Endelig uttalelse
Desember 2019

Internasjonal revisjonsstandard 315 (revidert 2019)

ISA 315 (revidert 2019)

og

relaterte endringer i andre internasjonale standarder på bakgrunn av ISA 315 (revidert 2019).

IAASB International Auditing and Assurance Standards Board

Om IAASB

Dette dokumentet er utarbeidet og godkjent av International Auditing and Assurance Standards Board.

IAASBs mål er å ivareta allmennhetens interesser ved å sette standarder av høy kvalitet for revisjon, attestasjonsoppdrag og andre beslektede tjenester, og ved å fremme harmonisering av internasjonale og nasjonale revisjonsstandarder og standarder for attestasjonsoppdrag for derigjennom å høyne kvaliteten og ensartetheten av praksis over hele verden, og styrke allmennhetens tillit til profesjonen som leverer revisjonstjenester og attestasjonsoppdrag globalt.

IAASB utarbeider standarder for revisjonsoppdrag og andre attestasjonsoppdrag, og veiledninger for alle profesjonelle revisorer gjennom et samarbeid for standardsetting som omfatter Public Interest Oversight Board, som fører tilsyn med virksomheten til IAASB, og IAASB Consultative Advisory Group, som sørger for at det tas hensyn til allmennhetens interesser i utarbeidelsen av standardene og veiledningene. Strukturene og prosessene som støtter virksomheten til IAASB, er tilrettelagt av International Federation of Accountants (IFAC).

Se side 207 for informasjon om opphavsrett, varemerker og tillatelser.

INNHOLD

INTERNASJONAL REVISJONSSTANDARD 315 (REVIDERT 2019)

IDENTIFISERING OG VURDERING AV RISIKOENE FOR VESENTLIG FEILINFORMASJON

(Gjelder for revisjon av regnskaper for perioder som begynner 15. desember 2021 eller senere.)

INNHOLD

Internasjonal revisjonsstandard (ISA) 315 (revidert 2019) *Identifisering og vurdering av risikoene for vesentlig feilinformasjon* må leses i sammenheng med ISA 200 *Overordnede mål for den uavhengige revisor og gjennomføringen av en revisjon i samsvar med de internasjonale revisjonsstandardene*.

ISA 315 (revidert 2019) er godkjent av Public Interest Oversight Board (PIOB), som har konkludert med at utarbeidelsen av standarden er gjort på foreskreven måte og at det er tatt hensyn til allmennhetens interesse.

Innledning

Denne ISA-ens virkeområde

1. Denne internasjonale revisjonsstandarden (ISA-en) omhandler revisors oppgaver med og plikter til å identifisere og anslå risikoene for vesentlig feilinformasjon i regnskapet.

Nøkkelbegreper i denne ISA-en

2. ISA 200 omhandler revisors overordnede mål ved revisjon av regnskapet,[1] herunder å innhente tilstrekkelig og hensiktsmessig revisjonsbevis for å redusere revisjonsrisikoen til et akseptabelt lavt nivå.[2] Revisjonsrisiko er en funksjon av risikoene for vesentlig feilinformasjon og oppdagelsesrisiko.[3] ISA 200 forklarer at risikoene for vesentlig feilinformasjon kan foreligge på to nivåer:[4] på regnskapsnivå, og på påstandsnivå for transaksjonsklasser, kontosaldoer og tilleggsopplysninger.

3. ISA 200 krever at revisor utøver profesjonelt skjønn ved planlegging og gjennomføring av en revisjon, og at revisor planlegger og gjennomfører revisjonen med profesjonell skepsis og er innforstått med at det kan foreligge omstendigheter som kan medføre at regnskapet inneholder vesentlig feilinformasjon.[5]

4. Risiko på regnskapsnivå omfatter risikoer som er gjennomgripende for regnskapet som helhet, og kan påvirke mange påstander. Risiko for vesentlig feilinformasjon på påstandsnivå består av to komponenter, iboende risiko og kontrollrisiko:

   - Iboende risiko er muligheten for at en påstand om en transaksjonsklasse, kontosaldo eller tilleggsopplysning kan inneholde feilinformasjon som kan være vesentlig, enten enkeltvis eller sammen med annen feilinformasjon, før eventuelle tilhørende kontroller tas i betraktning.
   - Kontrollrisiko er risikoen for at feilinformasjon, som kan forekomme i en påstand om en transaksjonsklasse, kontosaldo eller tilleggsopplysning og som kan være vesentlig, enten enkeltvis eller sammen med annen feilinformasjon, ikke forhindres eller avdekkes og korrigeres i rett tid av enhetens internkontrollsystem.

