärssystem)
Frågor hänförliga till graden av automatisering och dataanvändning:			
• I vilken grad automatiserade processer används för bearbetning, och komplexiteten i de processerna, inbegripet om det förekommer högautomatiserad, papperslös bearbetning.	Ej tillämpligt	Ej tillämpligt	Omfattande och ofta komplexa automatiserade processer
• I vilken grad företaget förlitar sig på systemgenererade rapporter när	Enkel automatiserad rapportlogik	Enkel relevant automatiserad rapportlogik	Komplex automatiserad rapportlogik; programvara för att skriva rapporter

	Exempel på typiska kännetecken för:		
	Icke-komplex kommersiell programvara	Medelstor och relativt komplex kommersiell programvara eller IT-applikationer	Stora eller komplexa IT-applikationer (t.ex. affärssystem)
informationen bearbetas.			
• Hur data läggs in (dvs. manuell registrering, registrering av kunder eller leverantörer, eller uppladdning av filer).	Manuell registrering av data	Små mängder indata eller enkla gränssnitt	Stora mängder indata eller komplexa gränssnitt
• Hur IT underlättar kommunikationen mellan program, databaser och andra aspekter av IT-miljön, internt eller externt, beroende på vilket som är lämpligt, genom systemgränssnitt.	Inga automatiserade gränssnitt (bara manuell registrering)	Små mängder indata eller enkla gränssnitt	Stora mängder indata eller komplexa gränssnitt
• Volym och komplexitet på den data i digital form som bearbetas i informationssystemet, inklusive om räkenskapsmaterial eller annan information lagras i	Låg volym av data eller enkla data som kan verifieras manuellt; data tillgänglig lokalt	Låg volym av data eller enkla data	Stor volym av data eller komplexa data; datalager;[76] Användning av interna eller externa IT-tjänsteleverantörer (t.ex.

[76] Ett datalager beskrivs allmänt som ett centrallager för databaser av integrerad data från en eller flera åtskilda källor (såsom flera olika databaser) från vilka det går att generera rapporter eller som kan användas av företaget för andra dataanalysaktiviteter. En rapportskrivare är en IT-applikation som används för att extrahera data från en eller flera källor (såsom ett datalager, en databas eller ett IT-applikation) och presentera uppgifterna i ett angivet format.

	Exempel på typiska kännetecken för:		
	Icke-komplex kommersiell programvara	Medelstor och relativt komplex kommersiell programvara eller IT-applikationer	Stora eller komplexa IT-applikationer (t.ex. affärssystem)
digital form och var lagrade data finns.			tredjepartslagring eller datavärdar)
Frågor hänförliga till IT-applikationer och IT-infrastruktur:			
• Typen av program (t.ex. ett kommersiellt program med liten eller ingen anpassning, eller ett höggradigt anpassat eller höggradigt integrerat program som kan ha köpts och anpassats, eller utvecklats, internt).	Köpt program med liten eller ingen kundanpassning	Köpt program eller ett äldre och enklare affärssystemsapplikationer med liten eller ingen anpassning	Program utvecklade av kunden eller mer komplexa affärssystem med en betydande anpassning
• Komplexiteten i karaktären på IT-applikationer och den underliggande IT-infrastrukturen.	Liten, enkel lösning anpassad till en bärbar dator eller server	Mogen och stabil stordator, liten eller enkel serverbaserad, molnbaserade program (SaaS)	Komplex stordator, stor eller komplex serverbaserad, webbapplikation, molnbaserad infrastruktur (IaaS)
• Om det förekommer tredjepartsvärdar eller outsourcing av IT.	Om IT är outsourcat, kompetent, mogen, beprövad leverantör (t.ex. molnleverantör)	Om IT är outsourcat, kompetent, mogen, beprövad leverantör (t.ex. molnleverantör)	Kompetent, mogen, beprövad leverantör för vissa program och nya eller nystartade leverantörer för andra
• Om företaget använder ny teknik som påverkar dess finansiella rapportering.	Ingen användning av ny teknik	Begränsad användning av ny teknik i vissa program	Blandad användning av ny teknik på olika plattformar

	Exempel på typiska kännetecken för:		
	Icke-komplex kommersiell programvara	Medelstor och relativt komplex kommersiell programvara eller IT-applikationer	Stora eller komplexa IT-applikationer (t.ex. affärssystem)
Frågor hänförliga till IT-processer:			
• Personalen som arbetar med att upprätthålla IT-miljön (antalet och kompetensnivån på IT-supportresurserna som hanterar säkerhet och förändringar av IT-miljön).	Få medarbetare med begränsade kunskaper om IT för att bearbeta uppgraderingar från leverantörer och hantera åtkomst	Begränsat antal personer med IT-kompetens/som arbetar med IT	Särskilda IT-avdelningar med kompetent personal, inklusive kompetens inom programmering
• Komplexiteten i processer för att hantera åtkomsträttigheter.	Ensam person med administrativ åtkomst hanterar åtkomsträttigheter	Ett fåtal personer med administrativ åtkomst hanterar åtkomsträttigheter	Komplexa processer för åtkomsträttigheter som hanteras av IT-avdelning
• Komplexiteten i säkerheten i IT-miljön, inklusive sårbarheten för cyberrisker hos IT-applikationer, databaser och andra aspekter av IT-miljön, i synnerhet när det förekommer webbaserade transaktioner eller transaktioner som innefattar externa gränssnitt.	Enkel intern åtkomst utan externa webbapplikationer	Vissa webbaserade applikationer med huvudsakligen enkel rollbaserad säkerhet	Ett flertal plattformar med webbaserad åtkomst och komplexa säkerhetsmodeller

	Exempel på typiska kännetecken för:		
	Icke-komplex kommersiell programvara	Medelstor och relativt komplex kommersiell programvara eller IT-applikationer	Stora eller komplexa IT-applikationer (t.ex. affärssystem)
• Om det har gjorts förändringar i programmet avseende hur informationen bearbetas, och omfattningen av sådana förändringar under perioden.	Kommersiell programvara utan installerad källkod	Vissa kommersiella applikationer utan källkod och andra mogna program med få eller enkla förändringar, traditionell systemutvecklingslivscykel	Nya, många eller komplexa förändringar, flera utvecklingscykler varje år
• Omfattningen av förändringar i IT-miljön (t.ex. nya aspekter på IT-miljön eller betydande förändringar i IT-applikationerna eller den underliggande IT-infrastrukturen).	Förändringar begränsade till versionsuppgraderingar av kommersiell programvara	Förändringar består av kommersiella programvaruuppgraderingar, versionsuppgraderingar av affärssystem eller förbättringar av äldre program	Nya, många eller komplexa förändringar, flera utvecklingscykler varje år, betydande anpassning av affärssystem
• Om det har skett en större datakonvertering under perioden och, i så fall, arten på och betydelsen av de förändringar som har gjorts, och hur konverteringen genomfördes.	Mjukvaruuppgraderingar som tillhandahålls av leverantören; Inga data konverterad vid uppgraderingen	Mindre versionsuppgraderingar för kommersiella programvaror med konvertering av vissa data	Större versionsuppgradering, ny release, byte av plattform

Ny teknik

5. Företag kan använda ny teknik (t.ex. blockkedja, robotteknik eller artificiell intelligens) eftersom sådan teknik kan erbjuda specifika möjligheter att öka effektiviteten i verksamheten eller förbättra den finansiella rapporteringen. När ny teknik som används i företagets informationssystem är relevant för upprättandet av de finansiella rapporterna kan revisorn ta med sådan teknik i identifieringen av IT-applikationer och andra aspekter av företagets IT-miljö som är föremål för IT-

relaterade risker. Samtidigt som ny teknik kan betraktas som mer sofistikerad eller mer komplex jämfört med befintlig teknik förblir revisorns ansvar i förhållande till IT-applikationer och identifierade allmänna IT-kontroller enligt punkterna 26(b)–(c) oförändrat.

Skalbarhet

6. Att skaffa sig en förståelse av företagets IT-miljö kan vara enklare för ett mindre komplext företag som använder kommersiell programvara och när företaget inte har tillgång till källkoden för att göra några ändringar i programmet. Sådana företag kanske inte har särskilda IT-resurser men kan ha en person utsedd till en administratörsroll i syfte att bevilja medarbetare åtkomst eller att installera uppgraderingar från leverantören i IT-applikationerna. Särskilda frågor som revisorn kan beakta för att förstå karaktären på ett kommersiellt redovisningsprogrampaket, som kan vara den enda IT-applikation som används av ett mindre komplext företag i deras informationssystem, kan omfatta följande:

   - I vilken grad programvaran är väletablerad och har ett anseende som tillförlitlig.
   - I vilken grad det är möjligt för företaget att modifiera källkoden i programvaran för att inkludera ytterligare moduler (dvs. tillägg) till basprogramvaran, eller göra direkta förändringar i data.
   - Arten på och omfattningen av de modifieringar som har gjorts av programvaran. Även om ett företag inte kan modifiera programvarans källkod medger många programvarupaket konfigurationer (t.ex. att ställa in eller ändra rapportparametrar). Dessa innefattar vanligtvis inte modifieringar av källkoden, däremot kan revisorn överväga i vilken grad företaget kan konfigurera programvaran när han eller hon beaktar fullständigheten och korrektheten i den information som tas fram av programvaran och som används som revisionsbevis, och
   - I vilken grad data hänförlig till att upprätta de finansiella rapporterna går att få åtkomst till direkt (dvs. direkt åtkomst till databasen utan att använda IT-applikationen) och volymen på de data som bearbetas. Ju större datavolym, desto mer sannolikt att företaget kan behöva kontroller som hanterar datas integritet, vilket kan omfatta allmänna IT-kontroller gällande obehörig åtkomst och förändringar av data.

7. Komplexa IT-miljöer kan omfatta höggradigt anpassade eller höggradigt integrerade IT-applikationer och kan därför kräva mer arbete för att förstå. Processer eller IT-applikationer för finansiell rapportering kan integreras med andra IT-applikationer. En sådan integration kan innefatta IT-applikationer som används i företagets affärsverksamhet och som tillhandahåller information till IT-applikationer relevanta för transaktionsflöden och informationsbearbetning i företagets informationssystem. Under sådana omständigheter kan vissa IT-applikationer som används i företagets affärsverksamhet också vara relevanta för upprättandet av de finansiella rapporterna. Komplexa IT-miljöer kan också kräva särskilda IT-avdelningar som har strukturerade IT-processer som stöds av personal som har kompetens inom programvaruutveckling och IT-underhåll. I andra fall kan ett företag använda interna eller externa tjänsteleverantörer för att hantera vissa aspekter av, eller IT-processer inom, sin IT-miljö (t.ex. tredjepartsvärdar).

Identifiera IT-applikationer som är föremål för IT-relaterade risker

8. Genom att förstå arten på och komplexiteten i företagets IT-miljö, däribland arten på och omfattningen av informationsbearbetningskontrollerna, kan revisorn fastställa vilka IT-applikationer som företaget förlitar sig på för att på ett korrekt sätt bearbeta och upprätthålla integriteten i den finansiella informationen. Identifieringen av de IT-applikationer som företaget förlitar sig på kan påverka revisorns beslut att testa de automatiserade kontrollerna i sådana IT-applikationer, under förutsättning att sådana automatiserade kontroller hanterar identifierade risker för väsentliga felaktigheter. På motsatt sätt, om företaget inte förlitar sig på en IT-applikation kommer de automatiserade kontrollerna i en sådan IT-applikation sannolikt inte att vara lämpliga eller tillräckligt exakta för att användas för att testa kontrollernas funktion. Automatiserade kontroller som kan identifieras enligt punkt 26(b) kan till exempel inbegripa automatiserade beräkningar eller kontroller över indata, bearbetning eller utdata, såsom en trepunktsmatchning för en inköpsorder, ett fraktdokument från leverantören och en leverantörsfaktura. När revisorn identifierar automatiserade kontroller och han eller hon fastställer, genom sin förståelse av IT-miljön, att företaget förlitar sig på IT-applikationen som innefattar de automatiserade kontrollerna, kan det vara mer sannolikt att revisorn identifierar IT-applikationen som en som är föremål för IT-relaterade risker.

9. När revisorn beaktar om de IT-applikationer för vilka han eller hon har identifierat automatiserade kontroller är föremål för IT-relaterade risker kommer revisorn sannolikt att överväga om, och i vilken grad, företaget har tillgång till källkod som gör det möjligt för ledningen att göra programändringar av sådana kontroller eller IT-applikationerna. I vilken grad företaget genomför program- eller konfigureringsändringar och i vilken grad IT-processerna hänförliga till sådana förändringar är formaliserade kan också vara relevanta frågor. Revisorn kommer sannolikt också att beakta risken för obehörig åtkomst eller förändringar av data.

10. Systemgenererade rapporter som revisorn kan ha för avsikt att använda som revisionsbevis kan till exempel omfatta en åldersanalys för leverantörsfordringar eller en lagervärderingsrapport. För sådana rapporter kan revisorn inhämta revisionsbevis om fullständigheten och korrektheten i rapporterna genom substansgranskning av in- och utdata i rapporten. I andra fall kan revisorn planera att granska kontrollernas funktion i fråga om upprättandet och underhållet av rapporten, i vilket fall IT-applikationen från vilken den har tagits fram sannolikt är föremål för IT-relaterade risker. Utöver att testa fullständigheten och korrektheten i rapporten kan revisorn planera att testa funktionerna hos de allmänna IT-kontrollerna som hanterar risker hänförliga till otillbörliga eller obehöriga programändringar, eller förändringar av data, i rapporten.

11. Vissa IT-applikationer kan innehålla funktioner för rapportskrivning medan vissa företag också kan använda sig av separata rapportskrivningsprogram (dvs. rapportskrivare). I sådana fall kan revisorn behöva fastställa källorna till de systemgenererade rapporterna (dvs. applikationen som upprättar rapporten och de datakällor som används av rapporten) för att fastställa vilka IT-applikationer som är föremål för IT-relaterade risker.

12. Datakällorna som används av IT-applikationen kan vara databaser som till exempel bara går att få åtkomst till genom IT-applikationen eller av IT-personal med databasadministrationsrättigheter. I andra fall kan datakällor vara ett datalager som i sig betraktas som en IT-applikation som är föremål för IT-relaterade risker.

13. Revisorn kan ha identifierat en risk för vilken enbart substansgranskning inte är tillräcklig på grund av företagets användning av högautomatiserad och papperslös bearbetning av transaktioner, som kan innefatta ett flertal integrerade IT-applikationer. Under sådana omständigheter inbegriper kontrollerna som identifieras av revisorn sannolikt automatiserade kontroller. Vidare kan företaget förlita sig på allmänna IT-kontroller för att upprätthålla integriteten i de transaktioner som bearbetas och annan information som används vid bearbetningen. I sådana fall är IT-applikationerna som ingår i bearbetningen och lagringen av informationen sannolikt föremål för IT-relaterade risker.

Slutanvändarnas databehandling

14. Även om revisionsbevis också kan ta sig formen av systemgenererade utdata som används vid en beräkning som utförs i en slutanvändares datorverktyg (t.ex. programvara för kalkylark eller enkla databaser) identifieras sådana verktyg normalt inte som IT-applikationer inom ramen för punkt 26(b). Det kan vara svårt att utforma och implementera kontroller kring åtkomst till och förändringar av slutanvändares datorverktyg, och sådana kontroller motsvarar sällan och är sällan så effektiva som allmänna IT-kontroller. Revisorn kan snarare överväga en kombination av informationsbearbetningskontroller, med beaktande av syftet med och komplexiteten i slutanvändarnas bearbetning av data, såsom

    - informationsberbetningskontroller över initierandet och bearbetningen av källdata, inklusive relevanta automatiserade kontroller eller gränssnittskontroller till den punkt där data extraheras (dvs. datalagret)
    - kontroller för att se om logiken fungerar som avsett, till exempel kontroller som ”bevisar” extraheringen av data, såsom att stämma av rapporten mot de data den har upprättats utifrån, jämföra enskilda uppgifter från rapporten med källan och vice versa, samt kontroller över formler eller makron, eller
    - användning av mjukvaruverktyg för validering, som systematiskt kontrollerar formler eller makron, så som integritetsverktyg för kalkylark.

Skalbarhet

15. Företagets förmåga att upprätthålla integriteten i den information som lagras och bearbetas i informationssystemet kan variera baserat på komplexiteten i och volymen av de hänförliga transaktionerna och annan information. Ju större komplexitet och datavolym som ligger till grund för ett betydande transaktionsslag, konto eller en betydande upplysning, desto mindre sannolikt kan det bli att företaget kan upprätthålla informationens integritet enbart genom informationsbearbetningskontroller (t.ex. kontroller av in- och utdata). Det blir också mindre sannolikt att revisorn kan inhämta revisionsbevis om fullständigheten och korrektheten i sådan information enbart genom substansgranskning när sådan information används som revisionsbevis. Under vissa omständigheter, när volymen eller komplexiteten på transaktionerna är lägre, kan ledningen ha en informationsbearbetningskontroll som är tillräcklig för att verifiera korrektheten och fullständigheten i data (t.ex. enskilda försäljningsorder som har bearbetats och fakturerats kan stämmas av mot utskriften som ursprungligen lades in i IT-applikationen). När företaget förlitar sig på allmänna IT-kontroller för att upprätthålla integriteten i viss information som används av IT-applikationerna kan

revisorn fastställa att de IT-applikationer som innehåller den informationen är föremål för IT-relaterade risker.

Exempel på kännetecken för en IT-applikation som sannolikt inte är föremål för IT-relaterade risker	Exempel på kännetecken för en IT-applikation som sannolikt är föremål för IT-relaterade risker
• Fristående applikationer. • Datavolymen (transaktioner) är inte betydande. • Applikationens funktion är inte komplex. • Alla transaktioner stöds av ursprunglig dokumentation på original på papper.	• Applikationerna har gränssnitt. • Datavolymen (transaktioner) är betydande. • Applikationens funktion är komplex eftersom – applikationen automatiskt initierar transaktioner, och – det finns ett antal olika komplexa beräkningar som ligger till grund för de automatiserade bokföringsposterna.
IT-applikationen är sannolikt inte föremål för IT-relaterade risker på grund av att • datavolymen inte är betydande och därför förlitar sig inte ledningen på allmänna IT-kontroller för att bearbeta och underhålla data. • Ledningen inte förlitar sig på automatiserade kontroller eller andra automatiserade funktioner, och revisorn inte har identifierat automatiserade kontroller enligt punkt 26(a). • Även om ledningen använder systemgenererade rapporter i sina kontroller förlitar den sig inte på dessa rapporter. I stället stämmer ledningen av rapporterna mot dokumentationen på papper och verifierar beräkningarna i rapporterna. • Revisorn kommer direkt att kontrollera informationen som har tagits fram av företaget och som används som revisionsbevis.	IT-applikationen är sannolikt föremål för IT-relaterade risker på grund av att • ledningen förlitar sig på ett programsystem för att bearbeta eller underhålla data eftersom datavolymen är betydande, • ledningen förlitar sig på programsystemet för att utföra vissa automatiserade kontroller som revisorn också har identifierat.

Andra aspekter på företagets IT-miljö som är föremål för IT-relaterade risker

16. När revisorn identifierar IT-applikationer som är föremål för IT-relaterade risker är andra aspekter på IT-miljön vanligtvis också föremål för IT-relaterade risker. IT-infrastrukturen omfattar databaser, operativsystem och nätverk. Databaser lagrar data som används av IT-applikationer och kan bestå av många sammanhängande datatabeller. IT-personalen eller annan personal med databasadministrationsrättigheter kan också ha direkt åtkomst till data i databaser genom databashanteringssystem. Operativsystemet ansvarar för att hantera kommunikationen mellan maskinvara, IT-applikationer och annan programvara som används i nätverket. På så sätt går det att ha åtkomst till IT-applikationer och databaser genom operativsystemet. Ett nätverk används i IT-infrastrukturen för att överföra data och för att dela information, resurser och tjänster genom en gemensam kommunikationslänk. Nätverket etablerar också vanligtvis en nivå av logisk säkerhet (som möjliggörs genom operativsystemet) för åtkomst till de underliggande resurserna.

17. När IT-applikationer identifieras av revisorn som föremål för IT-relaterade risker identifieras vanligtvis även databasen/databaserna som lagrar de data som bearbetas av ett identifierat IT-program. På ett liknande sätt, eftersom en IT-applikations förmåga att fungera ofta är beroende av operativsystemet, och det går att få åtkomst till IT-applikationer och databaser direkt från operativsystemet, är operativsystemet vanligtvis föremål för IT-relaterade risker. Nätverket kan identifieras när det är en central kontaktpunkt för de identifierade IT-applikationerna och hänförliga databaser eller när en IT-applikation samverkar med leverantörer eller externa parter genom internet, eller när IT-applikationer med gränssnitt mot internet identifieras av revisorn.

Identifiera IT-relaterade risker och allmänna IT-kontroller

18. Exempel på IT-relaterade risker omfattar risker hänförliga till ett otillbörligt beroende av IT-applikationer som behandlar data på ett felaktigt sätt, behandlar felaktiga data eller båda delarna, så som följande:

    - Obehörig tillgång till data, vilket kan leda till att data förstörs eller till felaktiga ändringar av data, däribland att icke godkända eller icke existerande transaktioner redovisas eller att transaktioner redovisas på ett felaktigt sätt. Särskilda risker kan uppstå när flera användare har tillgång till en gemensam databas.
    - Möjligheten att IT-personal får större åtkomstprivilegier än vad som är nödvändigt för att utföra sina arbetsuppgifter, vilket gör att arbetsfördelningen inte fungerar.
    - Obehöriga ändringar av stående data.
    - Obehöriga ändringar i IT-applikationer eller andra aspekter av IT-miljön.
    - Underlåtenhet att utföra nödvändiga ändringar i IT-applikationer eller andra aspekter av IT-miljön.
    - Felaktig manuell påverkan på data.
    - Potentiell förlust av data eller svårigheter att komma åt data.

19. Revisorns beaktande av obehörig åtkomst kan omfatta risker hänförliga till obehörig åtkomst av interna eller externa parter (kallas ofta cybersäkerhetsrisker). Sådana risker behöver inte

nödvändigtvis påverka den finansiella rapporteringen, eftersom ett företags IT-miljö även kan inkludera IT-applikationer och relaterade data som hanterar behov för verksamheten eller efterlevnad. Det är viktigt att notera att cyberincidenter ofta uppkommer först på nivån för externa och interna nätverk, som tenderar att ligga längre bort från IT-applikationen, databasen och operativsystemen som påverkar upprättandet av de finansiella rapporterna. Följaktligen beaktar revisorn vanligtvis, om information om en säkerhetsöverträdelse har identifierats, i vilken grad en sådan överträdelse hade potential att påverka den finansiella rapporteringen. Om den finansiella rapporteringen kan ha påverkats kan revisorn bestämma sig för att förstå och granska de hänförliga kontrollerna för att fastställa den möjliga påverkan från eller omfattningen av möjliga felaktigheter i de finansiella rapporterna eller kan fastställa att företaget har tillhandahållit korrekta upplysningar i samband med en sådan säkerhetsöverträdelse.

20. Även dataskyddslagar kan ingå i lagar och andra förordningar som kan ha en direkt eller indirekt påverkan på företagets finansiella rapporter. Att beakta företagets efterlevnad av sådana lagar eller förordningar enligt ISA 250 (omarbetad)[77] kan innefatta att förstå företagets IT-processer och allmänna IT-kontroller som företaget har infört för att hantera de relevanta lagarna eller förordningarna.

21. Allmänna IT-kontroller införts för att hantera IT-relaterade risker. Följaktligen använder revisorn den förståelse som har inhämtats av de identifierade IT-applikationerna och andra aspekter på IT-miljön och de tillämpliga IT-relaterade riskerna när han eller hon fastställer de allmänna IT-kontroller som ska identifieras. I vissa fall kan ett företag använda gemensamma IT-processer i hela sin IT-miljö eller i vissa IT-applikationer, i vilket fall gemensamma IT-relaterade risker och gemensamma allmänna IT-kontroller kan identifieras.

22. Generellt kommer ett större antal allmänna IT-kontroller hänförliga till IT-applikationer och databaser sannolikt att identifieras än för andra aspekter på IT-miljön. Det beror på att dessa aspekter är de som är närmast förknippade med informationsbearbetningen och lagringen av information i företagets informationssystem. När revisorn identifierar allmänna IT-kontroller kan han eller hon beakta kontroller av åtgärder både av slutanvändare och företagets IT-personal eller IT-tjänsteleverantörer.

23. **Bilaga 6** ger ytterligare förklaringar av arten på de allmänna IT-kontroller som vanligtvis införs för olika aspekter av IT-miljön. Därutöver ges exempel på allmänna IT-kontroller för olika IT-processer.

[77] ISA 250 (omarbetad)

Bilaga 6

(Se punkt 25(c)(ii), A173–A174)

Vad som behöver beaktas för att förstå de allmänna IT-kontrollerna

Denna bilaga innehåller ytterligare omständigheter som revisorn kan överväga för att förstå allmänna IT-kontroller.

1. Arten på de allmänna IT-kontroller som vanligtvis införs för varje aspekt av IT-miljön:

   (a) Applikationer

   Allmänna IT-kontroller på IT-applikationsnivån korrelerar med typ och omfattningen av applikationernas funktion och de åtkomstvägar som tekniken tillåter. Exempelvis är fler kontroller relevanta för högintegrerade IT-applikationer med komplexa säkerhetslösningar än för en äldre IT-applikation som stödjer ett litet antal konton med åtkomstmetoder enbart genom transaktioner.

   (b) Databaser

   Allmänna IT-kontroller på databasnivån hanterar vanligtvis IT-relaterade risker hänförliga till obehöriga uppdateringar av den finansiella rapportinformationen i databasen genom direkt åtkomst till databasen eller genom att köra ett skript eller program.

   (c) Operativsystem

   Allmänna IT-kontroller på operativsystemnivån hanterar vanligtvis IT-relaterade risker hänförliga till administrativ åtkomst, som kan göra det lättare att sätta sig över andra kontroller. Detta omfattar åtgärder som att missbruka andra användares autentiseringsuppgifter, att lägga till nya obehöriga användare, ladda ner skadlig kod eller köra skript eller andra obehöriga program.

   (d) Nätverk

   Allmänna IT-kontroller på nätverksnivån hanterar vanligtvis IT-relaterade risker hänförliga till nätverkssegmentering, fjärråtkomst och autentisering. Nätverkskontroller kan vara relevanta när ett företag har webbapplikationer som används i den finansiella rapporteringen. Nätverkskontroller kan också vara relevanta när företaget har betydande affärspartnerrelationer eller outsourcing till tredje part, vilket kan öka dataöverföringar och behovet av fjärråtkomst.

2. Exempel på allmänna IT-kontroller som kan finnas, organiserade efter IT-process omfattar

   (a) process för att hantera åtkomst:

   - *Autentisering*

     Kontroller som säkerställer att en användare som får åtkomst till IT-applikationen eller någon annan aspekt av IT-miljön använder användarens egna inloggningsuppgifter (dvs. att användaren inte använder någon annans uppgifter).

- *Godkännande*

  Kontroller som ger användarna åtkomst till den information som är nödvändig för dessas ansvarsområden och inget därutöver, vilket medger en god fördelning av arbetsuppgifter.

- *Nya behörigheter*

  Kontroller för att ge nya användare behörighet och modifiera befintliga användares behörigheter.

- *Ta bort behörigheter*

  Kontroller för att ta bort behörigheter vid uppsägning eller förflyttning.

- *Priviligierad åtkomst*

  Kontroller över åtkomsten för dem som administrerar IT eller har omfattande behörighet.

- *Granskningar av användaråtkomst*

  Kontroller för att omcertifiera eller utvärdera användaråtkomst för dem som har behörigheter över tid.

- *Säkerhetskonfigurationskontroller*

  Alla typer av teknik har vanligen viktiga konfigurationer som hjälper till att begränsa åtkomst till IT-miljön.

- *Fysisk åtkomst*

  Kontroller av fysisk åtkomst till datacenter eller maskinvara, eftersom sådan åtkomst kan användas för att kringgå andra kontroller.

(b) Process för att hantera program eller andra förändringar av IT-miljön:

- *Process för att hantera förändringar*

  Kontroller över processen för att utforma, programmera, testa och driftsätta förändringar i en produktionsmiljö (dvs. slutanvändarmiljö).

- *Arbetsfördelning gällande driftsättning av förändringar*

  Kontroller som fördelar åtkomst att genomföra och driftsätta ändringar till en produktionsmiljö.

- *Utveckling av system eller förvärv eller införande*

  Kontroller över initial utveckling eller införande av IT-applikationer (eller i relation till andra aspekter på IT-miljön).

- *Datakonvertering*

  Kontroller över datakonvertering under utveckling, införande eller uppgraderingar av IT-miljön.

(c) Process för att hantera IT-driften

- *Schemaläggning av arbete*

  Kontroller över åtkomst för att schemalägga och initiera arbeten eller program som kan påverka den finansiella rapporteringen.

- *Övervakning av arbete*

  Kontroller för att övervaka finansiella rapporteringsjobb eller program så att de genomförs framgångsrikt.

- *Säkerhetskopiering och återställning*

  Kontroller för att säkerställa att säkerhetskopiering görs som planerat av data för den finansiella redovisningen samt att sådana data är tillgängliga och går att få åtkomst till för en snabb återställning i händelse av ett avbrott eller en attack.

- *Upptäckt av intrång*

  Kontroller för att övervaka sårbarhet och/eller intrång i IT-miljön.

Tabellen nedan ger exempel på allmänna IT-kontroller för att hantera exempel på IT-relaterade risker, däribland för olika IT-applikationer utifrån deras art.

Process	**Risker**	**Kontroller**	**IT-applikationer**		
IT-process	**Exempel IT-relaterade risker**	**Exempel allmänna IT-kontroller**	**Icke-komplex kommersiell programvara – tillämpligt (ja/nej)**	**Medelstor och relativt komplex kommersiell programvara eller IT-applikationer – tillämpligt (ja/nej)**	**Stora eller komplexa IT-applikationer (t.ex. affärssystem) – tillämpligt (ja/nej)**
Hantera åtkomst	Behörigheter: Användarna har större behörigheter än vad som är nödvändigt för att utföra sina arbetsuppgifter	Ledningen godkänner karaktären på och omfattningen av behörigheter för ny och ändrad behörighet, inklusive profiler	Ja – i stället för granskningar av behörigheter som anges nedan	Ja	Ja

Process	Risker	Kontroller	IT-applikationer		
IT-process	**Exempel IT-relaterade risker**	**Exempel allmänna IT-kontroller**	**Icke-komplex kommersiell programvara – tillämpligt (ja/nej)**	**Medelstor och relativt komplex kommersiell programvara eller IT-applikationer – tillämpligt (ja/nej)**	**Stora eller komplexa IT-applikationer (t.ex. affärssystem) – tillämpligt (ja/nej)**
	, vilket kan skapa en olämplig arbetsfördelning.	och roller i standardprogram, viktiga transaktioner i den finansiella rapporteringen samt arbetsfördelning			
		Behörigheter för användare som har slutat eller flyttat tas bort eller modifieras snabbt	Ja – i stället för granskningar av behörigheter nedan	Ja	Ja
		Behörigheter granskas regelbundet	Ja – i stället kontroller av nya/tillbakadragna behörigheter ovan	Ja – för vissa program	Ja
		Arbetsfördelningen övervakas och behörigheter i konflikt med varandra tas antingen bort eller övervakas av kompenserande kontroller som	ET – ingen systemstödd fördelning	Ja – för vissa program	Ja

Process	**Risker**	**Kontroller**	**IT-applikationer**		
IT-process	**Exempel IT-relaterade risker**	**Exempel allmänna IT-kontroller**	**Icke-komplex kommersiell programvara – tillämpligt (ja/nej)**	**Medelstor och relativt komplex kommersiell programvara eller IT-applikationer – tillämpligt (ja/nej)**	**Stora eller komplexa IT-applikationer (t.ex. affärssystem) – tillämpligt (ja/nej)**
		dokumenteras och testas			
		Priviligierad nivå på behörighet (t.ex. konfigurations-, data- och säkerhetsadminstratörer) godkänns och begränsas på lämpligt sätt	Ja – sannolikt endast på IT-applikationsnivå	Ja – på IT-applikationsnivå och vissa nivåer av IT-miljö för plattform	Ja – på alla nivåer av IT-miljö för plattform
Hantera åtkomst	Direkt åtkomst till data: Felaktiga ändringar görs direkt av finansiella data på andra sätt än genom programtransaktioner.	Åtkomst till programdatafiler eller databasobjekt/tabeller/data är begränsad till behörig personal, baserat på deras ansvarsområden och deras roll, och sådan åtkomst godkänns av ledningen	Ej tillämpligt	Ja – för vissa program och databaser	Ja

Process	**Risker**	**Kontroller**	**IT-applikationer**		
IT-process	**Exempel IT-relaterade risker**	**Exempel allmänna IT-kontroller**	**Icke-komplex kommersiell programvara – tillämpligt (ja/nej)**	**Medelstor och relativt komplex kommersiell programvara eller IT-applikationer – tillämpligt (ja/nej)**	**Stora eller komplexa IT-applikationer (t.ex. affärssystem) – tillämpligt (ja/nej)**
Hantera åtkomst	Systeminställningar: Systemen är inte korrekt konfigurerade eller uppdaterade för att begränsa systemåtkomst till korrekt auktoriserade och lämpliga användare.	Åtkomst autentiseras genom unika användar-ID och lösenord eller andra metoder som en mekanism för att validera att användarna är behöriga att få åtkomst till systemet. Lösenordsparametrar uppfyller företags- eller branschstandarder (t.ex. lösenordets minimilängd och komplexitet, när det löper ut, när personen blir utelåst från kontot)	Ja – enbart lösenordsautentisering	Ja – kombination av lösenord och multifaktorautentisering	Ja
		De viktigaste stegen i säkerhetskonfigurationen har införts korrekt	ET – det finns ingen teknisk säkerhetskonfiguration	Ja – för vissa program och databaser	Ja

Process	**Risker**	**Kontroller**	**IT-applikationer**		
IT-process	**Exempel IT-relaterade risker**	**Exempel allmänna IT-kontroller**	**Icke-komplex kommersiell programvara – tillämpligt (ja/nej)**	**Medelstor och relativt komplex kommersiell programvara eller IT-applikationer – tillämpligt (ja/nej)**	**Stora eller komplexa IT-applikationer (t.ex. affärssystem) – tillämpligt (ja/nej)**
Hantera förändringar	Ändringar i programvara: Felaktiga förändringar görs i datasystemen eller program som innehåller relevanta automatiserade kontroller (dvs. inställningar som går att konfigurera, automatiserade algoritmer, automatiserade beräkningar och automatiserad extrahering av data) eller rapportlogik.	Applikationsändringar testas på ett korrekt sätt och godkänns innan de flyttas in i produktionsmiljön	ET – skulle verifiera att ingen källkod är installerad	Ja – för icke-kommersiell programvara	Ja
		Åtkomst för att föra in förändringar i produktionsmiljön är begränsad på ett korrekt sätt och avskild från utvecklingsmiljön	Ej tillämpligt	Ja – för icke-kommersiell programvara	Ja
Hantera förändringar	Ändringar i databaser: Felaktiga	Ändringar i databaser testas på ett korrekt sätt	ET – inga ändringar i databaser görs på företaget	Ja – för icke-kommersiell programvara	Ja

Process	Risker	Kontroller	IT-applikationer		
IT-process	**Exempel IT-relaterade risker**	**Exempel allmänna IT-kontroller**	**Icke-komplex kommersiell programvara – tillämpligt (ja/nej)**	**Medelstor och relativt komplex kommersiell programvara eller IT-applikationer – tillämpligt (ja/nej)**	**Stora eller komplexa IT-applikationer (t.ex. affärssystem) – tillämpligt (ja/nej)**
	ändringar görs av databasstrukturen och relationerna mellan data.	och godkänns innan de flyttas in i produktionsmiljön			
Hantera förändringar	Ändringar i systemets mjukvara: Felaktiga ändringar görs av systemets mjukvara (t.ex. operativsystem, nätverk, programvara för hantering av ändringar, programvara för åtkomstkontroll).	Förändringar av systemprogramvaran testas på ett korrekt sätt och godkänns innan de flyttas över till produktionen	ET – inga systemprogramvaruförändringar görs på företaget	Ja	Ja

Process	**Risker**	**Kontroller**	**IT-applikationer**		
IT-process	**Exempel IT-relaterade risker**	**Exempel allmänna IT-kontroller**	**Icke-komplex kommersiell programvara – tillämpligt (ja/nej)**	**Medelstor och relativt komplex kommersiell programvara eller IT-applikationer – tillämpligt (ja/nej)**	**Stora eller komplexa IT-applikationer (t.ex. affärssystem) – tillämpligt (ja/nej)**
Hantera förändringar	Datakonvertering: Data konverterad från äldre system eller tidigare versioner leder till datafel om konverteringen överför inkompletta, överflödiga, föråldrade eller inkorrekta data.	Ledningen godkänner resultatet av datakonverteringen (t.ex. balans- och avstämningsaktiviteter) från det gamla programsystemet eller den gamla datastrukturen och övervakar att konverteringen genomförs i enlighet med etablerade riktlinjer och processer för konvertering.	ET – hanteras genom manuella kontroller	Ja	Ja
IT-drift	Nätverk: Nätverket förhindrar inte på ett korrekt sätt obehöriga användare från att få otillåten	Åtkomst autentiseras genom unika användar-ID och lösenord eller andra metoder som en mekanism	ET – det finns inga separata metoder för nätverksautentisering	Ja	Ja

Process	Risker	Kontroller	IT-applikationer		
IT-process	**Exempel IT-relaterade risker**	**Exempel allmänna IT-kontroller**	**Icke-komplex kommersiell programvara – tillämpligt (ja/nej)**	**Medelstor och relativt komplex kommersiell programvara eller IT-applikationer – tillämpligt (ja/nej)**	**Stora eller komplexa IT-applikationer (t.ex. affärssystem) – tillämplig t (ja/nej)**
	åtkomst till informationssystemen.	för att validera att användarna är behöriga att få åtkomst till systemet. Lösenordsparametrar uppfyller företagets eller professionella riktlinjer och standarder (t.ex. lösenordets minimilängd och komplexitet, när det löper ut, när personen blir utelåst från kontot)			
		Nätverket är utformat så att webbapplikationer skiljs från det interna nätverket, där det finns åtkomst till program med intern kontroll över	ET – ingen nätverkssegmentering används	Ja – med omdöme	Ja – med omdöme

Process	Risker	Kontroller	IT-applikationer		
IT-process	**Exempel IT-relaterade risker**	**Exempel allmänna IT-kontroller**	**Icke-komplex kommersiell programvara – tillämpligt (ja/nej)**	**Medelstor och relativt komplex kommersiell programvara eller IT-applikationer – tillämpligt (ja/nej)**	**Stora eller komplexa IT-applikationer (t.ex. affärssystem) – tillämpligt (ja/nej)**
		den finansiella rapporteringen			
		Regelbundna sårbarhetsgenomsökningar av nätverkets externa kopplingar genomförs av nätverkshantering steamet, som också utreder möjlig sårbarhet	Ej tillämpligt	Ja – med omdöme	Ja – med omdöme
		Varningar skapas regelbundet för att uppmärksamma om hot som har identifierats av system för upptäckt av intrång. Dessa hot utreds av nätverkshantering steamet	Ej tillämpligt	Ja – med omdöme	Ja – med omdöme
		Kontroller införs för att begränsa VPN-åtkomst	Ej tillämpligt – inget VPN	Ja – med omdöme	Ja – med omdöme

Process	**Risker**	**Kontroller**	**IT-applikationer**		
IT-process	**Exempel IT-relaterade risker**	**Exempel allmänna IT-kontroller**	**Icke-komplex kommersiell programvara – tillämpligt (ja/nej)**	**Medelstor och relativt komplex kommersiell programvara eller IT-applikationer – tillämpligt (ja/nej)**	**Stora eller komplexa IT-applikationer (t.ex. affärssystem) – tillämpligt (ja/nej)**
		(Virtual Private Network) till behöriga och lämpliga användare			
IT-drift	Säkerhetskopiering av data och återställning: Finansiella data kan inte återställas och går inte att få åtkomst till inom en rimlig tidsperiod när det sker en förlust av data.	Finansiella data säkerhetskopieras regelbundet enligt ett fastställt schema och med regelbundna mellanrum	ET – förlitar sig på manuell säkerhetskopiering av ekonomiavdelningen	Ja	Ja
IT-drift	Schemaläggning av jobb: Produktionssystem, program eller jobb resulterar i en felaktig, ofullständig	Endast behöriga användare har tillgång till att uppdatera batchjobb (inklusive gränssnittsjobb) i programvaran för	Ej tillämpligt – inga batchjobb	Ja – för vissa program	Ja

Process	**Risker**	**Kontroller**	**IT-applikationer**		
IT-process	**Exempel IT-relaterade risker**	**Exempel allmänna IT-kontroller**	**Icke-komplex kommersiell programvara – tillämpligt (ja/nej)**	**Medelstor och relativt komplex kommersiell programvara eller IT-applikationer – tillämpligt (ja/nej)**	**Stora eller komplexa IT-applikationer (t.ex. affärssystem) – tillämplig t (ja/nej)**
	eller obehörig bearbetning av data.	att schemalägga arbetet			
		Viktiga system, program eller jobb övervakas, och fel i bearbetningen korrigeras för att säkerställa att jobbet blir korrekt avslutat.	Ej tillämpligt – ingen övervakning av jobb	Ja – för vissa program	Ja

FÖLJDÄNDRINGAR I ANDRA INTERNATIONELLA STANDARDER

Note: The following are conforming amendments to other International Standards as a result of the approval of ISA 315 (Revised 2019). These amendments will become effective at the same time as ISA 315 (Revised 2019), and are shown with marked changes from the latest approved versions of the International Standards that are amended. The footnote numbers within these amendments do not align with the International Standards that are amended, and reference should be made to those International Standards. These conforming amendments have received the approval of the PIOB which concluded that due process was followed in the development of the conforming amendments and that proper regard was paid to the public interest.

ISA 200, *Overall objectives of the Independent Auditor and the Conduct of an Audit in Accordance with International Standards on Auditing*

Scope of this ISA

…

An Audit of Financial Statements

...

7. The ISAs contain objectives, requirements and application and other explanatory material that are designed to support the auditor in obtaining reasonable assurance. The ISAs require that the auditor exercise professional judgment and maintain professional skepticism throughout the planning and performance of the audit and, among other things:

    - Identify and assess risks of material misstatement, whether due to fraud or error, based on an understanding of the entity and its environment, the applicable financial reporting framework and ~~including~~ the entity's system of internal control.
    - Obtain sufficient appropriate audit evidence about whether material misstatements exist, through designing and implementing appropriate responses to the assessed risks.
    - Form an opinion on the financial statements based on conclusions drawn from the audit evidence obtained.

…

Effective Date

…

Overall Objectives of the Auditor

…

Definitions

13. For purposes of the ISAs, the following terms have the meanings attributed below:

    …

(n) Risk of material misstatement – The risk that the financial statements are materially misstated prior to audit. This consists of two components, described as follows at the assertion level: (Ref: Para. A15a)

(i) Inherent risk – The susceptibility of an assertion about a class of transaction, account balance or disclosure to a misstatement that could be material, either individually or when aggregated with other misstatements, before consideration of any related controls.

(ii) Control risk – The risk that a misstatement that could occur in an assertion about a class of transactions, account balance or disclosure and that could be material, either individually or when aggregated with other misstatements, will not be prevented, or detected and corrected, on a timely basis by the entity's ~~internal~~ controls.

…

Requirements

Ethical Requirements Relating to an Audit of Financial Statements

…

Professional Skepticism

…

Professional Judgment

…

Sufficient Appropriate Audit Evidence and Audit Risk

17. To obtain reasonable assurance, the auditor shall obtain sufficient appropriate audit evidence to reduce audit risk to an acceptably low level and thereby enable the auditor to draw reasonable conclusions on which to base the auditor's opinion. (Ref: Para. A30–A54)

Conduct of an Audit in Accordance with ISAs

Complying with ISAs Relevant to the Audit

…

19. The auditor shall have an understanding of the entire text of an ISA, including its application and other explanatory material, to understand its objectives and to apply its requirements properly. (Ref: Para. A60–A68)

…

Objectives Stated in Individual ISAs

…

Complying with Relevant Requirements

…

Failure to Achieve an Objective

…

Application and Other Explanatory Material

An Audit of Financial Statements

Scope of the Audit (Ref: Para. 3)

…

Preparation of the Financial Statements (Ref: Para. 4)

…

Considerations Specific to Audits in the Public Sector

…

Form of the Auditor's Opinion (Ref: Para. 8)

…

Definitions

Financial Statements (Ref: Para. 13(f))

…

Risk of Material Misstatement (Ref: Para. 13(n))

A15a. For the purposes of the ISAs, a risk of material misstatement exists when there is a reasonable possibility of:

(a) A misstatement occurring (i.e., its likelihood); and

(b) Being material if it were to occur (i.e., its magnitude).

Ethical Requirements Relating to an Audit of Financial Statements (Ref: Para. 14)

…

Professional Skepticism (Ref: Para. 15)

…

Professional Judgment (Ref: Para. 16)

…

Sufficient Appropriate Audit Evidence and Audit Risk (Ref: Para. 5 and 17)

Sufficiency and Appropriateness of Audit Evidence

A30. Audit evidence is necessary to support the auditor's opinion and report. It is cumulative in nature and is primarily obtained from audit procedures performed during the course of the audit. It may, however, also include information obtained from other sources such as previous audits (provided the auditor

has determined whether changes have occurred since the previous audit that may affect its relevance to the current audit[78]) or a firm's quality control procedures for client acceptance and continuance. In addition to other sources inside and outside the entity, the entity's accounting records are an important source of audit evidence. Also, information that may be used as audit evidence may have been prepared by an expert employed or engaged by the entity. Audit evidence comprises both information that supports and corroborates management's assertions, and any information that contradicts such assertions. In addition, in some cases, the absence of information (for example, management's refusal to provide a requested representation) is used by the auditor, and therefore, also constitutes audit evidence. Most of the auditor's work in forming the auditor's opinion consists of obtaining and evaluating audit evidence.

…

Audit Risk

…

Risks of Material Misstatement

…

A40. Inherent risk is influenced by inherent risk factors. ~~higher for some assertions and related classes of transactions, account balances, and disclosures than for others.~~ Depending on the degree to which the inherent risk factors affect the susceptibility to misstatement of an assertion, the level of inherent risk varies on a scale that is referred to as the spectrum of inherent risk. The auditor determines significant classes of transactions, account balances and disclosures, and their relevant assertions, as part of the process of identifying and assessing the risks of material misstatement. For example, ~~it may be higher for complex calculations or for~~ account~~s~~ balances consisting of amounts derived from accounting estimates that are subject to significant estimation uncertainty may be identified as significant account balances, and the auditor's assessment of inherent risk for the related risks at the assertion level may be higher because of the high estimation uncertainty.

A40a. External circumstances giving rise to business risks may also influence inherent risk. For example, technological developments might make a particular product obsolete, thereby causing inventory to be more susceptible to overstatement. Factors in the entity and its environment that relate to several or all of the classes of transactions, account balances, or disclosures may also influence the inherent risk related to a specific assertion. Such factors may include, for example, a lack of sufficient working capital to continue operations or a declining industry characterized by a large number of business failures.