5. ISA 200 forklarer at risikoer for vesentlig feilinformasjon identifiseres og anslås på påstandsnivå for å fastsette typen, tidspunktet og omfanget av videre revisjonshandlinger som er nødvendige for å innhente tilstrekkelig og hensiktsmessig revisjonsbevis.[6] Denne ISA-en krever separat vurdering av iboende risiko og kontrollrisiko for de identifiserte risikoene for vesentlig feilinformasjon på påstandsnivå. Som forklart i ISA 200, er iboende risiko høyere for noen påstander og tilknyttede

---

1 ISA 200 *Overordnede mål for den uavhengige revisor og gjennomføringen av en revisjon i samsvar med revisjonsstandardene*

2 ISA 200, punkt 17

3 ISA 200, punkt 13(c)

4 ISA 200, punkt A36

5 ISA 200, punkt 15–16

6 ISA 200, punkt A43a, og ISA 330 *Revisors håndtering av anslåtte risikoer*, punkt 6

transaksjonsklasser, kontosaldoer og tilleggsopplysninger enn for andre. Variasjonen i nivået på iboende risiko er i denne ISA-en referert til som «spekteret av iboende risiko».

6. Risikoer for vesentlig feilinformasjon som skal identifiseres og anslås av revisor, omfatter både risikoer som skyldes feil og misligheter. Selv om begge er omhandlet i denne ISA-en, er konsekvensen av misligheter av så stor betydning at ytterligere krav og veiledning til risikovurderingshandlinger og tilknyttede aktiviteter for å innhente informasjon til bruk for å identifisere, vurdere og håndtere risikoer for vesentlig feilinformasjon som skyldes misligheter er inkludert i ISA 240.[7]

7. Revisors identifisering og vurdering av risikoer er en repeterende og dynamisk prosess. Revisors forståelse av enheten og dens omgivelser, det gjeldende rammeverket for finansiell rapportering samt enhetens interne kontroll, og kravene om å identifisere og anslå risikoene for vesentlig feilinformasjon er innbyrdes avhengig av hverandre. Ved å opparbeide seg forståelsen som kreves i denne ISA-en, vil revisor kunne danne en forventning av risiko, som kan bli klarlagt gjennom arbeidet revisor utfører med å identifisere og anslå risikoer. Denne ISA-en og ISA 330 krever videre at revisor oppdaterer både sine risikovurderinger, overordnede handlinger og videre revisjonshandlinger, basert på revisjonsbevis innhentet gjennom de revisjonshandlingene som er utført i samsvar med ISA 330, eller på bakgrunn av ny informasjon.

8. ISA 330 krever at revisor utformer og iverksetter overordnede handlinger for å håndtere anslåtte risikoer for vesentlig feilinformasjon på regnskapsnivå.[8] ISA 330 forklarer videre at revisors vurdering av risikoene for vesentlig feilinformasjon på regnskapsnivå og revisors overordnede handlinger, påvirkes av revisors forståelse av kontrollmiljøet. ISA 330 krever også at revisor utformer og iverksetter videre revisjonshandlinger hvis type, tidspunkt og omfang er basert på og tilpasset de anslåtte risikoene for vesentlig feilinformasjon på påstandsnivå.[9]

---

7 ISA 240 *Revisors oppgaver med og plikter til å vurdere misligheter ved revisjon av regnskaper*

8 ISA 330, punkt 5

9 ISA 330, punkt 6

Skalerbarhet

9. ISA 200 stadfester at enkelte ISA-er inneholder veiledning for hvordan praktiseringen av kravene kan skaleres for alle enheter, uavhengig av om enhetens art og dens omgivelser er mer eller mindre komplekse.[10] Denne ISA-en er ment for revisjon av alle enheter, uavhengig av størrelse eller kompleksitet, og inneholder derfor spesifikke betraktninger knyttet til både mindre og mer komplekse enheter, der det er relevant. Selv om størrelsen på en enhet kan gi en indikasjon på enhetens kompleksitet, kan enkelte mindre enheter likevel være komplekse og enkelte større enheter mindre komplekse.

Ikrafttredelsesdato

10. Denne ISA-en gjelder for revisjon av regnskaper for perioder som begynner 15. desember 2021 eller senere.

Mål

11. Revisors mål er å identifisere og anslå risikoene for vesentlig feilinformasjon, enten de skyldes misligheter eller feil, på regnskaps- og påstandsnivå, for å danne grunnlag for utforming og gjennomføring av handlinger for å håndtere de anslåtte risikoene for vesentlig feilinformasjon

Definisjoner

12. I ISA-ene har følgende begreper den betydning som er beskrevet nedenfor:

    (a) *Påstander* – Uttalelser, eksplisitt eller på annet vis, om innregning, måling, presentasjon og tilleggsinformasjon, som er inkorporert i regnskapet, fremstilt av ledelsen og utarbeidet i samsvar med det gjeldende rammeverket for finansiell rapportering. Påstander benyttes av revisor ved identifisering, vurdering og håndtering av risikoene for de ulike typene av vesentlig feilinformasjon som kan forekomme (Jf. punkt A1).