A41. Control risk is a function of the effectiveness of the design, implementation and maintenance of ~~internal~~ control~~s~~ by management to address identified risks that threaten the achievement of the entity's objectives relevant to preparation of the entity's financial statements. However, internal control, no matter how well designed and operated, can only reduce, but not eliminate, risks of

[78] ISA 315 (Revised 2019), *Identifying and Assessing the Risks of Material Misstatement ~~through Understanding the Entity and Its Environment~~*, paragraph 16~~9~~

material misstatement in the financial statements, because of the inherent limitations of ~~internal~~ controls. These include, for example, the possibility of human errors or mistakes, or of controls being circumvented by collusion or inappropriate management override. Accordingly, some control risk will always exist. The ISAs provide the conditions under which the auditor is required to, or may choose to, test the operating effectiveness of controls in determining the nature, timing and extent of substantive procedures to be performed.[79]

A42.[80] The assessment of the risks of material misstatement may be expressed in quantitative terms, such as in percentages, or in non-quantitative terms. In any case, the need for the auditor to make appropriate risk assessments is more important than the different approaches by which they may be made. The ISAs typically ~~do not ordinarily~~ refer to ~~inherent risk and control risk separately, but rather to a combined assessment of~~ the "risks of material misstatement~~.~~" rather than to inherent risk and control risk separately. However, ISA ~~540~~315 (Revised 2019)[81] requires a ~~separate assessment of~~ inherent risk to be assessed separately from ~~and~~ control risk to provide a basis for designing and performing further audit procedures to respond to the assessed risks of material misstatement at the assertion level~~,~~ ~~including significant risks, for accounting estimates at the assertion level~~ in accordance with ISA 330.[82] ~~In identifying and assessing risks of material misstatement for significant classes of transactions, account balances or disclosures other than accounting estimates, the auditor may make separate or combined assessments of inherent and control risk depending on preferred audit techniques or methodologies and practical considerations.~~

A43a. Risks of material misstatement are assessed at the assertion level in order to determine the nature, timing and extent of further audit procedures necessary to obtain sufficient appropriate audit evidence.[83]

Detection Risk

…

Inherent Limitations of an Audit

…

The Nature of Financial Reporting

…

---

79 ISA 330, *The Auditor's Reponses to Assessed Risks*, paragraphs 7–17

80 Note that paragraph A42 of ISA 200 is marked to the updated paragraph presented separately as a conforming amendment relating to ISA 540 (Revised) and its conforming amendments.

81 ISA ~~540~~315 (Revised 2019), ~~*Auditing Accounting Estimates and Disclosures,* paragraph 15~~*Identifying and Assessing the Risks of Material Misstatement*

~~82 ISA 330, paragraph 7(b)~~

83 ISA 330, paragraph 6

The Nature of Audit Procedures

…

Timeliness of Financial Reporting and the Balance between Benefit and Cost

…

A52. In light of the approaches described in paragraph A51, the ISAs contain requirements for the planning and performance of the audit and require the auditor, among other things, to:

- Have a basis for the identification and assessment of risks of material misstatement at the financial statement and assertion levels by performing risk assessment procedures and related activities;[84] and
- Use testing and other means of examining populations in a manner that provides a reasonable basis for the auditor to draw conclusions about the population.[85]

Other Matters that Affect the Inherent Limitations of an Audit

…

Conduct of an Audit in Accordance with ISAs

Nature of the ISAs (Ref: Para. 18)

…

Considerations Specific to Audits in the Public Sector

…

Contents of the ISAs (Ref: Para. 19)

A60. In addition to objectives and requirements (requirements are expressed in the ISAs using “shall”), an ISA contains related guidance in the form of application and other explanatory material. It may also contain introductory material that provides context relevant to a proper understanding of the ISA, and definitions. The entire text of an ISA, therefore, is relevant to an understanding of the objectives stated in an ISA and the proper application of the requirements of an ISA.

A61. Where necessary, the application and other explanatory material provides further explanation of the requirements of an ISA and guidance for carrying them out. In particular, it may:

- Explain more precisely what a requirement means or is intended to cover, including in some ISAs such as ISA 315 (Revised 2019), why a procedure is required.
- Include examples of procedures that may be appropriate in the circumstances. In some ISAs, such as ISA 315 (Revised 2019), examples are presented in boxes.

---

[84] ISA 315 (Revised 2019), paragraphs 17~~5~~–22~~10~~

[85] ISA 330; ISA 500; ISA 520, *Analytical Procedures*; ISA 530, *Audit Sampling*

While such guidance does not in itself impose a requirement, it is relevant to the proper application of the requirements of an ISA. The application and other explanatory material may also provide background information on matters addressed in an ISA.

~~Considerations Specific to Smaller Entities~~ Scalability Considerations

A65a Scalability considerations have been included in some ISAs (e.g., ISA 315 (Revised 2019)), illustrating the application of the requirements to all entities regardless of whether their nature and circumstances are less complex or more complex. Less complex entities are entities for which the characteristics in paragraph A66 may apply.

A65b. The "considerations specific to smaller entities" included in some ~~the~~ ISAs have been developed primarily with unlisted entities in mind. Some of the considerations, however, may be helpful in audits of smaller listed entities.

A66. For purposes of specifying additional considerations to audits of smaller entities, a "smaller entity" refers to an entity which typically possesses qualitative characteristics such as:

(a) Concentration of ownership and management in a small number of individuals (often a single individual – either a natural person or another enterprise that owns the entity provided the owner exhibits the relevant qualitative characteristics); and

(b) One or more of the following:

(i) Straightforward or uncomplicated transactions;

(ii) Simple record-keeping;

(iii) Few lines of business and few products within business lines;

(iv) Simpler systems of ~~Few~~ internal control~~s~~;

(v) Few levels of management with responsibility for a broad range of controls; or

(vi) Few personnel, many having a wide range of duties.

These qualitative characteristics are not exhaustive, they are not exclusive to smaller entities, and smaller entities do not necessarily display all of these characteristics.

A67 [*Moved – now A65b*]

Considerations Specific to Automated Tools and Techniques

A67a. The considerations specific to "automated tools and techniques" included in some ISAs (for example, ISA 315 (Revised 2019)) have been developed to explain how the auditor may apply certain requirements when using automated tools and techniques in performing audit procedures.

Objectives Stated in Individual ISAs (Ref: Para. 21)

…

Use of Objectives to Determine Need for Additional Audit Procedures (Ref: Para. 21(a))

…

Use of Objectives to Evaluate Whether Sufficient Appropriate Audit Evidence Has Been Obtained (Ref: Para. 21(b))

…

Complying with Relevant Requirements

Relevant Requirements (Ref: Para. 22)

…

Departure from a Requirement (Ref: Para. 23)

…

Failure to Achieve an Objective (Ref: Para. 24)…

ISA 210, *Agreeing the Terms of Audit Engagements*

Application and Other Explanatory Material

…

Preconditions for an Audit

…

Agreement of the Responsibilities of Management

…

Internal Control

…

A18. It is for management to determine what internal control is necessary to enable the preparation of the financial statements. The term "internal control" encompasses a wide range of activities within components of the system of internal control that may be described as the control environment; the entity's risk assessment process; the entity's process to monitor the system of internal control, the information system~~, including the related business processes relevant to financial reporting,~~ and communication; and control activities~~; and monitoring of controls~~. This division, however, does not necessarily reflect how a particular entity may design, implement and maintain its internal control, or how it may classify any particular component.[86] An entity's internal control (in particular, its accounting books and records, or accounting

[86] ISA 315 (Revised 2019),-paragraph A9159 and Appendix 31

systems) will reflect the needs of management, the complexity of the business, the nature of the risks to which the entity is subject, and relevant laws or regulation.

ISA 230, *Audit Documentation*

Application and Other Explanatory Material

…

Documentation of the Audit Procedures Performed and Audit Evidence Obtained

…

Identification of Specific Items or Matters Tested, and of the Preparer and Reviewer (Ref: Para. 9)

…

Considerations Specific to Smaller Entities (Ref. Para 8)

…

A17. When preparing audit documentation, the auditor of a smaller entity may also find it helpful and efficient to record various aspects of the audit together in a single document, with cross-references to supporting working papers as appropriate. Examples of matters that may be documented together in the audit of a smaller entity include the understanding of the entity and its environment, the applicable financial reporting framework, and the entity's system of internal control, the overall audit strategy and audit plan, materiality determined in accordance with ISA 320,[87] assessed risks, significant matters noted during the audit, and conclusions reached.

…

ISA 250 (Revised), *Consideration of Laws and Regulations in an Audit of Financial Statements*

Application and Other Explanatory Material

…

Audit Procedures When Non-Compliance is Identified or Suspected

…

Evaluating the Implications of Identified or Suspected Non-Compliance (Ref: Para. 22)

A23. As required by paragraph 22, the auditor evaluates the implications of identified or suspected non-compliance in relation to other aspects of the audit, including the auditor's risk assessment and the reliability of written representations. The implications of particular identified or suspected non-compliance will depend on the relationship of the perpetration and concealment, if any, of the act to specific controls ~~activities~~ and the level of management or individuals working for, or under the

[87] ISA 320, *Materiality in Planning and Performing an Audit*

direction of, the entity involved, especially implications arising from the involvement of the highest authority within the entity. As noted in paragraph 9, the auditor's compliance with law, regulation or relevant ethical requirements may provide further information that is relevant to the auditor's responsibilities in accordance with paragraph 22.

…

ISA 260 (Revised), *Communication with Those Charged with Governance*

Application and Other Explanatory Material

…

Matters to Be Communicated

…

Planned Scope and Timing of the Audit (Ref: Para. 15)

…

A12. Communicating significant risks identified by the auditor helps those charged with governance understand those matters and why they were determined to be significant risks ~~require special audit consideration~~. The communication about significant risks may assist those charged with governance in fulfilling their responsibility to oversee the financial reporting process.

A13**.** Matters communicated may include: …

- How the auditor plans to address the significant risks of material misstatement, whether due to fraud or error.
- How the auditor plans to address areas of higher assessed risks of material misstatement.
- The auditor's approach to the entity's system of internal control. ~~relevant to the audit.~~
- The application of the concept of materiality in the context of an audit.
- …

Appendix 2 (Ref: Para. 16(a), A19–A20)

Qualitative Aspects of Accounting Practices

The communication required by paragraph 16(a), and discussed in paragraphs A19–A20, may include such matters as:

…

Accounting Estimates

- For items for which estimates are significant, issues discussed in ISA 540,[1] including, for example:

- How management identifies those transactions, events ~~and~~ or conditions that may give rise to the need for accounting estimates to be recognized or disclosed in the financial statements.

…

ISA 265, *Communicating Deficiencies in Internal Control to Those Charged with Governance*

Introduction

Scope of this ISA

1. This International Standard on Auditing (ISA) deals with the auditor's responsibility to communicate appropriately to those charged with governance and management deficiencies in internal control that the auditor has identified in an audit of financial statements. This ISA does not impose additional responsibilities on the auditor regarding obtaining an understanding of the entity's system of internal control and designing and performing tests of controls over and above the requirements of ISA 315 (Revised 2019) and ISA 330. ISA 260 (Revised) establishes further requirements and provides guidance regarding the auditor's responsibility to communicate with those charged with governance in relation to the audit.

2. The auditor is required to obtain an understanding of the entity's system of internal control ~~relevant to the audit~~ when identifying and assessing the risks of material misstatement.[4] In making those risk assessments, the auditor considers the entity's system of internal control in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of internal control. The auditor may identify control deficiencies in internal control not only during this risk assessment process but also at any other stage of the audit. This ISA specifies which identified deficiencies the auditor is required to communicate to those charged with governance and management.

…

Application and Other Explanatory Material

Determination of Whether Deficiencies in Internal Control Have Been Identified (Ref: Para 7)

…

Considerations Specific to Smaller Entities

A3. While the concepts underlying controls in the control activities component in smaller entities are likely to be similar to those in larger entities, the formality with which they operate will vary. Further, smaller entities may find that certain types of controls ~~activities~~ are not necessary because of controls applied by management. For example, management's sole authority for granting credit to customers and approving significant purchases can provide effective control over important account balances and transactions, lessening or removing the need for more detailed controls ~~activities~~.

…

Significant Deficiencies in Internal Control (Ref: Para. 6(b), 8)

A8. Controls may be designed to operate individually or in combination to effectively prevent, or detect and correct, misstatements. For example, controls over accounts receivable may consist of both automated and manual controls designed to operate together to prevent, or detect and correct, misstatements in the account balance. A deficiency in internal control on its own may not be sufficiently important to constitute a significant deficiency. However, a combination of deficiencies affecting the same account balance or disclosure, ~~relevant~~ assertion, or component of the entity's system of internal control may increase the risks of misstatement to such an extent as to give rise to a significant deficiency.

ISA 240, *The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements*

Introduction

Scope of this ISA

…

Characteristics of Fraud

…

Responsibility for the Prevention and Detection of Fraud

…

Responsibilities of the Auditor

…

7. Furthermore, the risk of the auditor not detecting a material misstatement resulting from management fraud is greater than for employee fraud, because management is frequently in a position to directly or indirectly manipulate accounting records, present fraudulent financial information or override controls ~~procedures~~ designed to prevent similar frauds by other employees.

…

Effective Date

…

Objectives

…

Definitions

…

Requirements

Professional Skepticism

12. In accordance with ISA 200,[88] the auditor shall maintain professional skepticism throughout the audit, recognizing the possibility that a material misstatement due to fraud could exist, notwithstanding the auditor's past experience of the honesty and integrity of the entity's management and those charged with governance. (Ref: Para. A7–A8)

13. Unless the auditor has reason to believe the contrary, the auditor may accept records and documents as genuine. If conditions identified during the audit cause the auditor to believe that a document may not be authentic or that terms in a document have been modified but not disclosed to the auditor, the auditor shall investigate further. (Ref: Para. A9)

14. Where responses to inquiries of management or those charged with governance are inconsistent, the auditor shall investigate the inconsistencies.

Discussion among the Engagement Team

15. ISA 315 (Revised 2019) requires a discussion among the engagement team members and a determination by the engagement partner of which matters are to be communicated to those team members not involved in the discussion.[89] This discussion shall place particular emphasis on how and where the entity's financial statements may be susceptible to material misstatement due to fraud, including how fraud might occur. The discussion shall occur setting aside beliefs that the engagement team members may have that management and those charged with governance are honest and have integrity. (Ref: Para. A10–A11)

Risk Assessment Procedures and Related Activities

16. When performing risk assessment procedures and related activities to obtain an understanding of the entity and its environment, the applicable financial reporting framework and ~~including~~ the entity's system of internal control, required by ISA 315 (Revised 2019),[~~90~~] the auditor shall perform the procedures in paragraphs 23~~17–18~~ –43~~24~~ to obtain information for use in identifying the risks of material misstatement due to fraud.

Management and Others within the Entity

…

Those Charged with Governance

20. Unless all of those charged with governance are involved in managing the entity,[91] the auditor shall obtain an understanding of how those charged with governance exercise oversight of management's

---

88 ISA 200, paragraph 15

89 ISA 315 (Revised 2019), paragraph 17–18 ~~10~~

~~90 ISA 315 (Revised), paragraphs 5–24~~

91 ISA 260 (Revised), *Communication with Those Charged with Governance*, paragraph 13

processes for identifying and responding to the risks of fraud in the entity and the ~~internal~~ controls that management has established to mitigate these risks. (Ref: Para. A19–A21)

…

Unusual or Unexpected Relationships Identified

…

Other Information

23. The auditor shall consider whether other information obtained by the auditor indicates risks of material misstatement due to fraud. (Ref: Para. A22)

Evaluation of Fraud Risk Factors

24. The auditor shall evaluate whether the information obtained from the other risk assessment procedures and related activities performed indicates that one or more fraud risk factors are present. While fraud risk factors may not necessarily indicate the existence of fraud, they have often been present in circumstances where frauds have occurred and therefore may indicate risks of material misstatement due to fraud. (Ref: Para. A23–A27)

Identification and Assessment of the Risks of Material Misstatement Due to Fraud

25. In accordance with ISA 315 (Revised 2019), the auditor shall identify and assess the risks of material misstatement due to fraud at the financial statement level, and at the assertion level for classes of transactions, account balances and disclosures.[92]

26. When identifying and assessing the risks of material misstatement due to fraud, the auditor shall, based on a presumption that there are risks of fraud in revenue recognition, evaluate which types of revenue, revenue transactions or assertions give rise to such risks. Paragraph 47 specifies the documentation required where the auditor concludes that the presumption is not applicable in the circumstances of the engagement and, accordingly, has not identified revenue recognition as a risk of material misstatement due to fraud. (Ref: Para. A28–A30)

27. The auditor shall treat those assessed risks of material misstatement due to fraud as significant risks and accordingly, to the extent not already done so, the auditor shall ~~obtain an understanding of the entity's related~~ identify the entity's controls~~, including control activities, relevant to~~ that address such risks, and evaluate their design and determine whether they have been implemented).[93] (Ref: Para. A31–A32)

Responses to the Assessed Risks of Material Misstatement Due to Fraud

Overall Responses

…

[92] ISA 315 (Revised 2019), paragraph 28~~2~~

[93] ISA 315 (Revised 2019), paragraph 26(a)(i) and 26(d)

Audit Procedures Responsive to Assessed Risks of Material Misstatement Due to Fraud at the Assertion Level

…

Audit Procedures Responsive to Risks Related to Management Override of Controls

…

32. Irrespective of the auditor's assessment of the risks of management override of controls, the auditor shall design and perform audit procedures to:

    (a) Test the appropriateness of journal entries recorded in the general ledger and other adjustments made in the preparation of the financial statements. In designing and performing audit procedures for such tests, the auditor shall:

        (i) Make inquiries of individuals involved in the financial reporting process about inappropriate or unusual activity relating to the processing of journal entries and other adjustments;

        (ii) Select journal entries and other adjustments made at the end of a reporting period; and

        (iii) Consider the need to test journal entries and other adjustments throughout the period. (Ref: Para. A41–A44)

    …

Evaluation of Audit Evidence (Ref: Para. A49)

…

Auditor Unable to Continue the Engagement

…

Written Representations

…

Communications to Management and with Those Charged with Governance

…

Communications to Regulatory and Enforcement Authorities

…

Documentation

44. The auditor shall include the following in the audit documentation[94] ~~of the auditor's understanding of the entity and its environment and~~ of the identification and the assessment of the risks of material misstatement required by ISA 315 (Revised 2019):[95]

---

[94] ISA 230, *Audit Documentation*, paragraphs 8–11, and paragraph A6

[95] ISA 315 (Revised 2019), paragraph 38~~32~~

(a) The significant decisions reached during the discussion among the engagement team regarding the susceptibility of the entity's financial statements to material misstatement due to fraud; ~~and~~

(b) The identified and assessed risks of material misstatement due to fraud at the financial statement level and at the assertion level~~;~~ and

(c) Identified controls in the control activities component that address assessed risks of material misstatement due to fraud.

…

Application and Other Explanatory Material

Characteristics of Fraud (Ref: Para. 3)

…

Professional Skepticism *(Ref: Para. 12–14)*

A7. Maintaining professional skepticism requires an ongoing questioning of whether the information and audit evidence obtained suggests that a material misstatement due to fraud may exist. It includes considering the reliability of the information to be used as audit evidence and ~~the~~ identified controls in the control activities component, if any, over its preparation and maintenance. ~~where relevant.~~ Due to the characteristics of fraud, the auditor's professional skepticism is particularly important when considering the risks of material misstatement due to fraud.

…

Discussion Among the Engagement Team *(Ref: Para. 15)*

…

Risk Assessment Procedures and Related Activities

Inquiries of Management

Management's Assessment of the Risk of Material Misstatement Due to Fraud (Ref: Para. 17(a))

…

Inquiry of Internal Audit (Ref: Para. 19)

A18. ISA 315 (Revised 2019) and ISA 610 (Revised 2013) establish requirements and provide guidance relevant to audits of those entities that have an internal audit function.[96] In carrying out the requirements of those ISAs in the context of fraud, the auditor may inquire about specific activities of the function including, for example:

[96] ISA 315 (Revised 2019), paragraphs 14(a) and 24(a)(ii)~~6 and 23~~, and ISA 610 (Revised 2013), *Using the Work of Internal Auditors*

- The procedures performed, if any, by the internal auditor function during the year to detect fraud.
- Whether management has satisfactorily responded to any findings resulting from those procedures.

Obtaining an Understanding of Oversight Exercised by Those Charged with Governance (Ref: Para. 20)

A19. Those charged with governance of an entity oversee the entity's systems for monitoring risk, financial control and compliance with the law. In many countries, corporate governance practices are well developed and those charged with governance play an active role in oversight of the entity's assessment of the risks of fraud and ~~of the relevant internal control~~ the controls that address such risks. Since the responsibilities of those charged with governance and management may vary by entity and by country, it is important that the auditor understands their respective responsibilities to enable the auditor to obtain an understanding of the oversight exercised by the appropriate individuals.[97]

A20. An understanding of the oversight exercised by those charged with governance may provide insights regarding the susceptibility of the entity to management fraud, the adequacy of ~~internal~~ controls that address ~~over~~ risks of fraud, and the competency and integrity of management. The auditor may obtain this understanding in a number of ways, such as by attending meetings where such discussions take place, reading the minutes from such meetings or making inquiries of those charged with governance.

Considerations Specific to Smaller Entities

…

Consideration of Other Information (Ref: Para. 23)

A22. In addition to information obtained from applying analytical procedures, other information obtained about the entity and its environment, the applicable financial reporting framework and the entity's system of internal control may be helpful in identifying the risks of material misstatement due to fraud. The discussion among team members may provide information that is helpful in identifying such risks. In addition, information obtained from the auditor's client acceptance and retention processes, and experience gained on other engagements performed for the entity, for example, engagements to review interim financial information, may be relevant in the identification of the risks of material misstatement due to fraud.

[97] ISA 260 (Revised), paragraphs A1–A8, discuss with whom the auditor communicates when the entity's governance structure is not well defined.

Evaluation of Fraud Risk Factors (Ref: Para. 24)

…

A25. Examples of fraud risk factors related to fraudulent financial reporting and misappropriation of assets are presented in Appendix 1. These illustrative risk factors are classified based on the three conditions that are generally present when fraud exists:

- An incentive or pressure to commit fraud;
- A perceived opportunity to commit fraud; and
- An ability to rationalize the fraudulent action.

Fraud risk factors may relate to incentives, pressures or opportunities that arise from conditions that create susceptibility to misstatement, before consideration of controls. Fraud risk factors, which include intentional management bias, are, insofar as they affect inherent risk, inherent risk factors.[98] Fraud risk factors may also relate to conditions within the entity's system of internal control that provide opportunity to commit fraud or that may affect management's attitude or ability to rationalize fraudulent actions. Fraud r~~R~~isk factors reflective of an attitude that permits rationalization of the fraudulent action may not be susceptible to observation by the auditor. Nevertheless, the auditor may become aware of the existence of such information through, for example, the required understanding of the entity's control environment.[99] Although the fraud risk factors described in Appendix 1 cover a broad range of situations that may be faced by auditors, they are only examples and other risk factors may exist.

…

Identification and Assessment of the Risks of Material Misstatement Due to Fraud

Risks of Fraud in Revenue Recognition (Ref: Para. 26)

…

Identifying and Assessing the Risks of Material Misstatement Due to Fraud and Understanding the Entity's Related Controls (Ref: Para. 27)

A31. Management may make judgments on the nature and extent of the controls it chooses to implement, and the nature and extent of the risks it chooses to assume. In determining which controls to implement to prevent and detect fraud, management considers the risks that the financial statements may be materially misstated as a result of fraud. As part of this consideration, management may conclude that it is not cost effective to implement and maintain a particular control in relation to the reduction in the risks of material misstatement due to fraud to be achieved.

A32. It is therefore important for the auditor to obtain an understanding of the controls that management has designed, implemented and maintained to prevent and detect fraud. ~~In doing so,~~ In identifying the controls that address the risks of material misstatement due to fraud, the auditor may learn, for

[98] ISA 315 (Revised 2019), paragraph 12(f)

[99] ISA 315 (Revised 2019), paragraph 21

example, that management has consciously chosen to accept the risks associated with a lack of segregation of duties. Information from ~~obtaining this understanding~~ identifying these controls, and evaluating their design and determining whether they have been implemented, may also be useful in identifying fraud risks factors that may affect the auditor's assessment of the risks that the financial statements may contain material misstatement due to fraud.

Responses to the Assessed Risks of Material Misstatement Due to Fraud

Overall Responses (Ref: Para. 28)

…

Assignment and Supervision of Personnel (Ref: Para. 29(a))

…

Unpredictability in the Selection of Audit Procedures (Ref: Para. 29(c))

…

*Audit Procedures Responsive to Assessed Risks of Material Misstatement Due to Fraud at the Assertion Level (*Ref: Para. 30)

…

Audit Procedures Responsive to Risks Related to Management Override of Controls

Journal Entries and Other Adjustments (Ref: Para. 32(a))

…

A42. Further, the auditor's consideration of the risks of material misstatement associated with inappropriate override of controls over journal entries[100] is important since automated processes and controls may reduce the risk of inadvertent error but do not overcome the risk that individuals may inappropriately override such automated processes, for example, by changing the amounts being automatically passed to the general ledger or to the financial reporting system. Furthermore, where IT is used to transfer information automatically, there may be little or no visible evidence of such intervention in the information systems.

A43. When identifying and selecting journal entries and other adjustments for testing and determining the appropriate method of examining the underlying support for the items selected, the following matters are of relevance:

- *The identification and assessment of the risks of material misstatement due to fraud* – the presence of fraud risk factors and other information obtained during the auditor's identification and assessment of the risks of material misstatement due to fraud may assist the auditor to identify specific classes of journal entries and other adjustments for testing.
- *Controls that have been implemented over journal entries and other adjustments* – effective controls over the preparation and posting of journal entries and other adjustments may reduce

[100] ISA 315 (Revised 2019), paragraph 26(a)(ii)

the extent of substantive testing necessary, provided that the auditor has tested the operating effectiveness of the controls.

- *The entity's financial reporting process and the nature of evidence that can be obtained* – for many entities routine processing of transactions involves a combination of manual and automated ~~steps and procedures~~ controls. Similarly, the processing of journal entries and other adjustments may involve both manual and automated ~~procedures and~~ controls. Where information technology is used in the financial reporting process, journal entries and other adjustments may exist only in electronic form.
- *The characteristics of fraudulent journal entries or other adjustments* – inappropriate journal entries or other adjustments often have unique identifying characteristics. Such characteristics may include entries (a) made to unrelated, unusual, or seldom-used accounts, (b) made by individuals who typically do not make journal entries, (c) recorded at the end of the period or as post-closing entries that have little or no explanation or description, (d) made either before or during the preparation of the financial statements that do not have account numbers, or (e) containing round numbers or consistent ending numbers.
- *The nature and complexity of the accounts* – inappropriate journal entries or adjustments may be applied to accounts that (a) contain transactions that are complex or unusual in nature, (b) contain significant estimates and period-end adjustments, (c) have been prone to misstatements in the past, (d) have not been reconciled on a timely basis or contain unreconciled differences, (e) contain inter-company transactions, or (f) are otherwise associated with an identified risk of material misstatement due to fraud. In audits of entities that have several locations or components, consideration is given to the need to select journal entries from multiple locations.
- *Journal entries or other adjustments processed outside the normal course of business* – non standard journal entries may not be subject to the same ~~level of internal~~ nature and extent of controls as those journal entries used on a recurring basis to record transactions such as monthly sales, purchases and cash disbursements.

…

Accounting Estimates *(Ref: Para. 32(b))*

…

Business Rationale for Significant Transactions *(Ref: Para. 32(c))*

…

Evaluation of Audit Evidence (Ref: Para. 34–37)

…

Analytical Procedures Performed Near the End of the Audit in Forming an Overall Conclusion (Ref: Para. 34)

…

Consideration of Identified Misstatements (Ref: Para. 35–37)

…

Auditor Unable to Continue the Engagement (Ref: Para. 38)

…

Written Representations (Ref: Para. 39)

…

Communications to Management and with Those Charged with Governance

Communication to Management (Ref: Para. 40)

…

Communication with Those Charged with Governance (Ref: Para. 41)

…

Other Matters Related to Fraud (Ref: Para. 42)

…

Communications to Regulatory and Enforcement Authorities (Ref: Para. 43)

…

Appendix 1

(Ref: Para. A25)

Examples of Fraud Risk Factors

The fraud risk factors identified in this Appendix are examples of such factors that may be faced by auditors in a broad range of situations. Separately presented are examples relating to the two types of fraud relevant to the auditor's consideration – that is, fraudulent financial reporting and misappropriation of assets. For each of these types of fraud, the risk factors are further classified based on the three conditions generally present when material misstatements due to fraud occur: (a) incentives/pressures, (b) opportunities, and (c) attitudes/rationalizations. Although the risk factors cover a broad range of situations, they are only examples and, accordingly, the auditor may identify additional or different risk factors. Not all of these examples are relevant in all circumstances, and some may be of greater or lesser significance in entities of different size or with different ownership characteristics or circumstances. Also, the order of the examples of risk factors provided is not intended to reflect their relative importance or frequency of occurrence.

Fraud risk factors may relate to incentives or pressures, or opportunities, that arise from conditions that create susceptibility to misstatement before consideration of controls (i.e., the inherent risk). Such factors are inherent risk factors, insofar as they affect inherent risk, and may be due to management bias. Fraud risk factors related to opportunities may also arise from other identified inherent risk factors (for example, complexity or uncertainty may create opportunities that result in susceptibility to misstatement due to fraud). Fraud risk factors related to opportunities may also relate to conditions within the entity's system of internal

control, such as limitations or deficiencies in the entity's internal control that create such opportunities. Fraud risk factors related to attitudes or rationalizations may arise, in particular, from limitations or deficiencies in the entity's control environment.

Risk Factors Relating to Misstatements Arising from Fraudulent Financial Reporting

The following are examples of risk factors relating to misstatements arising from fraudulent financial reporting.

Incentives/Pressures

Financial stability or profitability is threatened by economic, industry, or entity operating conditions, such as (or as indicated by):

…

Excessive pressure exists for management to meet the requirements or expectations of third parties due to the following:

…

Information available indicates that the personal financial situation of management or those charged with governance is threatened by the entity's financial performance arising from the following:

…

Opportunities

The nature of the industry or the entity's operations provides opportunities to engage in fraudulent financial reporting that can arise from the following:

…

The monitoring of management is not effective as a result of the following:

…

There is a complex or unstable organizational structure, as evidenced by the following:

…

~~Internal control components are deficient~~ Deficiencies in internal control as a result of the following:

- Inadequate ~~monitoring of controls~~ process to monitor the entity's system of internal control, including automated controls and controls over interim financial reporting (where external reporting is required).
- High turnover rates or employment of staff in accounting, information technology, or the internal audit function that are not effective.
- Accounting and information systems that are not effective, including situations involving significant deficiencies in internal control.

Attitudes/Rationalizations

…

Risk Factors Arising from Misstatements Arising from Misappropriation of Assets

Risk factors that relate to misstatements arising from misappropriation of assets are also classified according to the three conditions generally present when fraud exists: incentives/pressures, opportunities, and attitudes/rationalization. Some of the risk factors related to misstatements arising from fraudulent financial reporting also may be present when misstatements arising from misappropriation of assets occur. For example, ineffective monitoring of management and other deficiencies in internal control may be present when misstatements due to either fraudulent financial reporting or misappropriation of assets exist. The following are examples of risk factors related to misstatements arising from misappropriation of assets.

Incentives/Pressures

…

Opportunities

Certain characteristics or circumstances may increase the susceptibility of assets to misappropriation. For example, opportunities to misappropriate assets increase when there are the following:

…

Inadequate ~~internal~~ control<u>s</u> over assets may increase the susceptibility of misappropriation of those assets. For example, misappropriation of assets may occur because there is the following:

- Inadequate segregation of duties or independent checks.
- Inadequate oversight of senior management expenditures, such as travel and other reimbursements.
- Inadequate management oversight of employees responsible for assets, for example, inadequate supervision or monitoring of remote locations.
- Inadequate job applicant screening of employees with access to assets.
- Inadequate record keeping with respect to assets.
- Inadequate system of authorization and approval of transactions (for example, in purchasing).
- Inadequate physical safeguards over cash, investments, inventory, or fixed assets.
- Lack of complete and timely reconciliations of assets.
- Lack of timely and appropriate documentation of transactions, for example, credits for merchandise returns.
- Lack of mandatory vacations for employees performing key control functions.
- Inadequate management understanding of information technology, which enables information technology employees to perpetrate a misappropriation.

- Inadequate access controls over automated records, including controls over and review of computer systems event logs.

Attitudes/Rationalizations

- Disregard for the need for monitoring or reducing risks related to misappropriations of assets.
- Disregard for ~~internal~~ controls over misappropriation of assets by overriding existing controls or by failing to take appropriate remedial action on known deficiencies in internal control.
- Behavior indicating displeasure or dissatisfaction with the entity or its treatment of the employee.
- Changes in behavior or lifestyle that may indicate assets have been misappropriated.
- Tolerance of petty theft.

Appendix 2

(Ref: Para. A40)

Examples of Possible Audit Procedures to Address the Assessed Risks of Material Misstatement Due to Fraud

The following are examples of possible audit procedures to address the assessed risks of material misstatement due to fraud resulting from both fraudulent financial reporting and misappropriation of assets. Although these procedures cover a broad range of situations, they are only examples and, accordingly they may not be the most appropriate nor necessary in each circumstance. Also the order of the procedures provided is not intended to reflect their relative importance.

Consideration at the Assertion Level

Specific responses to the auditor's assessment of the risks of material misstatement due to fraud will vary depending upon the types or combinations of fraud risk factors or conditions identified, and the classes of transactions, account balances, disclosures and assertions they may affect.

The following are specific examples of responses:

…

- If the work of an expert becomes particularly significant with respect to a financial statement item for which the assessed risk of material misstatement due to fraud is high, performing additional procedures relating to some or all of the expert's assumptions, methods or findings to determine that the findings are not unreasonable, or engaging another expert for that purpose.

…

Specific Responses—Misstatement Resulting from Fraudulent Financial Reporting

Examples of responses to the auditor's assessment of the risks of material misstatement due to fraudulent financial reporting are as follows:

…

Appendix 3

(Ref: Para. A49)

Examples of Circumstances that Indicate the Possibility of Fraud

The following are examples of circumstances that may indicate the possibility that the financial statements may contain a material misstatement resulting from fraud.

…

ISA 300, *Planning an Audit of Financial Statements*

Application and Other Explanatory Material

…

Documentation (Ref: Para. 12)

…

Considerations Specific to Smaller Entities

A21. As discussed in paragraph A11, a suitable, brief memorandum may serve as the documented strategy for the audit of a smaller entity. For the audit plan, standard audit programs or checklists (see paragraph A19) drawn up on the assumption of few ~~relevant~~ controls[101] ~~activities~~, as is likely to be the case in a smaller entity, may be used provided that they are tailored to the circumstances of the engagement, including the auditor's risk assessments.

…

[101] ISA 315 (Revised 2019), paragraph 26(a)

ISA 402, *Audit Considerations Relating to an Entity Using a Service Organization*

Introduction

Scope of this ISA

1. This International Standard on Auditing (ISA) deals with the user auditor's responsibility to obtain sufficient appropriate audit evidence when a user entity uses the services of one or more service organizations. Specifically, it expands on how the user auditor applies ISA 315 (Revised 2019) and ISA 330 in obtaining an understanding of the user entity, including the entity's system of internal control relevant to the preparation of the financial statements ~~relevant to the audit~~, sufficient to identify and assess the risks of material misstatement and in designing and performing further audit procedures responsive to those risks.

…

3. Services provided by a service organization are relevant to the audit of a user entity's financial statements when those services, and the controls over them, are part of the user entity's information system ~~, including related business processes,~~ relevant to ~~financial reporting~~ the preparation of the financial statements. ~~Although m~~ Most controls at the service organization are likely to ~~relate to financial reporting~~ be part of the user entity's information system relevant to the preparation of the financial statements, ~~there may be other~~ or related controls ~~that may also be relevant to the audit~~, such as controls over the safeguarding of assets. A service organization's services are part of a user entity's information system~~,~~ ~~including related business processes, relevant to financial reporting~~ if these services affect any of the following:

   (a) How information relating to significant classes of transactions, account balances and disclosures flows through the user entity's information system, whether manually or using IT, and whether obtained from within or outside the general ledger and subsidiary ledgers. ~~The classes of transactions in the user entity's operations that are significant to the user entity's financial statements;~~ This includes when the service organization's services affect how:

      (i) ~~(b) The procedures, within both information technology (IT) and manual systems, by which the user entity's transactions are initiated, recorded, processed, corrected as necessary, transferred to the general ledger and reported in the financial statements;~~ Transactions of the user entity are initiated, and how information about them is recorded, processed, corrected as necessary, and incorporated in the general ledger and reported in the financial statements; and

      (ii) Information about events or conditions, other than transactions, is captured, processed and disclosed by the user entity in the financial statements.

   (b) ~~(c)~~ The ~~related~~ accounting records, ~~either in electronic or manual form, supporting information and~~ specific accounts in the user entity's financial statements and other supporting records relating to the flows of information in paragraph 3(a) ~~that are used to initiate, record, process and report the user entity's transactions; this includes the correction of incorrect information and how information is transferred to the general ledger~~;

~~(d) How the user entity's information system captures events and conditions, other than transactions, that are significant to the financial statements;~~

(c~~e~~) The financial reporting process used to prepare the user entity's financial statements from the records described in paragraph 3(b), including as it relates to disclosures and to accounting estimates relating to significant classes of transactions, account balances and disclosures ~~accounting estimates and disclosures~~; and

(d) The entity's IT environment relevant to (a) to (c) above.

~~(f) Controls surrounding journal entries, including non-standard journal entries used to record non-recurring, unusual transactions or adjustments.~~

…

Objectives

7. The objectives of the user auditor, when the user entity uses the services of a service organization, are:

   (a) To obtain an understanding of the nature and significance of the services provided by the service organization and their effect on the user entity's system of internal control ~~relevant to the audit~~, sufficient to provide an appropriate basis for the identification and assessment of ~~identify and assess~~ the risks of material misstatement; and

   (b) To design and perform audit procedures responsive to those risks.

…

Requirements

Obtaining an Understanding of the Services Provided by a Service Organization, Including Internal Control

…

10. When obtaining an understanding of the entity's system of internal control ~~relevant to the audit~~ in accordance with ISA 315 (Revised 2019),~~[102]~~ the user auditor shall identify controls in the control activities component[103] ~~evaluate the design and implementation of relevant controls~~ at the user entity, from those that relate to the services provided by the service organization, including those that are applied to the transactions processed by the service organization, and evaluate their design and determine whether they have been implemented.[104] (Ref: Para. A12–A14)

11. The user auditor shall determine whether a sufficient understanding of the nature and significance of the services provided by the service organization and their effect on the user entity's system of

~~[102] ISA 315 (Revised), paragraph 12~~

[103] ISA 315 (Revised 2019), paragraphs 26(a)

[104] ISA 315 (Revised 2019), paragraph 26(d)

internal control ~~relevant to the audit~~ has been obtained to provide an appropriate basis for the identification and assessment of the risks of material misstatement.

12. If the user auditor is unable to obtain a sufficient understanding from the user entity, the user auditor shall obtain that understanding from one or more of the following procedures:

…

(c) Visiting the service organization and performing procedures that will provide the necessary information about the relevant controls at the service organization; or

(d) Using another auditor to perform procedures that will provide the necessary information about ~~the relevant~~ controls at the service organization. (Ref: Para. A15–A20)

Using a Type 1 or Type 2 Report to Support the User Auditor's Understanding of the Service Organization

…

14. If the user auditor plans to use a type 1 or type 2 report as audit evidence to support the user auditor's understanding about the design and implementation of controls at the service organization, the user auditor shall:

…

(b) Evaluate the sufficiency and appropriateness of the evidence provided by the report for the understanding of the ~~user entity's internal~~ controls at the service organization ~~relevant to the audit~~; and

…

Application and Other Explanatory Material

Obtaining an Understanding of the Services Provided by a Service Organization, Including Internal Control

…

Further Procedures When a Sufficient Understanding Cannot Be Obtained from the User Entity (Ref: Para. 12)

…

A19. Another auditor may be used to perform procedures that will provide the necessary information about the relevant controls at the service organization related to services provided to the user entity. If a type 1 or type 2 report has been issued, the user auditor may use the service auditor to perform these procedures as the service auditor has an existing relationship with the service organization. The user auditor using the work of another auditor may find the guidance in ISA 600 useful as it relates to understanding another auditor (including that auditor's independence and professional competence), involvement in the work of another auditor in planning the nature, timing and extent of such work, and in evaluating the sufficiency and appropriateness of the audit evidence obtained.

…

Using a Type 1 or Type 2 Report to Support the User Auditor's Understanding of the Service Organization (Ref: Para. 13–14)

…

A22. A type 1 or type 2 report, along with information about the user entity, may assist the user auditor in obtaining an understanding of:

(a) The aspects of controls at the service organization that may affect the processing of the user entity's transactions, including the use of subservice organizations;

(b) The flow of significant transactions through the service organization to determine the points in the transaction flow where material misstatements in the user entity's financial statements could occur;

(c) The control objectives at the service organization that are relevant to the user entity's financial statement assertions; and

(d) Whether controls at the service organization are suitably designed and implemented to prevent, or detect and correct processing errors that could result in material misstatements in the user entity's financial statements.

A type 1 or type 2 report may assist the user auditor in obtaining a sufficient understanding to identify and assess the risks of material misstatement. A type 1 report, however, does not provide any evidence of the operating effectiveness of the ~~relevant~~ controls.

Responding to the Assessed Risks of Material Misstatement

…

Test of Controls

A29. The user auditor is required by ISA 330 to design and perform tests of controls to obtain sufficient appropriate audit evidence as to the operating effectiveness of ~~relevant~~ controls in certain circumstances. In the context of a service organization, this requirement applies when:

…

A30. If a type 2 report is not available, a user auditor may contact the service organization, through the user entity, to request that a service auditor be engaged to provide a type 2 report that includes tests of the operating effectiveness of the ~~relevant~~ controls or the user auditor may use another auditor to perform procedures at the service organization that test the operating effectiveness of those controls. A user auditor may also visit the service organization and perform tests of ~~relevant~~ controls if the service organization agrees to it. The user auditor's risk assessments are based on the combined evidence provided by the work of another auditor and the user auditor's own procedures.

Using a Type 2 Report as Audit Evidence that Controls at the Service Organization Are Operating Effectively

…

A33. It may also be necessary for the user auditor to obtain additional evidence about significant changes to the ~~relevant~~ controls at the service organization outside of the period covered by the type 2 report or determine additional audit procedures to be performed. Relevant factors in determining what additional audit evidence to obtain about controls at the service organization that were operating outside of the period covered by the service auditor's report may include:

…

- The effectiveness of the control environment and the user entity's process to monitor the system of internal control ~~monitoring of controls at the user entity~~.

A34. Additional audit evidence may be obtained, for example, by extending tests of controls over the remaining period or testing the user entity's process to monitor the system of internal control ~~monitoring of controls~~.

…

A39. The user auditor is required to communicate in writing significant deficiencies identified during the audit to both management and those charged with governance on a timely basis.[11] The user auditor is also required to communicate to management at an appropriate level of responsibility on a timely basis other deficiencies in internal control identified during the audit that, in the user auditor's professional judgment, are of sufficient importance to merit management's attention.[12] Matters that the user auditor may identify during the audit and may communicate to management and those charged with governance of the user entity include:

- Any controls within the entity's process to monitor the system of internal control ~~monitoring of controls~~ that could be implemented by the user entity, including those identified as a result of obtaining a type 1 or type 2 report;

…

ISA 330, *The Auditor's Responses to Assessed Risks*

Introduction

(a) Scope of this ISA

1. This International Standard on Auditing (ISA) deals with the auditor's responsibility to design and implement responses to the risks of material misstatement identified and assessed by the auditor in accordance with ISA 315 (Revised 2019)[105] in an audit of financial statements.

Effective Date

2. This ISA is effective for audits of financial statements for periods beginning on or after December 15, 2009.

---

[105] ISA 315 (Revised 2019), *Identifying and Assessing the Risks of Material Misstatement ~~through Understanding the Entity and Its Environment~~*

Objective

3. The objective of the auditor is to obtain sufficient appropriate audit evidence regarding the assessed risks of material misstatement, through designing and implementing appropriate responses to those risks.

Definitions

4. For purposes of the ISAs, the following terms have the meanings attributed below:

   (a) Substantive procedure – An audit procedure designed to detect material misstatements at the assertion level. Substantive procedures comprise:

      (i) Tests of details (of classes of transactions, account balances, and disclosures); and

      (ii) Substantive analytical procedures.

   (b) Test of controls – An audit procedure designed to evaluate the operating effectiveness of controls in preventing, or detecting and correcting, material misstatements at the assertion level.

Requirements

Overall Responses

5. The auditor shall design and implement overall responses to address the assessed risks of material misstatement at the financial statement level. (Ref: Para. A1–A3)

Audit Procedures Responsive to the Assessed Risks of Material Misstatement at the Assertion Level

6. The auditor shall design and perform further audit procedures whose nature, timing and extent are based on and are responsive to the assessed risks of material misstatement at the assertion level. (Ref: Para. A4–A8; A42-A52)

7. In designing the further audit procedures to be performed, the auditor shall:

   (a) Consider the reasons for the assessment given to the risk of material misstatement at the assertion level for each significant class of transactions, account balance, and disclosure, including:

      (i) The likelihood and magnitude of ~~material~~ misstatement due to the particular characteristics of the ~~relevant~~ significant class of transactions, account balance, or disclosure (that is, the inherent risk); and

      (ii) Whether the risk assessment takes account of ~~relevant~~ controls that address the risk of material misstatement (that is, the control risk), thereby requiring the auditor to obtain audit evidence to determine whether the controls are operating effectively (that is, the auditor ~~intends to rely on~~plans to test the operating effectiveness of controls in determining the nature, timing and extent of substantive procedures); and (Ref: Para. A9–A18)

(b) Obtain more persuasive audit evidence the higher the auditor's assessment of risk. (Ref: Para. A19)

Tests of Controls

8. The auditor shall design and perform tests of controls to obtain sufficient appropriate audit evidence as to the operating effectiveness of ~~relevant~~ controls if:

   (a) The auditor's assessment of risks of material misstatement at the assertion level includes an expectation that the controls are operating effectively (that is, the auditor ~~intends~~ plans to test ~~to rely on~~ the operating effectiveness of controls in determining the nature, timing and extent of substantive procedures); or

   (b) Substantive procedures alone cannot provide sufficient appropriate audit evidence at the assertion level. (Ref: Para. A20–A24)

9. In designing and performing tests of controls, the auditor shall obtain more persuasive audit evidence the greater the reliance the auditor places on the effectiveness of a control. (Ref: Para. A25)

Nature and Extent of Tests of Controls

10. In designing and performing tests of controls, the auditor shall:

   (a) Perform other audit procedures in combination with inquiry to obtain audit evidence about the operating effectiveness of the controls, including:

      (i) How the controls were applied at relevant times during the period under audit;

      (ii) The consistency with which they were applied; and

      (iii) By whom or by what means they were applied. (Ref: Para. A26–A29a)

   (b) To the extent not already addressed, d~~D~~etermine whether the controls to be tested depend upon other controls (indirect controls), and, if so, whether it is necessary to obtain audit evidence supporting the effective operation of those indirect controls. (Ref: Para. A30–A31)

Timing of Tests of Controls

11. The auditor shall test controls for the particular time, or throughout the period, for which the auditor intends to rely on those controls, subject to paragraphs 12 and 15 below, in order to provide an appropriate basis for the auditor's intended reliance. (Ref: Para. A32)

Using audit evidence obtained during an interim period

12. If the auditor obtains audit evidence about the operating effectiveness of controls during an interim period, the auditor shall:

   (a) Obtain audit evidence about significant changes to those controls subsequent to the interim period; and

   (b) Determine the additional audit evidence to be obtained for the remaining period. (Ref: Para. A33–A34)

Using audit evidence obtained in previous audits

13. In determining whether it is appropriate to use audit evidence about the operating effectiveness of controls obtained in previous audits, and, if so, the length of the time period that may elapse before retesting a control, the auditor shall consider the following:

    (a) The effectiveness of other ~~elements~~ components of the entity's system of internal control, including the control environment, the entity's process to monitor~~ing~~ ~~of~~ the system of internal control~~s~~, and the entity's risk assessment process;

    (b) The risks arising from the characteristics of the control, including whether it is manual or automated;

    (c) The effectiveness of general IT controls;

    (d) The effectiveness of the control and its application by the entity, including the nature and extent of deviations in the application of the control noted in previous audits, and whether there have been personnel changes that significantly affect the application of the control;

    (e) Whether the lack of a change in a particular control poses a risk due to changing circumstances; and

    (f) The risks of material misstatement and the extent of reliance on the control. (Ref: Para. A35)

14. If the auditor plans to use audit evidence from a previous audit about the operating effectiveness of specific controls, the auditor shall establish the continuing relevance and reliability of that evidence by obtaining audit evidence about whether significant changes in those controls have occurred subsequent to the previous audit. The auditor shall obtain this evidence by performing inquiry combined with observation or inspection, to confirm the understanding of those specific controls, and:

    (a) If there have been changes that affect the continuing relevance of the audit evidence from the previous audit, the auditor shall test the controls in the current audit. (Ref: Para. A36)

    (b) If there have not been such changes, the auditor shall test the controls at least once in every third audit, and shall test some controls each audit to avoid the possibility of testing all the controls on which the auditor intends to rely in a single audit period with no testing of controls in the subsequent two audit periods. (Ref: Para. A37–A39)

Controls over significant risks

15. If the auditor ~~plans~~ intends to rely ~~test~~ on controls over a risk the auditor has determined to be a significant risk, the auditor shall test those controls in the current period.

Evaluating the Operating Effectiveness of Controls

16. When evaluating the operating effectiveness of ~~relevant~~ controls upon which the auditor intends to rely, the auditor shall evaluate whether misstatements that have been detected by substantive procedures indicate that controls are not operating effectively. The absence of misstatements detected by substantive procedures, however, does not provide audit evidence that controls related to the assertion being tested are effective. (Ref: Para. A40)

17. If deviations from controls upon which the auditor intends to rely are detected, the auditor shall make specific inquiries to understand these matters and their potential consequences, and shall determine whether: (Ref: Para. A41)

    (a) The tests of controls that have been performed provide an appropriate basis for reliance on the controls;

    (b) Additional tests of controls are necessary; or

    (c) The ~~potential~~ risks of material misstatement need to be addressed using substantive procedures.

Substantive Procedures

18. Irrespective of the assessed risks of material misstatement, the auditor shall design and perform substantive procedures for each material class of transactions, account balance, and disclosure. (Ref: Para. A42–A47)

19. The auditor shall consider whether external confirmation procedures are to be performed as substantive audit procedures. (Ref: Para. A48–A51)

Substantive Procedures Related to the Financial Statement Closing Process

20. The auditor's substantive procedures shall include the following audit procedures related to the financial statement closing process:

    (a) Agreeing or reconciling information in the financial statements with the underlying accounting records, including agreeing or reconciling information in disclosures, whether such information is obtained from within or outside of the general and subsidiary ledgers; and

    (b) Examining material journal entries and other adjustments made during the course of preparing the financial statements. (Ref: Para. A52)

Substantive Procedures Responsive to Significant Risks

21. If the auditor has determined that an assessed risk of material misstatement at the assertion level is a significant risk, the auditor shall perform substantive procedures that are specifically responsive to that risk. When the approach to a significant risk consists only of substantive procedures, those procedures shall include tests of details. (Ref: Para. A53)

Timing of Substantive Procedures

22. If substantive procedures are performed at an interim date, the auditor shall cover the remaining period by performing:

    (a) substantive procedures, combined with tests of controls for the intervening period; or

    (b) if the auditor determines that it is sufficient, further substantive procedures only,

    that provide a reasonable basis for extending the audit conclusions from the interim date to the period end. (Ref: Para. A54–A57)

23. If misstatements that the auditor did not expect when assessing the risks of material misstatement are detected at an interim date, the auditor shall evaluate whether the related assessment of risk and the planned nature, timing or extent of substantive procedures covering the remaining period need to be modified. (Ref: Para. A58)

Adequacy of Presentation of the Financial Statements

24. The auditor shall perform audit procedures to evaluate whether the overall presentation of the financial statements is in accordance with the applicable financial reporting framework. In making this evaluation, the auditor shall consider whether the financial statements are presented in a manner that reflects the appropriate:

    - Classification and description of financial information and the underlying transactions, events and conditions; and
    - Presentation, structure and content of the financial statements. (Ref: Para. A59)

Evaluating the Sufficiency and Appropriateness of Audit Evidence

25. Based on the audit procedures performed and the audit evidence obtained, the auditor shall evaluate before the conclusion of the audit whether the assessments of the risks of material misstatement at the assertion level remain appropriate. (Ref: Para. A60–A61)

26. The auditor shall conclude whether sufficient appropriate audit evidence has been obtained. In forming an opinion, the auditor shall consider all relevant audit evidence, regardless of whether it appears to corroborate or to contradict the assertions in the financial statements. (Ref: Para. A62)

27. If the auditor has not obtained sufficient appropriate audit evidence ~~as to~~ related to a~~n~~ ~~material financial statement~~ relevant assertion about a class of transactions, account balance or disclosure, the auditor shall attempt to obtain further audit evidence. If the auditor is unable to obtain sufficient appropriate audit evidence, the auditor shall express a qualified opinion or disclaim an opinion on the financial statements.

Documentation

28. The auditor shall include in the audit documentation:[106]

    (a) The overall responses to address the assessed risks of material misstatement at the financial statement level, and the nature, timing and extent of the further audit procedures performed;

    (b) The linkage of those procedures with the assessed risks at the assertion level; and

    (c) The results of the audit procedures, including the conclusions where these are not otherwise clear. (Ref: Para. A63)

29. If the auditor plans to use audit evidence about the operating effectiveness of controls obtained in previous audits, the auditor shall include in the audit documentation the conclusions reached about relying on such controls that were tested in a previous audit.

[106] ISA 230, *Audit Documentation*, paragraphs 8–11, and A6

30. The auditor's documentation shall demonstrate that information in the financial statements agrees or reconciles with the underlying accounting records, including agreeing or reconciling disclosures, whether such information is obtained from within or outside of the general and subsidiary ledgers.

Application and Other Explanatory Material

Overall Responses (Ref: Para. 5)

A1. Overall responses to address the assessed risks of material misstatement at the financial statement level may include:

- Emphasizing to the engagement team the need to maintain professional skepticism.
- Assigning more experienced staff or those with special skills or using experts.
- ~~Providing more supervision~~ Changes to the nature, timing and extent of direction and supervision of members of the engagement team and the review of the work performed.
- Incorporating additional elements of unpredictability in the selection of further audit procedures to be performed.
- Changes to the overall audit strategy as required by ISA 300, or planned audit procedures, and may include changes to:
  - The auditor's determination of performance materiality in accordance with ISA 320.
  - The auditor's plans to tests~~s~~ the operating effectiveness of controls, and the persuasiveness of audit evidence needed to support the planned reliance on the operating effectiveness of the controls, particularly when deficiencies in the control environment or the entity's monitoring activities are identified.
  - The nature, timing and extent of substantive procedures. For example, it may be appropriate to perform substantive procedures at or near the date of the financial statements when the risk of material misstatement is assessed as higher.
- ~~Making general changes to the nature, timing or extent of audit procedures, for example: performing substantive procedures at the period end instead of at an interim date; or modifying the nature of audit procedures to obtain more persuasive audit evidence~~.

A2. The assessment of the risks of material misstatement at the financial statement level, and thereby the auditor's overall responses, is affected by the auditor's understanding of the control environment. An effective control environment may allow the auditor to have more confidence in internal control and the reliability of audit evidence generated internally within the entity and thus, for example, allow the auditor to conduct some audit procedures at an interim date rather than at the period end. Deficiencies in the control environment, however, have the opposite effect; for example, the auditor may respond to an ineffective control environment by:

- Conducting more audit procedures as of the period end rather than at an interim date.
- Obtaining more extensive audit evidence from substantive procedures.
- Increasing the number of locations to be included in the audit scope.

A3. Such considerations, therefore, have a significant bearing on the auditor's general approach, for example, an emphasis on substantive procedures (substantive approach), or an approach that uses tests of controls as well as substantive procedures (combined approach).

Audit Procedures Responsive to the Assessed Risks of Material Misstatement at the Assertion Level

The Nature, Timing and Extent of Further Audit Procedures (Ref: Para. 6)

A4. The auditor's assessment of the identified risks of material misstatement at the assertion level provides a basis for considering the appropriate audit approach for designing and performing further audit procedures. For example, the auditor may determine that:

(a) Only by performing tests of controls may the auditor achieve an effective response to the assessed risk of material misstatement for a particular assertion;

(b) Performing only substantive procedures is appropriate for particular assertions and, therefore, the auditor excludes the effect of controls from the ~~relevant risk~~ assessment of the risk of material misstatement. This may be because the ~~auditor's risk assessment procedures have not identified any effective controls relevant to the assertion, or because~~ auditor has not identified a risk for which substantive procedures alone cannot provide sufficient appropriate audit evidence and therefore is not required to test the operating effectiveness of controls. ~~testing controls would be inefficient and~~ Ttherefore, the auditor ~~does~~ may not ~~intend to rely on~~ plan to test the operating effectiveness of controls in determining the nature, timing and extent of substantive procedures; or

(c) A combined approach using both tests of controls and substantive procedures is an effective approach.

The auditor need not design and perform further audit procedures where the assessment of the risk of material misstatement is below the acceptably low level. However, as required by paragraph 18, irrespective of the approach selected and the assessed risk of material misstatement, the auditor designs and performs substantive procedures for each material class of transactions, account balance, and disclosure.

A5. The nature of an audit procedure refers to its purpose (that is, test of controls or substantive procedure) and its type (that is, inspection, observation, inquiry, confirmation, recalculation, reperformance, or analytical procedure). The nature of the audit procedures is of most importance in responding to the assessed risks.

A6. Timing of an audit procedure refers to when it is performed, or the period or date to which the audit evidence applies.

A7. Extent of an audit procedure refers to the quantity to be performed, for example, a sample size or the number of observations of a control ~~activity~~.

A8. Designing and performing further audit procedures whose nature, timing and extent are based on and are responsive to the assessed risks of material misstatement at the assertion level provides a clear linkage between the auditor's further audit procedures and the risk assessment.

Responding to the Assessed Risks at the Assertion Level (Ref: Para. 7(a))

Nature

A9. ISA 315 (Revised 2019) requires that the auditor's assessment of the risks of material misstatement at the assertion level is performed by assessing inherent risk and control risk. The auditor assesses inherent risk by assessing the likelihood and magnitude of a misstatement taking into account how, and the degree to which the inherent risk factors affect the susceptibility to misstatement of relevant assertions.[107] The auditor's assessed risks, including the reasons for those assessed risks, may affect both the types of audit procedures to be performed and their combination. For example, when an assessed risk is high, the auditor may confirm the completeness of the terms of a contract with the counterparty, in addition to inspecting the document. Further, certain audit procedures may be more appropriate for some assertions than others. For example, in relation to revenue, tests of controls may be most responsive to the assessed risk of material misstatement of the completeness assertion, whereas substantive procedures may be most responsive to the assessed risk of material misstatement of the occurrence assertion.

A10. The reasons for the assessment given to a risk are relevant in determining the nature of audit procedures. For example, if an assessed risk is lower because of the particular characteristics of a class of transactions without consideration of the related controls, then the auditor may determine that substantive analytical procedures alone provide sufficient appropriate audit evidence. On the other hand, if the assessed risk is lower because ~~of internal~~ the auditor plans to test the operating effectiveness of controls, and the auditor intends to base the substantive procedures on that low assessment, then the auditor performs tests of those controls, as required by paragraph 8(a). This may be the case, for example, for a class of transactions of reasonably uniform, non-complex characteristics that are routinely processed and controlled by the entity's information system.

Timing

A11. The auditor may perform tests of controls or substantive procedures at an interim date or at the period end. The higher the risk of material misstatement, the more likely it is that the auditor may decide it is more effective to perform substantive procedures nearer to, or at, the period end rather than at an earlier date, or to perform audit procedures unannounced or at unpredictable times (for example, performing audit procedures at selected locations on an unannounced basis). This is particularly relevant when considering the response to the risks of fraud. For example, the auditor may conclude that, when the risks of intentional misstatement or manipulation have been identified, audit procedures to extend audit conclusions from interim date to the period end would not be effective.

A12. On the other hand, performing audit procedures before the period end may assist the auditor in identifying significant matters at an early stage of the audit, and consequently resolving them with the assistance of management or developing an effective audit approach to address such matters.

A13. In addition, certain audit procedures can be performed only at or after the period end, for example:

[107] ISA 315 (Revised 2019), paragraphs 31 and 34

- Agreeing or reconciling information in the financial statements with the underlying accounting records, including agreeing or reconciling disclosures, whether such information is obtained from within or outside of the general and subsidiary ledgers;
- Examining adjustments made during the course of preparing the financial statements; and
- Procedures to respond to a risk that, at the period end, the entity may have entered into improper sales contracts, or transactions may not have been finalized.

A14. Further relevant factors that influence the auditor's consideration of when to perform audit procedures include the following:

- The control environment.
- When relevant information is available (for example, electronic files may subsequently be overwritten, or procedures to be observed may occur only at certain times).
- The nature of the risk (for example, if there is a risk of inflated revenues to meet earnings expectations by subsequent creation of false sales agreements, the auditor may wish to examine contracts available on the date of the period end).
- The period or date to which the audit evidence relates.
- The timing of the preparation of the financial statements, particularly for those disclosures that provide further explanation about amounts recorded in the statement of financial position, the statement of comprehensive income, the statement of changes in equity or the statement of cash flows.

Extent

A15. The extent of an audit procedure judged necessary is determined after considering the materiality, the assessed risk, and the degree of assurance the auditor plans to obtain. When a single purpose is met by a combination of procedures, the extent of each procedure is considered separately. In general, the extent of audit procedures increases as the risk of material misstatement increases. For example, in response to the assessed risk of material misstatement due to fraud, increasing sample sizes or performing substantive analytical procedures at a more detailed level may be appropriate. However, increasing the extent of an audit procedure is effective only if the audit procedure itself is relevant to the specific risk.

A16. The use of computer-assisted audit techniques (CAATs) may enable more extensive testing of electronic transactions and account files, which may be useful when the auditor decides to modify the extent of testing, for example, in responding to the risks of material misstatement due to fraud. Such techniques can be used to select sample transactions from key electronic files, to sort transactions with specific characteristics, or to test an entire population instead of a sample.

Considerations specific to public sector entities

A17. For the audits of public sector entities, the audit mandate and any other special auditing requirements may affect the auditor's consideration of the nature, timing and extent of further audit procedures.

Considerations specific to smaller entities

A18. In the case of very small entities, there may not be many controls ~~activities~~ that could be identified by the auditor, or the extent to which their existence or operation have been documented by the entity may be limited. In such cases, it may be more efficient for the auditor to perform further audit procedures that are primarily substantive procedures. In some rare cases, however, the absence of controls ~~activities~~ or of ~~other~~ components of the system of internal control may make it impossible to obtain sufficient appropriate audit evidence.

Higher Assessments of Risk (Ref: Para 7(b))

A19. When obtaining more persuasive audit evidence because of a higher assessment of risk, the auditor may increase the quantity of the evidence, or obtain evidence that is more relevant or reliable, for example, by placing more emphasis on obtaining third party evidence or by obtaining corroborating evidence from a number of independent sources.

Tests of Controls

Designing and Performing Tests of Controls (Ref: Para. 8)

A20. Tests of controls are performed only on those controls that the auditor has determined are suitably designed to prevent, or detect and correct, a material misstatement in a~~n~~ relevant assertion, and the auditor plans to test those controls. If substantially different controls were used at different times during the period under audit, each is considered separately.

A21. Testing the operating effectiveness of controls is different from obtaining an understanding of and evaluating the design and implementation of controls. However, the same types of audit procedures are used. The auditor may, therefore, decide it is efficient to test the operating effectiveness of controls at the same time as evaluating their design and determining that they have been implemented.

A22. Further, although some risk assessment procedures may not have been specifically designed as tests of controls, they may nevertheless provide audit evidence about the operating effectiveness of the controls and, consequently, serve as tests of controls. For example, the auditor's risk assessment procedures may have included:

- Inquiring about management's use of budgets.
- Observing management's comparison of monthly budgeted and actual expenses.
- Inspecting reports pertaining to the investigation of variances between budgeted and actual amounts.

These audit procedures provide knowledge about the design of the entity's budgeting policies and whether they have been implemented, but may also provide audit evidence about the effectiveness of the operation of budgeting policies in preventing or detecting material misstatements in the classification of expenses.

A23. In addition, the auditor may design a test of controls to be performed concurrently with a test of details on the same transaction. Although the purpose of a test of controls is different from the purpose of a

test of details, both may be accomplished concurrently by performing a test of controls and a test of details on the same transaction, also known as a dual-purpose test. For example, the auditor may design, and evaluate the results of, a test to examine an invoice to determine whether it has been approved and to provide substantive audit evidence of a transaction. A dual-purpose test is designed and evaluated by considering each purpose of the test separately.

A24. In some cases, the auditor may find it impossible to design effective substantive procedures that by themselves provide sufficient appropriate audit evidence at the assertion level.[108] This may occur when an entity conducts its business using IT and no documentation of transactions is produced or maintained, other than through the IT system. In such cases, paragraph 8(b) requires the auditor to perform tests of ~~relevant~~ controls that address the risk for which substantive procedures alone cannot provide sufficient appropriate audit evidence.

Audit Evidence and Intended Reliance (Ref: Para. 9)

A25. A higher level of assurance may be sought about the operating effectiveness of controls when the approach adopted consists primarily of tests of controls, in particular where it is not possible or practicable to obtain sufficient appropriate audit evidence only from substantive procedures.

Nature and Extent of Tests of Controls

Other audit procedures in combination with inquiry (Ref: Para. 10(a))

A26. Inquiry alone is not sufficient to test the operating effectiveness of controls. Accordingly, other audit procedures are performed in combination with inquiry. In this regard, inquiry combined with inspection or reperformance may provide more assurance than inquiry and observation, since an observation is pertinent only at the point in time at which it is made.

A27. The nature of the particular control influences the type of procedure required to obtain audit evidence about whether the control was operating effectively. For example, if operating effectiveness is evidenced by documentation, the auditor may decide to inspect it to obtain audit evidence about operating effectiveness. For other controls, however, documentation may not be available or relevant. For example, documentation of operation may not exist for some factors in the control environment, such as assignment of authority and responsibility, or for some types of controls ~~activities~~, such as automated controls ~~activities performed by a computer~~. In such circumstances, audit evidence about operating effectiveness may be obtained through inquiry in combination with other audit procedures such as observation or the use of CAATs.

Extent of tests of controls

A28. When more persuasive audit evidence is needed regarding the effectiveness of a control, it may be appropriate to increase the extent of testing of the control. As well as the degree of reliance on controls, matters the auditor may consider in determining the extent of tests of controls include the following:

- The frequency of the performance of the control by the entity during the period.

[108] ISA 315 (Revised 2019), paragraph 33~~30~~

- The length of time during the audit period that the auditor is relying on the operating effectiveness of the control.
- The expected rate of deviation from a control.
- The relevance and reliability of the audit evidence to be obtained regarding the operating effectiveness of the control at the assertion level.
- The extent to which audit evidence is obtained from tests of other controls related to the assertion.

ISA 530[109] contains further guidance on the extent of testing.

A29. Because of the inherent consistency of IT processing, it may not be necessary to increase the extent of testing of an automated control. An automated control~~s~~ can be expected to function consistently unless the ~~program~~ IT application (including the tables, files, or other permanent data used by the ~~program~~ IT application) is changed. Once the auditor determines that an automated control is functioning as intended (which could be done at the time the control is initially implemented or at some other date), the auditor may consider performing tests to determine that the control continues to function effectively. Such tests ~~might~~ may include testing the general IT controls related to the IT application. ~~determining that:~~

- ~~Changes to the program are not made without being subject to the appropriate program change controls;~~
- ~~The authorized version of the program is used for processing transactions; and~~
- ~~Other relevant general controls are effective.~~

~~Such tests also might include determining that changes to the programs have not been made, as may be the case when the entity uses packaged software applications without modifying or maintaining them. For example, the auditor may inspect the record of the administration of IT security to obtain audit evidence that unauthorized access has not occurred during the period.~~

A29a. Similarly, the auditor may perform tests of controls that address risks of material misstatement related to the integrity of the entity's data, or the completeness and accuracy of the entity's system-generated reports, or to address risks of material misstatement for which substantive procedures alone cannot provide sufficient appropriate audit evidence. These tests of controls may include tests of general IT controls that address the matters in paragraph 10(a). When this is the case, the auditor may not need to perform any further testing to obtain audit evidence about the matters in paragraph 10(a).

A29b. When the auditor determines that a general IT control is deficient, the auditor may consider the nature of the related risk(s) arising from the use of IT that were identified in accordance with ISA 315 (Revised 2019)[110] to provide the basis for the design of the auditor's additional procedures to address the assessed risk of material misstatement. Such procedures may address determining whether:

[109] ISA 530, *Audit Sampling*

[110] ISA 315 (Revised 2019), paragraph 26(c)(i)

- The related risk(s) arising from IT has occurred. For example, if users have unauthorized access to an IT application (but cannot access or modify the system logs that track access), the auditor may inspect the system logs to obtain audit evidence that those users did not access the IT application during the period.
- There are any alternate or redundant general IT controls, or any other controls, that address the related risk(s) arising from the use of IT. If so, the auditor may identify such controls (if not already identified) and therefore evaluate their design, determine that they have been implemented and perform tests of their operating effectiveness. For example, if a general IT control related to user access is deficient, the entity may have an alternate control whereby IT management reviews end user access reports on a timely basis. Circumstances when an application control may address a risk arising from the use of IT may include when the information that may be affected by the general IT control deficiency can be reconciled to external sources (e.g., a bank statement) or internal sources not affected by the general IT control deficiency (e.g., a separate IT application or data source).

Testing of indirect controls (Ref: Para. 10(b))

A30. In some circumstances, it may be necessary to obtain audit evidence supporting the effective operation of indirect controls (e.g., general IT controls). As explained in paragraphs A29 to A29b, general IT controls may have been identified in accordance with ISA 315 (Revised 2019) because of their support of the operating effectiveness of automated controls or due to their support in maintaining the integrity of information used in the entity's financial reporting, including system-generated reports. The requirement in paragraph 10(b) acknowledges that the auditor may have already tested certain indirect controls to address the matters in paragraph 10(a). ~~For example, when the auditor decides to test the effectiveness of a user review of exception reports detailing sales in excess of authorized credit limits, the user review and related follow up is the control that is directly of relevance to the auditor. Controls over the accuracy of the information in the reports (for example, general IT controls) are described as "indirect" controls.~~

~~A31. Because of the inherent consistency of IT processing, audit evidence about the implementation of an automated application control, when considered in combination with audit evidence about the operating effectiveness of the entity's general controls (in particular, change controls), may also provide substantial audit evidence about its operating effectiveness.~~

Timing of Tests of Controls

Intended period of reliance (Ref: Para. 11)

A32. Audit evidence pertaining only to a point in time may be sufficient for the auditor's purpose, for example, when testing controls over the entity's physical inventory counting at the period end. If, on the other hand, the auditor intends to rely on a control over a period, tests that are capable of providing audit evidence that the control operated effectively at relevant times during that period are appropriate. Such tests may include tests of controls in the entity's process to monitor~~ing of~~ the system of internal controls.

Using audit evidence obtained during an interim period (Ref: Para. 12(b))

A33. Relevant factors in determining what additional audit evidence to obtain about controls that were operating during the period remaining after an interim period, include:

- The significance of the assessed risks of material misstatement at the assertion level.
- The specific controls that were tested during the interim period, and significant changes to them since they were tested, including changes in the information system, processes, and personnel.
- The degree to which audit evidence about the operating effectiveness of those controls was obtained.
- The length of the remaining period.
- The extent to which the auditor intends to reduce further substantive procedures based on the reliance of controls.
- The control environment.

A34. Additional audit evidence may be obtained, for example, by extending tests of controls over the remaining period or testing the entity's monitoring of controls.

Using audit evidence obtained in previous audits (Ref: Para. 13)

A35. In certain circumstances, audit evidence obtained from previous audits may provide audit evidence where the auditor performs audit procedures to establish its continuing relevance and reliability. For example, in performing a previous audit, the auditor may have determined that an automated control was functioning as intended. The auditor may obtain audit evidence to determine whether changes to the automated control have been made that affect its continued effective functioning through, for example, inquiries of management and the inspection of logs to indicate what controls have been changed. Consideration of audit evidence about these changes may support either increasing or decreasing the expected audit evidence to be obtained in the current period about the operating effectiveness of the controls.

Controls that have changed from previous audits (Ref: Para. 14(a))

A36. Changes may affect the relevance and reliability of the audit evidence obtained in previous audits such that there may no longer be a basis for continued reliance. For example, changes in a system that enable an entity to receive a new report from the system probably do not affect the relevance of audit evidence from a previous audit; however, a change that causes data to be accumulated or calculated differently does affect it.

Controls that have not changed from previous audits (Ref: Para. 14(b))

A37. The auditor's decision on whether to rely on audit evidence obtained in previous audits for controls that:

(a) have not changed since they were last tested; and

(b) are not controls that mitigate a significant risk,

is a matter of professional judgment. In addition, the length of time between retesting such controls is also a matter of professional judgment, but is required by paragraph 14 (b) to be at least once in every third year.

A38. In general, the higher the risk of material misstatement, or the greater the reliance on controls, the shorter the time period elapsed, if any, is likely to be. Factors that may decrease the period for retesting a control, or result in not relying on audit evidence obtained in previous audits at all, include the following:

- A deficient control environment.
- A ~~D~~deficiency~~t~~ in the entity's process to monitor~~ing of~~ the system of internal control~~s~~.
- A significant manual element to ~~the relevant~~ controls.
- Personnel changes that significantly affect the application of the control.
- Changing circumstances that indicate the need for changes in the control.
- Deficient general IT controls.

A39. When there are a number of controls for which the auditor intends to rely on audit evidence obtained in previous audits, testing some of those controls in each audit provides corroborating information about the continuing effectiveness of the control environment. This contributes to the auditor's decision about whether it is appropriate to rely on audit evidence obtained in previous audits.

Evaluating the Operating Effectiveness of Controls (Ref: Para.16–17)

A40. A material misstatement detected by the auditor's procedures is a strong indicator of the existence of a significant deficiency in internal control.

A41. The concept of effectiveness of the operation of controls recognizes that some deviations in the way controls are applied by the entity may occur. Deviations from prescribed controls may be caused by such factors as changes in key personnel, significant seasonal fluctuations in volume of transactions and human error. The detected rate of deviation, in particular in comparison with the expected rate, may indicate that the control cannot be relied on to reduce risk at the assertion level to that assessed by the auditor.

Substantive Procedures (Ref: Para. 6, 18)

A42. Paragraph 18 requires the auditor to design and perform substantive procedures for each material class of transactions, account balance, and disclosure~~, irrespective of the assessed risks of material misstatement~~. For significant classes of transactions, account balances and disclosures, substantive procedures may have already been performed because paragraph 6 requires the auditor to design and perform further audit procedures that are responsive to the assessed risks of material misstatement at the assertion level. Accordingly, substantive procedures are required to be designed and performed in accordance with paragraph 18:

- When the further audit procedures for significant classes of transactions, account balances or disclosures, designed and performed in accordance with paragraph 6, did not include substantive procedures; or
- For each class of transactions, account balance or disclosure that is not a significant class of transactions, account balance or disclosure, but that has been identified as material in accordance with ISA 315 (Revised 2019).[111]
- This requirement reflects the facts that: (a) the auditor's assessment of risk is judgmental and so may not identify all risks of material misstatement; and (b) there are inherent limitations to ~~internal~~ controls, including management override.

A42a. Not all assertions within a material class of transactions, account balance or disclosure are required to be tested. Rather, in designing the substantive procedures to be performed, the auditor's consideration of the assertion(s) in which, if a misstatement were to occur, there is a reasonable possibility of the misstatement being material, may assist in identifying the appropriate nature, timing and extent of the procedures to be performed.

Nature and Extent of Substantive Procedures

A43. Depending on the circumstances, the auditor may determine that:

- Performing only substantive analytical procedures will be sufficient to reduce audit risk to an acceptably low level. For example, where the auditor's assessment of risk is supported by audit evidence from tests of controls.
- Only tests of details are appropriate.
- A combination of substantive analytical procedures and tests of details are most responsive to the assessed risks.

A44. Substantive analytical procedures are generally more applicable to large volumes of transactions that tend to be predictable over time. ISA 520[112] establishes requirements and provides guidance on the application of analytical procedures during an audit.

A45. The ~~nature~~ assessment of the risk ~~and~~ or the nature of the assertion is relevant to the design of tests of details. For example, tests of details related to the existence or occurrence assertion may involve selecting from items contained in a financial statement amount and obtaining the relevant audit evidence. On the other hand, tests of details related to the completeness assertion may involve selecting from items that are expected to be included in the relevant financial statement amount and investigating whether they are included.

A10. Because the assessment of the risk of material misstatement takes account of ~~internal~~ controls that the auditor plans to test, the extent of substantive procedures may need to be increased when the results from tests of controls are unsatisfactory. However, increasing the extent of an audit procedure is appropriate only if the audit procedure itself is relevant to the specific risk.

---

111 ISA 315 (Revised 2019), paragraph 36

112 ISA 520, *Analytical Procedures*

A47. In designing tests of details, the extent of testing is ordinarily thought of in terms of the sample size. However, other matters are also relevant, including whether it is more effective to use other selective means of testing. See ISA 500.[113]

Considering Whether External Confirmation Procedures Are to Be Performed (Ref: Para. 19)

A48. External confirmation procedures frequently are relevant when addressing assertions associated with account balances and their elements, but need not be restricted to these items. For example, the auditor may request external confirmation of the terms of agreements, contracts, or transactions between an entity and other parties. External confirmation procedures also may be performed to obtain audit evidence about the absence of certain conditions. For example, a request may specifically seek confirmation that no "side agreement" exists that may be relevant to an entity's revenue cutoff assertion. Other situations where external confirmation procedures may provide relevant audit evidence in responding to assessed risks of material misstatement include:

- Bank balances and other information relevant to banking relationships.
- Accounts receivable balances and terms.
- Inventories held by third parties at bonded warehouses for processing or on consignment.
- Property title deeds held by lawyers or financiers for safe custody or as security.
- Investments held for safekeeping by third parties, or purchased from stockbrokers but not delivered at the balance sheet date.
- Amounts due to lenders, including relevant terms of repayment and restrictive covenants.
- Accounts payable balances and terms.

A49. Although external confirmations may provide relevant audit evidence relating to certain assertions, there are some assertions for which external confirmations provide less relevant audit evidence. For example, external confirmations provide less relevant audit evidence relating to the recoverability of accounts receivable balances, than they do of their existence.

A50. The auditor may determine that external confirmation procedures performed for one purpose provide an opportunity to obtain audit evidence about other matters. For example, confirmation requests for bank balances often include requests for information relevant to other financial statement assertions. Such considerations may influence the auditor's decision about whether to perform external confirmation procedures.

A51. Factors that may assist the auditor in determining whether external confirmation procedures are to be performed as substantive audit procedures include:

- The confirming party's knowledge of the subject matter – responses may be more reliable if provided by a person at the confirming party who has the requisite knowledge about the information being confirmed.

[113] ISA 500, *Audit Evidence*, paragraph 10

- The ability or willingness of the intended confirming party to respond – for example, the confirming party:
    - May not accept responsibility for responding to a confirmation request;
    - May consider responding too costly or time consuming;
    - May have concerns about the potential legal liability resulting from responding;
    - May account for transactions in different currencies; or
    - May operate in an environment where responding to confirmation requests is not a significant aspect of day-to-day operations.

  In such situations, confirming parties may not respond, may respond in a casual manner or may attempt to restrict the reliance placed on the response.
- The objectivity of the intended confirming party – if the confirming party is a related party of the entity, responses to confirmation requests may be less reliable.

Substantive Procedures Related to the Financial Statement Closing Process (Ref: Para. 20)

A52. The nature, and also the extent, of the auditor's substantive procedures related to the financial statement closing process depends on the nature and complexity of the entity's financial reporting process and the related risks of material misstatement.

Substantive Procedures Responsive to Significant Risks (Ref: Para. 21)

A53. Paragraph 21 of this ISA requires the auditor to perform substantive procedures that are specifically responsive to risks the auditor has determined to be significant risks. Audit evidence in the form of external confirmations received directly by the auditor from appropriate confirming parties may assist the auditor in obtaining audit evidence with the high level of reliability that the auditor requires to respond to significant risks of material misstatement, whether due to fraud or error. For example, if the auditor identifies that management is under pressure to meet earnings expectations, there may be a risk that management is inflating sales by improperly recognizing revenue related to sales agreements with terms that preclude revenue recognition or by invoicing sales before shipment. In these circumstances, the auditor may, for example, design external confirmation procedures not only to confirm outstanding amounts, but also to confirm the details of the sales agreements, including date, any rights of return and delivery terms. In addition, the auditor may find it effective to supplement such external confirmation procedures with inquiries of non-financial personnel in the entity regarding any changes in sales agreements and delivery terms.

Timing of Substantive Procedures (Ref: Para. 22–23)

A54. In most cases, audit evidence from a previous audit's substantive procedures provides little or no audit evidence for the current period. There are, however, exceptions, for example, a legal opinion obtained in a previous audit related to the structure of a securitization to which no changes have occurred, may be relevant in the current period. In such cases, it may be appropriate to use audit evidence from a previous audit's substantive procedures if that evidence and the related subject

matter have not fundamentally changed, and audit procedures have been performed during the current period to establish its continuing relevance.

Using audit evidence obtained during an interim period (Ref: Para. 22)

A55. In some circumstances, the auditor may determine that it is effective to perform substantive procedures at an interim date, and to compare and reconcile information concerning the balance at the period end with the comparable information at the interim date to:

(a) Identify amounts that appear unusual;

(b) Investigate any such amounts; and

(c) Perform substantive analytical procedures or tests of details to test the intervening period.

A56. Performing substantive procedures at an interim date without undertaking additional procedures at a later date increases the risk that the auditor will not detect misstatements that may exist at the period end. This risk increases as the remaining period is lengthened. Factors such as the following may influence whether to perform substantive procedures at an interim date:

- The control environment and other ~~relevant~~ controls.
- The availability at a later date of information necessary for the auditor's procedures.
- The purpose of the substantive procedure.
- The assessed risk of material misstatement.
- The nature of the class of transactions or account balance and related assertions.
- The ability of the auditor to perform appropriate substantive procedures or substantive procedures combined with tests of controls to cover the remaining period in order to reduce the risk that misstatements that may exist at the period end will not be detected.

A57. Factors such as the following may influence whether to perform substantive analytical procedures with respect to the period between the interim date and the period end:

- Whether the period-end balances of the particular classes of transactions or account balances are reasonably predictable with respect to amount, relative significance, and composition.
- Whether the entity's procedures for analyzing and adjusting such classes of transactions or account balances at interim dates and for establishing proper accounting cutoffs are appropriate.
- Whether the information system ~~relevant to financial reporting~~ will provide information concerning the balances at the period end and the transactions in the remaining period that is sufficient to permit investigation of:

  (a) Significant unusual transactions or entries (including those at or near the period end);

  (b) Other causes of significant fluctuations, or expected fluctuations that did not occur; and

  (c) Changes in the composition of the classes of transactions or account balances.

Misstatements detected at an interim date (Ref: Para. 23)

A58. When the auditor concludes that the planned nature, timing or extent of substantive procedures covering the remaining period need to be modified as a result of unexpected misstatements detected at an interim date, such modification may include extending or repeating the procedures performed at the interim date at the period end.

Adequacy of Presentation of the Financial Statements (Ref: Para. 24)

A59. Evaluating the appropriate presentation, arrangement and content of the financial statements includes, for example, consideration of the terminology used as required by the applicable financial reporting framework, the level of detail provided, the aggregation and disaggregation of amounts and the bases of amounts set forth.

Evaluating the Sufficiency and Appropriateness of Audit Evidence (Ref: Para. 25–27)

A60. An audit of financial statements is a cumulative and iterative process. As the auditor performs planned audit procedures, the audit evidence obtained may cause the auditor to modify the nature, timing or extent of other planned audit procedures. Information may come to the auditor's attention that differs significantly from the information on which the risk assessment was based. For example:

- The extent of misstatements that the auditor detects by performing substantive procedures may alter the auditor's judgment about the risk assessments and may indicate a significant deficiency in internal control.
- The auditor may become aware of discrepancies in accounting records, or conflicting or missing evidence.
- Analytical procedures performed at the overall review stage of the audit may indicate a previously unrecognized risk of material misstatement.

In such circumstances, the auditor may need to reevaluate the planned audit procedures, based on the revised consideration of assessed risks of material misstatement ~~for all or some of~~ and the effect on the significant classes of transactions, account balances, or disclosures and ~~related~~ their relevant assertions. ISA 315 (Revised 2019) contains further guidance on revising the auditor's risk assessment.[114]

A61. The auditor cannot assume that an instance of fraud or error is an isolated occurrence. Therefore, the consideration of how the detection of a misstatement affects the assessed risks of material misstatement is important in determining whether the assessment remains appropriate.

A62. The auditor's judgment as to what constitutes sufficient appropriate audit evidence is influenced by such factors as the following:

- Significance of the potential misstatement in the assertion and the likelihood of its having a material effect, individually or aggregated with other potential misstatements, on the financial statements.

[114] ISA 315 (Revised 2019), paragraph 53~~31~~

- Effectiveness of management's responses and controls to address the risks.
- Experience gained during previous audits with respect to similar potential misstatements.
- Results of audit procedures performed, including whether such audit procedures identified specific instances of fraud or error.
- Source and reliability of the available information.
- Persuasiveness of the audit evidence.
- Understanding of the entity and its environment, the applicable financial reporting framework and ~~including~~ the entity's system of internal control.

Documentation (Ref: Para. 28)

A63. The form and extent of audit documentation is a matter of professional judgment, and is influenced by the nature, size and complexity of the entity and its system of internal control, availability of information from the entity and the audit methodology and technology used in the audit.

ISA 500, *Audit Evidence*

Application and Other Explanatory Material

Sufficient Appropriate Audit Evidence (Ref: Para. 6)

A1. Audit evidence is necessary to support the auditor's opinion and report. It is cumulative in nature and is primarily obtained from audit procedures performed during the course of the audit. It may, however, also include information obtained from other sources such as previous audits (provided the auditor has evaluated whether such information remains relevant and reliable as audit evidence for the current audit ~~determined whether changes have occurred since the previous audit that may affect its relevance to the current audit~~) or a firm's quality control procedures for client acceptance and continuance. In addition to other sources inside and outside the entity, the entity's accounting records are an important source of audit evidence. Also, information that may be used as audit evidence may have been prepared using the work of a management's expert. Audit evidence comprises both information that supports and corroborates management's assertions, and any information that contradicts such assertions. In addition, in some cases the absence of information (for example, management's refusal to provide a requested representation) is used by the auditor, and therefore, also constitutes audit evidence.

…

Audit Procedures for Obtaining Audit Evidence

…

Observation

A17. Observation consists of looking at a process or procedure being performed by others, for example, the auditor's observation of inventory counting by the entity's personnel, or of the performance of

controls ~~activities~~. Observation provides audit evidence about the performance of a process or procedure, but is limited to the point in time at which the observation takes place, and by the fact that the act of being observed may affect how the process or procedure is performed. See ISA 501 for further guidance on observation of the counting of inventory.

…

ISA 501, *Audit Evidence—Special Considerations for Selected Items*

Application and Other Explanatory Material

Inventory

Attendance at Physical Inventory Counting (Ref: Para. 4(a))

…

Evaluate Management's Instructions and Procedures (Ref: Para. 4(a)(i))

A4. Matters relevant in evaluating management's instructions and procedures for recording and controlling the physical inventory counting include whether they address, for example:

- The application of appropriate controls ~~activities~~, for example, collection of used physical inventory count records, accounting for unused physical inventory count records, and count and re-count procedures.

…

ISA 530, *Audit Documentation*

Application and Other Explanatory Material

…

Sample Design, Size, and Selection of Items for Testing

Sample Design (Ref: Para. 6)

…

A7. In considering the characteristics of a population, for tests of controls, the auditor makes an assessment of the expected rate of deviation based on the auditor's understanding of the ~~relevant~~ controls or on the examination of a small number of items from the population. This assessment is made in order to design an audit sample and to determine sample size….

…

Appendix 2 (Ref: Para. A11)

Example of Factors Influencing Sample Size for Test of Controls

The following are factors that the auditor may consider when determining the sample size for tests of controls. These factors, which need to be considered together, assume the auditor does not modify the nature or timing of tests of controls or otherwise modify the approach to substantive procedures in response to assessed risks.

Factor 1 An increase in the extent to which the auditor's risk assessment takes into account ~~relevant~~ plans to test the operating effectiveness of controls.

…

ISA 550, Related Parties

Application and Other Explanatory Material

…

Risk Assessment Procedures and Related Activities

…

Understanding the Entity's Related Party Relationships and Transactions

Discussion among the Engagement Team (Ref: Para. 12)

A9. Matters that may be addressed in the discussion among the engagement team include:

- …
- The importance that management and those charged with governance attach to the identification, appropriate accounting for, and disclosure of related party relationships and transactions (if the applicable financial reporting framework establishes related party requirements), and the related risk of management override of ~~relevant~~ controls.

…

The Identity of the Entity's Related Parties (Ref: Para. 13(a))

…

A12. However, where the framework does not establish related party requirements, the entity may not have such information systems in place. Under such circumstances, it is possible that management may not be aware of the existence of all related parties. Nevertheless, the requirement to make the inquiries specified by paragraph 13 still applies because management may be aware of parties that meet the related party definition set out in this ISA. In such a case, however, the auditor's inquiries regarding the identity of the entity's related parties are likely to form part of the auditor's risk

assessment procedures and related activities performed in accordance with ISA 315 (Revised 2019) to obtain information regarding the entity's organizational structure, ownership, governance and business model.~~:~~

- ~~The entity's ownership and governance structures;~~
- ~~The types of investments that the entity is making and plans to make; and~~
- ~~The way the entity is structured and how it is financed.~~

In the particular case of common control relationships, as management is more likely to be aware of such relationships if they have economic significance to the entity, the auditor's inquiries are likely to be more effective if they are focused on whether parties with which the entity engages in significant transactions, or shares resources to a significant degree, are related parties.

…

Considerations specific to smaller entities

A20. Controls ~~activities~~ in smaller entities are likely to be less formal and smaller entities may have no documented processes for dealing with related party relationships and transactions. An owner-manager may mitigate some of the risks arising from related party transactions, or potentially increase those risks, through active involvement in all the main aspects of the transactions. For such entities, the auditor may obtain an understanding of the related party relationships and transactions, and any controls that may exist over these, through inquiry of management combined with other procedures, such as observation of management's oversight and review activities, and inspection of available relevant documentation.

…

Sharing Related Party Information with the Engagement Team (Ref: Para. 17)

A28. Relevant related party information that may be shared among the engagement team members includes, for example:

- The identity of the entity's related parties.
- The nature of the related party relationships and transactions.

Significant or complex related party relationships or transactions that may be determined to be significant risks ~~require special audit consideration~~, in particular transactions in which management or those charged with governance are financially involved.

…

Responses to the Risks of Material Misstatement Associated with Related Party Relationships and Transactions (Ref: Para. 20)

…

A34. Depending upon the results of the auditor's risk assessment procedures, the auditor may consider it appropriate to obtain audit evidence without testing the entity's controls over related party

relationships and transactions. In some circumstances, however, it may not be possible to obtain sufficient appropriate audit evidence from substantive audit procedures alone in relation to the risks of material misstatement associated with related party relationships and transactions. For example, where intra-group transactions between the entity and its components are numerous and a significant amount of information regarding these transactions is initiated, recorded, processed or reported electronically in an integrated system, the auditor may determine that it is not possible to design effective substantive audit procedures that by themselves would reduce the risks of material misstatement associated with these transactions to an acceptably low level. In such a case, in meeting the ISA 330 requirement to obtain sufficient appropriate audit evidence as to the operating effectiveness of ~~relevant~~ controls,[115] the auditor is required to test the entity's controls over the completeness and accuracy of the recording of the related party relationships and transactions.

…

ISA 540 (Revised), *Auditing Accounting Estimates and Related Disclosures*

Introduction

Scope of this ISA

1. This International Standard on Auditing (ISA) deals with the auditor's responsibilities relating to accounting estimates and related disclosures in an audit of financial statements. Specifically, it includes requirements and guidance that refer to, or expand on, how ISA 315 (Revised 2019),[116] ISA 330,[117] ISA 450,[118] ISA 500[119] and other relevant ISAs are to be applied in relation to accounting estimates and related disclosures. It also includes requirements and guidance on the evaluation of misstatements of accounting estimates and related disclosures, and indicators of possible management bias.

Nature of Accounting Estimates

2. Accounting estimates vary widely in nature and are required to be made by management when the monetary amounts cannot be directly observed. The measurement of these monetary amounts is subject to estimation uncertainty, which reflects inherent limitations in knowledge or data. These limitations give rise to inherent subjectivity and variation in the measurement outcomes. The process of making accounting estimates involves selecting and applying a method using assumptions and data, which requires judgment by management and can give rise to complexity in measurement. The effects of complexity, subjectivity or other inherent risk factors on the measurement of these monetary amounts affects their susceptibility to misstatement. (Ref: Para. A1–A6, Appendix 1)

---

115 ISA 330, paragraph 8(b)

116 ISA 315 (Revised 2019), *Identifying and Assessing the Risks of Material Misstatement ~~through Understanding the Entity and Its Environment~~*

117 ISA 330, *The Auditor's Responses to Assessed Risks*

118 ISA 450, *Evaluation of Misstatements Identified during the Audit*

119 ISA 500, *Audit Evidence*

3. Although this ISA applies to all accounting estimates, the degree to which an accounting estimate is subject to estimation uncertainty will vary substantially. The nature, timing and extent of the risk assessment and further audit procedures required by this ISA will vary in relation to the estimation uncertainty and the assessment of the related risks of material misstatement. For certain accounting estimates, estimation uncertainty may be very low, based on their nature, and the complexity and subjectivity involved in making them may also be very low. For such accounting estimates, the risk assessment procedures and further audit procedures required by this ISA would not be expected to be extensive. When estimation uncertainty, complexity or subjectivity are very high, such procedures would be expected to be much more extensive. This ISA contains guidance on how the requirements of this ISA can be scaled. (Ref: Para. A7)

Key Concepts of This ISA

4. ~~This~~ ISA 315 (Revised 2019) requires a separate assessment of inherent risk for identified risks of material misstatement at the assertion level.[120] ~~purposes of assessing the risks of material misstatement at the assertion level for accounting estimates.~~ In the context of ISA 540 (Revised), and ~~D~~depending on the nature of a particular accounting estimate, the susceptibility of an assertion to a misstatement that could be material may be subject to or affected by estimation uncertainty, complexity, subjectivity or other inherent risk factors, and the interrelationship among them. As explained in ISA 200,[121] inherent risk is higher for some assertions and related classes of transactions, account balances and disclosures than for others. Accordingly, the assessment of inherent risk depends on the degree to which the inherent risk factors affect the likelihood or magnitude of misstatement, and varies on a scale that is referred to ~~in this ISA~~ as the spectrum of inherent risk. (Ref: Para. A8–A9, A65–A66, Appendix 1)

5. This ISA refers to relevant requirements in ISA 315 (Revised 2019) and ISA 330, and provides related guidance, to emphasize the importance of the auditor's decisions about controls relating to accounting estimates, including decisions about whether:

   - There are controls ~~relevant to the audit~~ required to be identified by ISA 315 (Revised 2019), for which the auditor is required to evaluate their design and determine whether they have been implemented.
   - To test the operating effectiveness of ~~relevant~~ controls.

6. ~~This~~ ISA 315 (Revised 2019) also requires a separate assessment of control risk when assessing the risks of material misstatement at the assertion level ~~for accounting estimates~~. In assessing control risk, the auditor takes into account whether the auditor's further audit procedures contemplate planned reliance on the operating effectiveness of controls. If the auditor does not ~~perform~~ plan to test~~s~~ the operating effectiveness of controls, or does not intend to rely on the operating effectiveness of controls, the auditor's assessment of ~~the risk of material misstatement at the assertion level~~ control risk ~~cannot be reduced for the effective operation of controls with respect to the particular assertion~~

[120] ISA 315 (Revised 2019), paragraph 31

[121] ISA 200*, Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with International Standards on Auditing*, paragraph A40

is such that the assessment of the risk of material misstatement is the same as the assessment of inherent risk.[122] (Ref: Para. A10)

7. This ISA emphasizes that the auditor's further audit procedures (including, where appropriate, tests of controls) need to be responsive to the reasons for the assessed risks of material misstatement at the assertion level, taking into account the effect of one or more inherent risk factors and the auditor's assessment of control risk.

8. The exercise of professional skepticism in relation to accounting estimates is affected by the auditor's consideration of inherent risk factors, and its importance increases when accounting estimates are subject to a greater degree of estimation uncertainty or are affected to a greater degree by complexity, subjectivity or other inherent risk factors. Similarly, the exercise of professional skepticism is important when there is greater susceptibility to misstatement due to management bias or fraud other fraud risk factors insofar as they affect inherent risk. (Ref: Para. A11)

…

…

Objective

…

Definitions

…

Requirements

Risk Assessment Procedures and Related Activities

13. When obtaining an understanding of the entity and its environment, the applicable financial reporting framework and including the entity's system of internal control, as required by ISA 315 (Revised 2019),[123] the auditor shall obtain an understanding of the following matters related to the entity's accounting estimates. The auditor's procedures to obtain the understanding shall be performed to the extent necessary to obtain audit evidence that provides an appropriate basis for the identification and assessment of risks of material misstatement at the financial statement and assertion levels. (Ref: Para. A19–A22)

Obtaining an Understanding of tThe Entity and Its Environment and the Applicable Financial Reporting Framework

(a) The entity's transactions and other events orand conditions that may give rise to the need for, or changes in, accounting estimates to be recognized or disclosed in the financial statements. (Ref: Para. A23)

---

[122] ISA 530, *Audit Sampling*, Appendix 3

[123] ISA 315 (Revised 2019), paragraphs 3, 5–6, 9, 11–12, 15-17, and 20-2119–27

(b) The requirements of the applicable financial reporting framework related to accounting estimates (including the recognition criteria, measurement bases, and the related presentation and disclosure requirements); and how they apply in the context of the nature and circumstances of the entity and its environment, including how ~~transactions and other events or conditions are subject to, or affected by,~~ the inherent risk factors affect susceptibility to misstatement of assertions. (Ref: Para. A24–A25)

(c) Regulatory factors relevant to the entity's accounting estimates, including, when applicable, regulatory frameworks related to prudential supervision. (Ref: Para. A26)

(d) The nature of the accounting estimates and related disclosures that the auditor expects to be included in the entity's financial statements, based on the auditor's understanding of the matters in 13(a)–(c) above. (Ref: Para. A27)

Obtaining an Understanding of t~~T~~he Entity's System of Internal Control

(e) The nature and extent of oversight and governance that the entity has in place over management's financial reporting process relevant to accounting estimates. (Ref: Para. A28–A30).

(f) How management identifies the need for, and applies, specialized skills or knowledge related to accounting estimates, including with respect to the use of a management's expert. (Ref: Para. A31)

(g) How the entity's risk assessment process identifies and addresses risks relating to accounting estimates. (Ref: Para. A32–A33)

(h) The entity's information system as it relates to accounting estimates, including:

(i) How information relating to accounting estimates and related disclosures for significant classes of transactions, account balances or disclosures flows through the entity's information system ~~The classes of transactions, events and conditions, that are significant to the financial statements and that give rise to the need for, or changes in, accounting estimates and related disclosures~~; and (Ref: Para. A34–A35)

(ii) For such accounting estimates and related disclosures, how management:

a. Identifies the relevant methods, assumptions or sources of data, and the need for changes in them, that are appropriate in the context of the applicable financial reporting framework, including how management: (Ref: Para. A36–A37)

i. Selects or designs, and applies, the methods used, including the use of models; (Ref: Para. A38–A39)

ii. Selects the assumptions to be used, including consideration of alternatives, and identifies significant assumptions; (Ref: Para. A40–A43); and

iii. Selects the data to be used; (Ref: Para. A44)

b. Understands the degree of estimation uncertainty, including through considering the range of possible measurement outcomes; and (Ref: Para. A45)

c. Addresses the estimation uncertainty, including selecting a point estimate and related disclosures for inclusion in the financial statements. (Ref: Para.A46–A49)

(i) Identified controls in the control activities component[124] ~~activities relevant to the audit~~ over management's process for making accounting estimates as described in paragraph 13(h)(ii). (Ref: Para. A50–A54)

(j) How management reviews the outcome(s) of previous accounting estimates and responds to the results of that review.

14. The auditor shall review the outcome of previous accounting estimates, or, where applicable, their subsequent re-estimation to assist in identifying and assessing the risks of material misstatement in the current period. The auditor shall take into account the characteristics of the accounting estimates in determining the nature and extent of that review. The review is not intended to call into question judgments about previous period accounting estimates that were appropriate based on the information available at the time they were made. (Ref: Para. A55–A60)

…

Identifying and Assessing the Risks of Material Misstatement

16. In identifying and assessing the risks of material misstatement relating to an accounting estimate and related disclosures at the assertion level, including separately assessing inherent risk and control risk at the assertion level, as required by ISA 315 (Revised 2019),[125] the auditor shall ~~separately assess inherent risk and control risk. The auditor shall~~ take the following into account in identifying the risks of material misstatement and in assessing inherent risk: (Ref: Para. A64–A71)

(a) The degree to which the accounting estimate is subject to estimation uncertainty; and (Ref: Para. A72–A75)

(b) The degree to which the following are affected by complexity, subjectivity, or other inherent risk factors: (Ref: Para. A76–A79)

(i) The selection and application of the method, assumptions and data in making the accounting estimate; or

(ii) The selection of management's point estimate and related disclosures for inclusion in the financial statements.

17. The auditor shall determine whether any of the risks of material misstatement identified and assessed in accordance with paragraph 16 are, in the auditor's judgment, a significant risk.[126] If the auditor has determined that a significant risk exists, the auditor shall identify controls that ~~obtain an understanding of the entity's controls, including control activities, relevant to~~ address that risk.[127] and evaluate

[124] ISA 315 (Revised 2019), paragraphs 26(a)(i)–(iv)

[125] ISA 315 (Revised 2019), paragraph ~~25 and 26~~31 and 34

[126] ISA 315 (Revised 2019), paragraph 32~~27~~

[127] ISA 315 (Revised 2019), paragraph 26(a)(i)~~29~~

whether such controls have been designed effectively, and determine whether they have been implemented.[128] (Ref: Para. A80)

…

19. As required by ISA 330,[129] the auditor shall design and perform tests to obtain sufficient appropriate audit evidence as to the operating effectiveness of ~~relevant~~ controls, if:

    (b) The auditor's assessment of risks of material misstatement at the assertion level includes an expectation that the controls are operating effectively; or

    (c) Substantive procedures alone cannot provide sufficient appropriate audit evidence at the assertion level.

    In relation to accounting estimates, the auditor's tests of such controls shall be responsive to the reasons for the assessment given to the risks of material misstatement. In designing and performing tests of controls, the auditor shall obtain more persuasive audit evidence the greater the reliance the auditor places on the effectiveness of a control.[130] (Ref: Para. A85–A89)

…

Other Considerations Relating to Audit Evidence

30. In obtaining audit evidence regarding the risks of material misstatement relating to accounting estimates, irrespective of the sources of information to be used as audit evidence, the auditor shall comply with the relevant requirements in ISA 500.

    When using the work of a management's expert, the requirements in paragraphs 21–29 of this ISA may assist the auditor in evaluating the appropriateness of the expert's work as audit evidence for a relevant assertion in accordance with paragraph 8(c) of ISA 500. In evaluating the work of the management's expert, the nature, timing and extent of the further audit procedures are affected by the auditor's evaluation of the expert's competence, capabilities and objectivity, the auditor's understanding of the nature of the work performed by the expert, and the auditor's familiarity with the expert's field of expertise. (Ref: Para. A126–A132)

…

Documentation

39. The auditor shall include in the audit documentation:[131] (Ref: Para. A149–A152)

    (a) Key elements of the auditor's understanding of the entity and its environment, including the entity's internal control related to the entity's accounting estimates;

    (b) The linkage of the auditor's further audit procedures with the assessed risks of material

---

[128] ISA 315 (Revised 2019), paragraph 26(a)

[129] ISA 330, paragraph 8

[130] ISA 330, paragraph 9

[131] ISA 230, *Audit Documentation*, paragraphs 8–11, A6, A7 and A10

misstatement at the assertion level,[132] taking into account the reasons (whether related to inherent risk or control risk) given to the assessment of those risks;

(c) The auditor's response(s) when management has not taken appropriate steps to understand and address estimation uncertainty;

(d) Indicators of possible management bias related to accounting estimates, if any, and the auditor's evaluation of the implications for the audit, as required by paragraph 32; and

(e) Significant judgments relating to the auditor's determination of whether the accounting estimates and related disclosures are reasonable in the context of the applicable financial reporting framework, or are misstated.

Application and Other Explanatory Material

Nature of Accounting Estimates (Ref: Para. 2)

Examples of Accounting Estimates

…

Methods

A2. A method is a measurement technique used by management to make an accounting estimate in accordance with the required measurement basis. For example, one recognized method used to make accounting estimates relating to share-based payment transactions is to determine a theoretical option call price using the Black Scholes option pricing formula. A method is applied using a computational tool or process, sometimes referred to as a model, and involves applying assumptions and data and taking into account a set of relationships between them.

Assumptions and Data

A3. Assumptions involve judgments based on available information about matters such as the choice of an interest rate, a discount rate, or judgments about future conditions or events. An assumption may be selected by management from a range of appropriate alternatives. Assumptions that may be made or identified by a management's expert become management's assumptions when used by management in making an accounting estimate.

A4. For purposes of this ISA, data is information that can be obtained through direct observation or from a party external to the entity. Information obtained by applying analytical or interpretive techniques to data is referred to as derived data when such techniques have a well-established theoretical basis and therefore less need for management judgment. Otherwise, such information is an assumption.

A5. Examples of data include:

- Prices agreed in market transactions;
- Operating times or quantities of output from a production machine;

[132] ISA 330, paragraph 28(b)

- Historical prices or other terms included in contracts, such as a contracted interest rate, a payment schedule, and term included in a loan agreement;
- Forward-looking information such as economic or earnings forecasts obtained from an external information source, or
- A future interest rate determined using interpolation techniques from forward interest rates (derived data).

A6. Data can come from a wide range of sources. For example, data can be:

- Generated within the organization or externally;
- Obtained from a system that is either within or outside the general or subsidiary ledgers;
- Observable in contracts; or
- Observable in legislative or regulatory pronouncements.

Scalability (Ref: Para. 3)

A7. Examples of paragraphs that include guidance on how the requirements of this ISA can be scaled include paragraphs A20–A22, A63, A67, and A84.

Key Concepts of This ISA

Inherent Risk Factors (Ref: Para. 4)

A8. Inherent risk factors are characteristics of ~~conditions and~~ events or~~and~~ conditions that ~~may~~ affect ~~the~~ susceptibility ~~of an assertion~~ to misstatement, whether due to fraud or error, of an assertion about a class of transactions, account balance or disclosures, before consideration of controls.[133] Appendix 1 further explains the nature of these inherent risk factors, and their inter-relationships, in the context of making accounting estimates and their presentation in the financial statements.

A9. ~~In addition to the inherent risk factors of estimation uncertainty, complexity or subjectivity, other inherent risk factors that the auditor may consider in identifying and~~ When assessing the risks of material misstatement at the assertion level[134], in addition to estimation uncertainty, complexity, and subjectivity, the auditor also takes into account the degree ~~may include the extent~~ to which inherent risk factors included in ISA 315 (Revised 2019)~~,~~ (other than estimation uncertainty, complexity, and subjectivity)~~,~~ affect susceptibility ~~to misstatement~~ of assertions to misstatement about the accounting estimate. Such additional inherent risk factors include ~~is subject to, or affected by~~:

- Change in the nature or circumstances of the relevant financial statement items, or requirements of the applicable financial reporting framework which may give rise to the need for changes in the method, assumptions or data used to make the accounting estimate.
- Susceptibility to misstatement due to management bias, or other fraud risk factors insofar as they affect inherent risk, in making the accounting estimate.

[133] ISA 315 (Revised 2019), paragraph 12(f)

[134] ISA 315 (Revised 2019), paragraph 31

- Uncertainty, other than estimation uncertainty.

Control Risk (Ref: Para. 6)

A10. ~~An important consideration for the auditor i~~In assessing control risk at the assertion level in accordance with ISA 315 (Revised 2019), the auditor takes into account ~~is the effectiveness of the design of the controls that~~ whether the auditor ~~intends~~ plans to ~~rely~~ test ~~on~~ the operating effectiveness of controls. ~~and the extent to which the controls address the assessed inherent risks at the assertion level.~~ When the auditor is considering whether to test the operating effectiveness of controls, ~~T~~the auditor's evaluation that controls are effectively designed and have been implemented supports an expectation, by the auditor, about the operating effectiveness of the controls in ~~determining whether~~ establishing the plan to test them.

Professional Skepticism (Ref: Para. 8)

….

Concept of "Reasonable" (Ref: Para. 9, 35)

…

Risk Assessment Procedures and Related Activities

Obtaining an Understanding of the Entity and Its Environment, the Applicable Financial Reporting Framework, and the Entity's System of Internal Control (Ref: Para. 13)

A19. Paragraphs 19~~11–27~~24 of ISA 315 (Revised 2019) require the auditor to obtain an understanding of certain matters about the entity and its environment, the applicable financial reporting framework and ~~including~~ the entity's system of internal control. The requirements in paragraph 13 of this ISA relate more specifically to accounting estimates and build on the broader requirements in ISA 315 (Revised 2019).

Scalability

A20. The nature, timing, and extent of the auditor's procedures to obtain the understanding of the entity and its environment, ~~including~~ the applicable financial reporting framework, and the entity's system of internal control, related to the entity's accounting estimates, may depend, to a greater or lesser degree, on the extent to which the individual matter(s) apply in the circumstances. For example, the entity may have few transactions or other events ~~and~~ or conditions that give rise to the need for accounting estimates, the applicable financial reporting requirements may be simple to apply, and there may be no relevant regulatory factors. Further, the accounting estimates may not require significant judgments, and the process for making the accounting estimates may be less complex. In these circumstances, the accounting estimates may be subject to, or affected by, estimation uncertainty, complexity, subjectivity, or other inherent risk factors to a lesser degree, and there may be fewer identified controls in the control activities component ~~relevant to the audit~~. If so, the auditor's risk identification and assessment procedures are likely to be less extensive and may be obtained primarily through inquiries of management with appropriate responsibilities for the financial statements, such as ~~and~~ simple walk-throughs of management's process for making the accounting

estimate (including when evaluating whether identified controls in that process are designed effectively and when determining whether the control has been implemented).

A21. By contrast, the accounting estimates may require significant judgments by management, and the process for making the accounting estimates may be complex and involve the use of complex models. In addition, the entity may have a more sophisticated information system, and more extensive controls over accounting estimates. In these circumstances, the accounting estimates may be subject to or affected by estimation uncertainty, subjectivity, complexity or other inherent risk factors to a greater degree. If so, the nature or timing of the auditor's risk assessment procedures are likely to be different, or be more extensive, than in the circumstances in paragraph A20.

A22. The following considerations may be relevant for entities with only simple businesses, which may include many smaller entities:

- Processes relevant to accounting estimates may be uncomplicated because the business activities are simple or the required estimates may have a lesser degree of estimation uncertainty.
- Accounting estimates may be generated outside of the general and subsidiary ledgers, controls over their development may be limited, and an owner-manager may have significant influence over their determination. The owner-manager's role in making the accounting estimates may need to be taken into account by the auditor both when identifying the risks of material misstatement and when considering the risk of management bias.

The Entity and Its Environment

The entity's transactions and other events ~~and~~ or conditions (Ref: Para. 13(a))

A23. Changes in circumstances that may give rise to the need for, or changes in, accounting estimates may include, for example, whether:

- The entity has engaged in new types of transactions;
- Terms of transactions have changed; or
- New events or conditions have occurred.

The requirements of the applicable financial reporting framework (Ref: Para. 13(b))

A24. Obtaining an understanding of the requirements of the applicable financial reporting framework provides the auditor with a basis for discussion with management and, where applicable, those charged with governance about how management has applied the~~ose~~ requirements of the applicable financial reporting framework relevant to the accounting estimates, and about the auditor's determination of whether they have been applied appropriately. This understanding also may assist the auditor in communicating with those charged with governance when the auditor considers a significant accounting practice that is acceptable under the applicable financial reporting framework, not to be the most appropriate in the circumstances of the entity.[135]

[135] ISA 260 (Revised), paragraph 16(a)

A25. In obtaining this understanding, the auditor may seek to understand whether:

- The applicable financial reporting framework:
  - Prescribes certain criteria for the recognition, or methods for the measurement of accounting estimates;
  - Specifies certain criteria that permit or require measurement at a fair value, for example, by referring to management's intentions to carry out certain courses of action with respect to an asset or liability; or
  - Specifies required or suggested disclosures, including disclosures concerning judgments, assumptions, or other sources of estimation uncertainty relating to accounting estimates; and
- Changes in the applicable financial reporting framework require changes to the entity's accounting policies relating to accounting estimates.

Regulatory factors (Ref: Para. 13(c))

…

The nature of the accounting estimates and related disclosures that the auditor expects to be included in the financial statements (Ref: Para. 13(d))

…

The Entity's System of Internal Control ~~Relevant to the Audit~~

The nature and extent of oversight and governance (Ref: Para. 13(e))

A28. In applying ISA 315 (Revised 2019),[136] the auditor's understanding of the nature and extent of oversight and governance that the entity has in place over management's process for making accounting estimates may be important to the auditor's required evaluation of ~~as it relates to~~ whether:

- Management, with the oversight of those charged with governance, has created and maintained a culture of honesty and ethical behavior; ~~and~~
- The ~~strengths in the entity's~~ control environment ~~elements collectively~~ provides an appropriate foundation for the other components of the system of internal control considering the nature and size of the entity; and ~~whether~~
- ~~those other components are undermined by c~~Control deficiencies identified in the control environment undermine the other components of the system of internal control.

…

A30. Obtaining an understanding of the oversight by those charged with governance may be important when there are accounting estimates that:

[136] ISA 315 (Revised 2019), paragraph 21(a)~~14~~

- Require significant judgment by management to address subjectivity;
- Have high estimation uncertainty;
- Are complex to make, for example, because of the extensive use of information technology, large volumes of data or the use of multiple data sources or assumptions with complex interrelationships;
- Had, or ought to have had, a change in the method, assumptions or data compared to previous periods; or
- Involve significant assumptions.

Management's application of specialized skills or knowledge, including the use of management's experts (Ref: Para. 13(f))

…

The entity's risk assessment process (Ref: Para. 13(g))

A32. Understanding how the entity's risk assessment process identifies and addresses risks relating to accounting estimates may assist the auditor in considering changes in:

- The requirements of the applicable financial reporting framework related to the accounting estimates;
- The availability or nature of data sources that are relevant to making the accounting estimates or that may affect the reliability of the data used;
- The entity's information systems or IT environment; and
- Key personnel.

A33. Matters that the auditor may consider in obtaining an understanding of how management identified and addresses the susceptibility to misstatement due to management bias or fraud in making accounting estimates, include whether, and if so how, management:

- Pays particular attention to selecting or applying the methods, assumptions and data used in making accounting estimates.
- Monitors key performance indicators that may indicate unexpected or inconsistent performance compared with historical or budgeted performance or with other known factors.
- Identifies financial or other incentives that may be a motivation for bias.
- Monitors the need for changes in the methods, significant assumptions or the data used in making accounting estimates.
- Establishes appropriate oversight and review of models used in making accounting estimates.

- Requires documentation of the rationale for, or an independent review of, significant judgments made in making accounting estimates.

The entity's information system relating to accounting estimates (Ref: Para. 13(h)(i))

A34. The significant classes of transactions, events and conditions within the scope of paragraph 13(h) are the same as the significant classes of transactions, events and conditions relating to accounting estimates and related disclosures that are subject to paragraph~~s~~ 25(a)~~18~~(a)~~ and (d)~~ of ISA 315 (Revised 2019). In obtaining the understanding of the entity's information system as it relates to accounting estimates, the auditor may consider:

- Whether the accounting estimates arise from the recording of routine and recurring transactions or whether they arise from non-recurring or unusual transactions.
- How the information system addresses the completeness of accounting estimates and related disclosures, in particular for accounting estimates related to liabilities.

A35. During the audit, the auditor may identify classes of transactions, events ~~and~~ or conditions that give rise to the need for accounting estimates and related disclosures that management failed to identify. ISA 315 (Revised 2019) deals with circumstances where the auditor identifies risks of material misstatement that management failed to identify, including ~~determining whether there is a significant deficiency in internal control with regard to~~ considering the implications for the auditor's evaluation of the entity's risk assessment process.[137]

Management's Identification of the Relevant Methods, Assumptions and Sources of Data (Ref: Para. 13(h)(ii)(a)

…

Methods (Ref: Para. 13(h)(ii)(a)(i))

…

Models

A39. Management may design and implement specific controls around models used for making accounting estimates, whether management's own model or an external model. When the model itself has an increased level of complexity or subjectivity, such as an expected credit loss model or a fair value model using level 3 inputs, controls that address such complexity or subjectivity may be. When complexity in relation to models is present, controls over data integrity are also more likely to be identified controls in accordance with ISA 315 (Revised 2019)~~relevant to the audit~~. Factors that may be appropriate for the auditor to consider in obtaining an understanding of the model and ~~of~~ related identified control~~s~~ ~~activities~~ ~~relevant to the audit~~ include the following:

- How management determines the relevance and accuracy of the model;

[129] ISA 315 (Revised 2019), paragraph 22(b)~~43~~

- The validation or back testing of the model, including whether the model is validated prior to use and revalidated at regular intervals to determine whether it remains suitable for its intended use. The entity's validation of the model may include evaluation of:
    - The model's theoretical soundness;
    - The model's mathematical integrity; and
    - The accuracy and completeness of the data and the appropriateness of data and assumptions used in the model.
- How the model is appropriately changed or adjusted on a timely basis for changes in market or other conditions and whether there are appropriate change control policies over the model;
- Whether adjustments, also referred to as overlays in certain industries, are made to the output of the model and whether such adjustments are appropriate in the circumstances in accordance with the requirements of the applicable financial reporting framework. When the adjustments are not appropriate, such adjustments may be indicators of possible management bias; and
- Whether the model is adequately documented, including its intended applications, limitations, key parameters, required data and assumptions, the results of any validation performed on it and the nature of, and basis for, any adjustments made to its output.

Assumptions (Ref: Para. 13(h)(ii)(a)(ii))

…

Data (Ref: Para. 13(h)(ii)(a)(iii))

A44. Matters that the auditor may consider in obtaining an understanding of how management selects the data on which the accounting estimates are based include:

- The nature and source of the data, including information obtained from an external information source.
- How management evaluates whether the data is appropriate.
- The accuracy and completeness of the data.
- The consistency of the data used with data used in previous periods.
- The complexity of IT applications or other aspects of the entity's IT environment ~~the information technology systems~~ used to obtain and process the data, including when this involves handling large volumes of data.
- How the data is obtained, transmitted and processed and how its integrity is maintained.

How management understands and addresses estimation uncertainty (Ref: Para. 13(h)(ii)(b)–13(h)(ii)(c))

…

Identified Controls ~~Activities Relevant to the Audit~~ Over Management's Process for Making Accounting Estimates (Ref: Para 13(i))

A50. The auditor's judgment in identifying controls ~~relevant to the audit~~in the controls~~ activities component~~, and therefore the need to evaluate the design of those controls and determine whether they have been implemented, relates to management's process described in paragraph 13(h)(ii). The auditor may not identify ~~relevant~~ controls ~~activities~~ in relation to all ~~the elements~~ aspects of paragraph 13(h)(ii)., ~~depending on the complexity associated with the accounting estimate.~~

A51. As part of ~~obtaining an understanding of~~ identifying the controls ~~activities relevant to the audit~~, and evaluating their design and determining whether they have been implemented, the auditor may consider:

- How management determines the appropriateness of the data used to develop the accounting estimates, including when management uses an external information source or data from outside the general and subsidiary ledgers.
- The review and approval of accounting estimates, including the assumptions or data used in their development, by appropriate levels of management and, where appropriate, those charged with governance.
- The segregation of duties between those responsible for making the accounting estimates and those committing the entity to the related transactions, including whether the assignment of responsibilities appropriately takes account of the nature of the entity and its products or services. For example, in the case of a large financial institution, relevant segregation of duties may consist of an independent function responsible for estimation and validation of fair value pricing of the entity's financial products staffed by individuals whose remuneration is not tied to such products.
- The effectiveness of the design of the controls. ~~activities.~~ Generally, it may be more difficult for management to design controls that address subjectivity and estimation uncertainty in a manner that effectively prevents, or detects and corrects, material misstatements, than it is to design controls that address complexity. Controls that address subjectivity and estimation uncertainty may need to include more manual elements, which may be less reliable than automated controls as they can be more easily bypassed, ignored or overridden by management. The design effectiveness of controls addressing complexity may vary depending on the reason for, and the nature of, the complexity. For example, it may be easier to design more effective controls related to a method that is routinely used or over the integrity of data.

A52. When management makes extensive use of information technology in making an accounting estimate, identified controls ~~relevant to the audit~~ in the control activities component are likely to include general IT controls and ~~application~~ information processing controls. Such controls may address risks related to:

- Whether the IT applications or other aspects of the IT environment ~~information technology system~~ has the capability and is appropriately configured to process large volumes of data;
- Complex calculations in applying a method. When diverse IT applications ~~systems~~ are required to process complex transactions, regular reconciliations between the IT applications ~~systems~~

are made, in particular when the IT applications ~~systems~~ do not have automated interfaces or may be subject to manual intervention;

- Whether the design and calibration of models is periodically evaluated;
- The complete and accurate extraction of data regarding accounting estimates from the entity's records or from external information sources;
- Data, including the complete and accurate flow of data through the entity's information system, the appropriateness of any modification to the data used in making accounting estimates, the maintenance of the integrity and security of the data. When using external information sources, risks related to processing or recording the data;
- Whether management has controls around access, change and maintenance of individual models to maintain a strong audit trail of the accredited versions of models and to prevent unauthorized access or amendments to those models; and
- Whether there are appropriate controls over the transfer of information relating to accounting estimates into the general ledger, including appropriate controls over journal entries.

A53. In some industries, such as banking or insurance, the term governance may be used to describe activities within the control environment, the entity's process to monitor the system of internal control ~~monitoring of controls~~, and other components of the system of internal control, as described in ISA 315 (Revised 2019).[138]

A54. For entities with an internal audit function, its work may be particularly helpful to the auditor in obtaining an understanding of:

- The nature and extent of management's use of accounting estimates;
- The design and implementation of controls ~~activities~~ that address the risks related to the data, assumptions and models used to make the accounting estimates;
- The aspects of the entity's information system that generate the data on which the accounting estimates are based; and
- How new risks relating to accounting estimates are identified, assessed and managed.

Reviewing the Outcome or Re-Estimation of Previous Accounting Estimates (Ref: Para. 14)

…

A58. Based on the auditor's previous assessment of the risks of material misstatement, for example, if inherent risk is assessed as higher for one or more risks of material misstatement, the auditor may judge that a more detailed retrospective review is required. As part of the detailed retrospective review, the auditor may pay particular attention, when practicable, to the effect of data and significant assumptions used in making the previous accounting estimates. On the other hand, for example, for accounting estimates that arise from the recording of routine and recurring transactions, the auditor

[138] ISA 315 (Revised 2019), Appendix 3 ~~paragraph A77~~

may judge that the application of analytical procedures as risk assessment procedures is sufficient for purposes of the review.

A59. The measurement objective for fair value accounting estimates and other accounting estimates, based on current conditions at the measurement date, deals with perceptions about value at a point in time, which may change significantly and rapidly as the environment in which the entity operates changes. The auditor may therefore focus the review on obtaining information that may be relevant to identifying and assessing risks of material misstatement. For example, in some cases, obtaining an understanding of changes in marketplace participant assumptions that affected the outcome of a previous period's fair value accounting estimates may be unlikely to provide relevant audit evidence. In this case, audit evidence may be obtained by understanding the outcomes of assumptions (such as a cash flow projections) and understanding the effectiveness of management's prior estimation process that supports the identification and assessment of the risks of material misstatement in the current period.

A60. A difference between the outcome of an accounting estimate and the amount recognized in the previous period's financial statements does not necessarily represent a misstatement of the previous period's financial statements. However, such a difference may represent a misstatement if, for example, the difference arises from information that was available to management when the previous period's financial statements were finalized, or that could reasonably be expected to have been obtained and taken into account in the context of the applicable financial reporting framework.[139] Such a difference may call into question management's process for taking information into account in making the accounting estimate. As a result, the auditor may reassess any plan to test related controls and the related assessment of control risk ~~and~~ or may determine that more persuasive audit evidence needs to be obtained about the matter. Many financial reporting frameworks contain guidance on distinguishing between changes in accounting estimates that constitute misstatements and changes that do not, and the accounting treatment required to be followed in each case.

Specialized Skills or Knowledge (Ref: Para. 15)

…

Identifying and Assessing the Risks of Material Misstatement (Ref: Para. 4, 16)

A64. Identifying and assessing risks of material misstatement at the assertion level relating to accounting estimates is important for all accounting estimates, including not only those that are recognized in the financial statements, but also those that are included in the notes to the financial statements.

A65. Paragraph A42 of ISA 200 states that the ISAs ~~do not ordinarily refer to inherent risk and control risk separately~~ typically refer to the "risks of material misstatement" rather than to inherent risk and control risk separately. ~~However, this~~ ISA 315 (Revised 2019) requires a separate assessment of inherent risk and control risk to provide a basis for designing and performing further audit procedures to

[139] ISA 560, Subsequent Events, paragraph 14

respond to the risks of material misstatement at the assertion level,[140] including significant risks, ~~at the assertion level for accounting estimates~~ in accordance with ISA 330.[141]

A66. In identifying the risks of material misstatement and in assessing inherent risk for accounting estimates in accordance with ISA 315 (Revised 2019),[142] the auditor is required to take into account ~~the degree to which the accounting estimate is subject to, or affected by,~~ the inherent risk factors that affect susceptibility to misstatement of assertions, and how they do so ~~estimation uncertainty, complexity, subjectivity, or other inherent risk factors~~. The auditor's consideration of the inherent risk factors may also provide information to be used in ~~determining~~:

- Assessing the likelihood and magnitude of misstatement (i.e., ~~W~~where inherent risk is assessed on the spectrum of inherent risk); and
- Determining ~~T~~the reasons for the assessment given to the risks of material misstatement at the assertion level, and that the auditor's further audit procedures in accordance with paragraph 18 are responsive to those reasons.

The interrelationships between the inherent risk factors are further explained in Appendix 1.

A67. The reasons for the auditor's assessment of inherent risk at the assertion level may result from one or more of the inherent risk factors of estimation uncertainty, complexity, subjectivity or other inherent risk factors. For example:

(a) Accounting estimates of expected credit losses are likely to be complex because the expected credit losses cannot be directly observed and may require the use of a complex model. The model may use a complex set of historical data and assumptions about future developments in a variety of entity specific scenarios that may be difficult to predict. Accounting estimates for expected credit losses are also likely to be subject to high estimation uncertainty and significant subjectivity in making judgments about future events or conditions. Similar considerations apply to insurance contract liabilities.

(b) An accounting estimate for an obsolescence provision for an entity with a wide range of different inventory types may require complex systems and processes, but may involve little subjectivity and the degree of estimation uncertainty may be low, depending on the nature of the inventory.

(c) Other accounting estimates may not be complex to make but may have high estimation uncertainty and require significant judgment, for example, an accounting estimate that requires a single critical judgment about a liability, the amount of which is contingent on the outcome of the litigation.

A68. The relevance and significance of inherent risk factors may vary from one estimate to another. Accordingly, the inherent risk factors may, either individually or in combination, affect simple

---

[140] ISA 315 (Revised 2019), paragraphs 31 and 34

[141] ~~ISA 330, paragraph 7(b)~~

[142] ISA 315 (Revised 2019), paragraph 31(a)

accounting estimates to a lesser degree and the auditor may identify fewer risks or assess inherent risk ~~at~~ close to the lower end of the spectrum of inherent risk.

A69. Conversely, the inherent risk factors may, either individually or in combination, affect complex accounting estimates to a greater degree, and may lead the auditor to assess inherent risk at the higher end of the spectrum of inherent risk. For these accounting estimates, the auditor's consideration of the effects of the inherent risk factors is likely to directly affect the number and nature of identified risks of material misstatement, the assessment of such risks, and ultimately the persuasiveness of the audit evidence needed in responding to the assessed risks. Also, for these accounting estimates the auditor's application of professional skepticism may be particularly important.

A70. Events occurring after the date of the financial statements may provide additional information relevant to the auditor's assessment of the risks of material misstatement at the assertion level. For example, the outcome of an accounting estimate may become known during the audit. In such cases, the auditor may assess or revise the assessment of the risks of material misstatement at the assertion level,[143] regardless of how the inherent risk factors affect susceptibility of assertions to misstatement relating to ~~degree to which~~ the accounting estimate. ~~was subject to, or affected by, estimation uncertainty, complexity, subjectivity or other inherent risk factors.~~ Events occurring after the date of the financial statements also may influence the auditor's selection of the approach to testing the accounting estimate in accordance with paragraph 18. For example, for a simple bonus accrual that is based on a straightforward percentage of compensation for selected employees, the auditor may conclude that there is relatively little complexity or subjectivity in making the accounting estimate, and therefore may assess inherent risk at the assertion level ~~at~~ close to the lower end of the spectrum of inherent risk. The payment of the bonuses subsequent to period end may provide sufficient appropriate audit evidence regarding the assessed risks of material misstatement at the assertion level.

A71. The auditor's assessment of control risk may be done in different ways depending on preferred audit techniques or methodologies. The control risk assessment may be expressed using qualitative categories (for example, control risk assessed as maximum, moderate, minimum) or in terms of the auditor's expectation of how effective the control(s) is in addressing the identified risk, that is, the planned reliance on the effective operation of controls. For example, if control risk is assessed as maximum, the auditor contemplates no reliance on the effective operation of controls. If control risk is assessed at less than maximum, the auditor contemplates reliance on the effective operation of controls.

Estimation Uncertainty (Ref: Para. 16(a))

A72. In taking into account the degree to which the accounting estimate is subject to estimation uncertainty, the auditor may consider:

- Whether the applicable financial reporting framework requires:

[143] ISA 315 (Revised 2019), paragraph 37~~31~~

- The use of a method to make the accounting estimate that inherently has a high level of estimation uncertainty. For example, the financial reporting framework may require the use of unobservable inputs.
- The use of assumptions that inherently have a high level of estimation uncertainty, such as assumptions with a long forecast period, assumptions that are based on data that is unobservable and are therefore difficult for management to develop, or the use of various assumptions that are interrelated.
- Disclosures about estimation uncertainty.

- The business environment. An entity may be active in a market that experiences turmoil or possible disruption (for example, from major currency movements or inactive markets) and the accounting estimate may therefore be dependent on data that is not readily observable.
- Whether it is possible (or practicable, insofar as permitted by the applicable financial reporting framework) for management:
  - To make a precise and reliable prediction about the future realization of a past transaction (for example, the amount that will be paid under a contingent contractual term), or about the incidence and impact of future events or conditions (for example, the amount of a future credit loss or the amount at which an insurance claim will be settled and the timing of its settlement); or
  - To obtain precise and complete information about a present condition (for example, information about valuation attributes that would reflect the perspective of market participants at the date of the financial statements, to develop a fair value estimate).

A73. The size of the amount recognized or disclosed in the financial statements for an accounting estimate is not, in itself, an indicator of its susceptibility to misstatement because, for example, the accounting estimate may be understated.

A74. In some circumstances, the estimation uncertainty may be so high that a reasonable accounting estimate cannot be made. The applicable financial reporting framework may preclude recognition of an item in the financial statements, or its measurement at fair value. In such cases, there may be risks of material misstatement that relate not only to whether an accounting estimate should be recognized, or whether it should be measured at fair value, but also to the reasonableness of the disclosures. With respect to such accounting estimates, the applicable financial reporting framework may require disclosure of the accounting estimates and the estimation uncertainty associated with them (see paragraphs A112–A113, A143–A144).

A75. In some cases, the estimation uncertainty relating to an accounting estimate may cast significant doubt about the entity's ability to continue as a going concern. ISA 570 (Revised)[144] establishes requirements and provides guidance in such circumstances.

[144] ISA 570, (Revised), *Going Concern*

Complexity or Subjectivity (Ref: Para. 16(b))

The Degree to Which Complexity Affects the Selection and Application of the Method

A76. In taking into account the degree to which the selection and application of the method used in making the accounting estimate are affected by complexity, the auditor may consider:

- The need for specialized skills or knowledge by management which may indicate that the method used to make an accounting estimate is inherently complex and therefore the accounting estimate may have a greater susceptibility to material misstatement. There may be a greater susceptibility to material misstatement when management has developed a model internally and has relatively little experience in doing so, or uses a model that applies a method that is not established or commonly used in a particular industry or environment.
- The nature of the measurement basis required by the applicable financial reporting framework, which may result in the need for a complex method that requires multiple sources of historical and forward-looking data or assumptions, with multiple interrelationships between them. For example, an expected credit loss provision may require judgments about future credit repayments and other cash flows, based on consideration of historical experience data and the application of forward looking assumptions. Similarly, the valuation of an insurance contract liability may require judgments about future insurance contract payments to be projected based on historical experience and current and assumed future trends.

The Degree to Which Complexity Affects the Selection and Application of the Data

A77. In taking into account the degree to which the selection and application of the data used in making the accounting estimate are affected by complexity, the auditor may consider:

- The complexity of the process to derive the data, taking into account the relevance and reliability of the data source. Data from certain sources may be more reliable than from others. Also, for confidentiality or proprietary reasons, some external information sources will not (or not fully) disclose information that may be relevant in considering the reliability of the data they provide, such as the sources of the underlying data they used or how it was accumulated and processed.
- The inherent complexity in maintaining the integrity of the data. When there is a high volume of data and multiple sources of data, there may be inherent complexity in maintaining the integrity of data that is used to make an accounting estimate.
- The need to interpret complex contractual terms. For example, the determination of cash inflows or outflows arising from a commercial supplier or customer rebates may depend on very complex contractual terms that require specific experience or competence to understand or interpret.

The Degree to Which Subjectivity Affects the Selection and Application of the Method, Assumptions or Data

A78. In taking into account the degree to which the selection and application of method, assumptions or data are affected by subjectivity, the auditor may consider:

- The degree to which the applicable financial reporting framework does not specify the valuation approaches, concepts, techniques and factors to use in the estimation method.
- The uncertainty regarding the amount or timing, including the length of the forecast period. The amount and timing is a source of inherent estimation uncertainty, and gives rise to the need for management judgment in selecting a point estimate, which in turn creates an opportunity for management bias. For example, an accounting estimate that incorporates forward looking assumptions may have a high degree of subjectivity which may be susceptible to management bias.

Other Inherent Risk Factors (Ref: Para. 16(b))

A79. The degree of subjectivity associated with an accounting estimate influences the susceptibility of the accounting estimate to misstatement due to management bias or ~~fraud~~ other fraud risk factors insofar as they affect inherent risk. For example, when an accounting estimate is subject to a high degree of subjectivity, the accounting estimate is likely to be more susceptible to misstatement due to management bias or fraud and this may result in a wide range of possible measurement outcomes. Management may select a point estimate from that range that is inappropriate in the circumstances, or that is inappropriately influenced by unintentional or intentional management bias, and that is therefore misstated. For continuing audits, indicators of possible management bias identified during the audit of preceding periods may influence the planning and risk assessment procedures in the current period.

Significant Risks (Ref: Para. 17)

A80. The auditor's assessment of inherent risk, which takes into account the degree to which an accounting estimate is subject to, or affected by estimation uncertainty, complexity, subjectivity or other inherent risk factors, assists the auditor in determining whether any of the risks of material misstatement identified and assessed are a significant risk.

…

When the Auditor Intends to Rely on the Operating Effectiveness of ~~Relevant~~ Controls (Ref: Para: 19)

A85. Testing the operating effectiveness of ~~relevant~~ controls may be appropriate when inherent risk is assessed as higher on the spectrum of inherent risk, including for significant risks. This may be the case when the accounting estimate is subject to or affected by a high degree of complexity. When the accounting estimate is affected by a high degree of subjectivity, and therefore requires significant judgment by management, inherent limitations in the effectiveness of the design of controls may lead the auditor to focus more on substantive procedures than on testing the operating effectiveness of controls.

…

Overall Evaluation Based on Audit Procedures Performed (Ref: Para. 33)

…

Determining Whether the Accounting Estimates are Reasonable or Misstated (Ref: Para. 9, 35)

…

ISA 600, *Special Considerations—Audits of Group Financial Statements (Including the Work of Component Auditors)*

Requirements

Understanding the Group, Its Components and Their Environments

17. The auditor is required to identify and assess the risks of material misstatement through obtaining an understanding of the entity and its environment, the applicable financial reporting framework and the system of internal control.[7] The group engagement team shall:

    (a) …

Application and Other Explanatory Material

…

Definitions

…

Significant Component (Ref: Para. 9(m))

…

A6. The group engagement team may also identify a component as likely to include significant risks of material misstatement of the group financial statements due to its specific nature or circumstances. ~~(that is, risks that require special audit consideration[145]).~~ For example, a component could be responsible for foreign exchange trading and thus expose the group to a significant risk of material misstatement, even though the component is not otherwise of individual financial significance to the group.

…

Understanding the Group, Its Components, and Their Environments

Matters about Which the Group Engagement Team Obtains an Understanding (Ref: Para. 17)

A23. ISA 315 (Revised 2019) contains guidance on matters the auditor may consider when obtaining an understanding of the industry, regulatory, and other external factors that affect the entity, including the applicable financial reporting framework; the nature of the entity; objectives and strategies and

~~[145] ISA 315 (Revised), paragraphs 27–29~~

related business risks; and measurement and review of the entity's financial performance.[146] Appendix 2 of this ISA contains guidance on matters specific to a group including the consolidation process.

Appendix 2

Examples of Matters about Which the Group Engagement Team Obtains an Understanding

…

Group-Wide Controls

1. Group-wide controls may include a combination of the following:
   - Regular meetings between group and component management to discuss business developments and to review performance.
   - …
   - Controls ~~activities~~ within an IT system that is common for all or some components.
   - Controls within the group's process to monitor ~~Monitoring~~ the system of internal control~~s~~, including activities of the internal audit function and self-assessment programs.
   - …

Appendix 5

Required and Additional Matters Included in the Group Engagement Team's Letter of Instruction

Matters that are relevant to the planning of the work of the component auditor:

- …

…

Matters that are relevant to the conduct of the work of the component auditor:

- The findings of the group engagement team's tests of controls ~~activities~~ of a processing system that is common for all or some components, and tests of controls to be performed by the component auditor.
- …

[146] ISA 315 (Revised 2019), paragraphs A62~~25~~–A64~~49~~ and Appendix 1

ISA 610 (Revised 2013), *Using the Work of Internal Auditors*

Introduction

…

Relationship between ISA 315 (Revised 2019) and ISA 610 (Revised 2013)

…

7. ISA 315 (Revised 2019) addresses how the knowledge and experience of the internal audit function can inform the external auditor's understanding of the entity and its environment, the applicable financial reporting framework and the entity's system of internal control, and identification and assessment of risks of material misstatement. ISA 315 (Revised 2019)[3] also explains how effective communication between the internal and external auditors also creates an environment in which the external auditor can be informed of significant matters that may affect the external auditor's work.

…

Application and Other Explanatory Material

Definition of Internal Audit Function (Ref: Para. 2, 14(a))

…

A3. In addition, those in the entity with operational and managerial duties and responsibilities outside of the internal audit function would ordinarily face threats to their objectivity that would preclude them from being treated as part of an internal audit function for the purpose of this ISA, although they may perform controls ~~activities~~ that can be tested in accordance with ISA 330.[12] For this reason, monitoring controls performed by an owner-manager would not be considered equivalent to an internal audit function.

…

Evaluating the Internal Audit Function

…

Application of a Systematic and Disciplined Approach (Ref: Para. 15(c))

A10. The application of a systematic and disciplined approach to planning, performing, supervising, reviewing and documenting its activities distinguishes the activities of the internal audit function from other monitoring controls ~~activities~~ that may be performed within the entity.

…

A21. As explained in ISA 315 (Revised 2019),[147] significant risks ~~require special audit consideration~~ are risks assessed close to the upper end of the spectrum of inherent risk and therefore the external

[147] ISA 315 (Revised 2019), paragraph 12~~4~~(l)~~(e)~~

auditor's ability to use the work of the internal audit function in relation to significant risks will be restricted to procedures that involve limited judgment. In addition, where the risks of material misstatement is other than low, the use of the work of the internal audit function alone is unlikely to reduce audit risk to an acceptably low level and eliminate the need for the external auditor to perform some tests directly.

…

ISA 620, *Using the Work of an Auditor's Expert*

Application and Other Explanatory Material

…

Determining the Need for an Auditor's Expert (Ref: Para. 7)

A4. An auditor's expert may be needed to assist the auditor in one or more of the following:

- Obtaining an understanding of the entity and its environment, the applicable financial reporting framework and the~~, including its~~ entity's system of internal control.

• …

ISA 701, *Communicating Key Audit Matters in eth Independent Auditor's Report*

Application and Other Explanatory Material

…

Determining Key Audit Matters (Ref: Para. 9–10)

…

Considerations in Determining Those Matters that Required Significant Auditor Attention (Ref: Para. 9)

…

Areas of Higher Assessed Risk of Material Misstatement, or Significant Risks Identified in Accordance with ISA 315 (Revised 2019) (Ref: Para. 9(a))

…

A20. ISA 315 (Revised 2019) defines a significant risk as an identified ~~and assessed~~ risk of material misstatement for which the assessment of inherent risk is close to the upper end of the spectrum of inherent risk due to the degree to which the inherent risk factors affect the combination of the likelihood of a misstatement occurring and the magnitude of the potential misstatement should that misstatement occur ~~that, in the auditor's judgment, requires special audit consideration~~.[148] Areas of

[148] ISA 315 (Revised 2019), paragraph 12(l)

significant management judgment and significant unusual transactions may often be identified as significant risks. Significant risks are therefore often areas that require significant auditor attention.

…

ISA 720 (Revised), *The Auditor's Responsibilities Relating to Other Information*

Application and Other Explanatory Material

…

Reading and Considering the Other Information (Ref: Para. 14–15)

…

Considering Whether There Is a Material Inconsistency between the Other Information and the Auditor's Knowledge Obtained in the Audit (Ref: Para. 14(b))

…

A31. The auditor's knowledge obtained in the audit includes the auditor's understanding of the entity and its environment, the applicable financial reporting framework, and ~~including~~ the entity's system of internal control, obtained in accordance with ISA 315 (Revised 2019).[149] ISA 315 (Revised 2019) sets out the auditor's required understanding, which includes such matters as obtaining an understanding of:

(a) The entity's organizational structure, ownership and governance, and its business model, including the extent to which the business model integrates the use of IT;

(b) ~~The r~~Relevant industry, regulatory, and other external factors;

(c) The relevant measures used, internally and externally, to assess ~~measurement and review of~~ the entity's financial performance; ~~and~~

~~(b) The nature of the entity;~~

~~(c) The entity's selection and application of accounting policies;~~

~~(d) The entity's objectives and strategies;~~

…

[149] ISA 315 (Revised 2019), *Identifying and Assessing the Risks of Material Misstatement ~~through Understanding the Entity and Its Environment~~*, paragraphs 19~~11~~–27~~12~~

Responding When a Material Misstatement in the Financial Statements Exists or the Auditor's Understanding of the Entity and Its Environment Needs to Be Updated (Ref: Para. 20)

A51. In reading the other information, the auditor may become aware of new information that has implications for:

- The auditor's understanding of the entity and its environment, the financial reporting framework and the entity's system of internal control and, accordingly, may indicate the need to revise the auditor's risk assessment.
- …

…

The structures and processes that support the operations of the IAASB are facilitated by the International Federation of Accountants® or IFAC®.

The IAASB and IFAC do not accept responsibility for loss caused to any person who acts or refrains from acting in reliance on the material in this publication, whether such loss is caused by negligence or otherwise.

IAASB International Auditing and Assurance Standards Board

529 Fifth Avenue, New York, NY 10017
T + 1 (212) 286-9344 F +1 (212) 286-9570
www.iaasb.org