    (b) *Forretningsrisiko* – En risiko, som er et resultat av viktige forhold, hendelser, omstendigheter, handlinger eller mangel på handlinger, som kan ha en negativ innvirkning på enhetens evne til å nå sine mål og gjennomføre sine strategier, eller som er et resultat av at det er fastsatt uegnede mål og strategier.

    (c) *Kontroller* –Retningslinjer og rutiner som en enhet etablerer for å nå kontrollmålene til ledelsen eller dem som har overordnet ansvar for styring og kontroll. I denne sammenheng: (Jf. punkt A2–A5)

[10] ISA 200, punkt A65a

(i) Retningslinjer er uttalelser om hva som bør eller ikke bør gjøres i enheten for å utøve kontroll. Slike uttalelser kan være dokumentert, tydelig uttrykt gjennom kommunikasjon eller underforstått gjennom handlinger og beslutninger.

(ii) Rutiner er handlinger for å implementere retningslinjer.

(d) *Generelle IT-kontroller* – Kontroller knyttet til enhetens IT-prosesser som underbygger den kontinuerlige og forsvarlige driften av IT-miljøet, herunder at kontrollene i enhetens informasjonssystem over prosessering av informasjon og integriteten av informasjonen (dvs. fullstendigheten, nøyaktigheten og gyldigheten av informasjon) fungerer kontinuerlig. Se også definisjonen av *IT-miljø*.

(e) *Informasjonsbehandlingskontroller* – Kontroller knyttet til prosessering av informasjon i IT-applikasjoner, eller manuelle prosesser for behandling i enhetens informasjonssystem, som direkte håndterer risikoer knyttet til informasjonens integritet (dvs. fullstendigheten, nøyaktigheten og gyldigheten av transaksjoner og annen informasjon). (Jf. punkt A6)

(f) *Iboende risikofaktorer* – Særtrekk ved hendelser eller forhold som påvirker i hvilken grad en påstand om en transaksjonsklasse, kontosaldo eller tilleggsopplysning kan inneholde feilinformasjon, enten det skyldes misligheter eller feil, før kontroller tas i betraktning. Disse faktorene kan være kvalitative eller kvantitative, og omfatter kompleksitet, subjektivitet, endring, usikkerhet eller mulig feilinformasjon som følge av manglende objektivitet hos ledelsen eller andre mislighetsrisikofaktorer[11] i den grad de påvirker iboende risiko. (Jf. punkt A7–A8)

(g) *IT-miljø* – IT-applikasjoner og støttende IT-infrastruktur, så vel som IT-prosesser og personell som er involvert i disse prosessene, som en enhet bruker for å understøtte forretningsdriften og oppnå strategiske forretningsmål. For denne ISA-ens formål:

(i) En IT-applikasjon er et program eller et sett med programmer som benyttes til å initiere, behandle, registrere og rapportere transaksjoner eller informasjon. IT-applikasjoner omfatter også datavarehus og rapportgeneratorer.

(ii) IT-infrastrukturen omfatter nettverket, operativsystemene og databasene samt tilhørende maskinvare og programvare.

(iii) IT-prosessene er enhetens prosesser for å administrere tilgang til IT-miljøet, administrere programendringer eller endringer i IT-miljøet og administrere IT-drift.

(h) *Relevante påstander* – En påstand om en transaksjonsklasse, kontosaldo eller tilleggsopplysning er relevant når den er tilknyttet en identifisert risiko for vesentlig feilinformasjon. Fastsettelsen av hvorvidt en påstand er en relevant påstand foretas før eventuelle tilknyttede kontroller tas i betraktning (dvs. iboende risiko). (Jf. punkt A9)

(i) Risikoer som oppstår som en følge av bruken av IT – Mulighet for at informasjonsbehandlingskontroller kan være ineffektiv utforming eller gjennomført, eller

[11] ISA 240, punkt A24–A27

risikoer knyttet til informasjonens integritet (dvs. fullstendigheten, nøyaktigheten og gyldigheten av transaksjoner og annen informasjon) i enhetens informasjonssystem, som følge av ineffektiv utforming eller drift av kontroller i enhetens IT-prosesser (se IT-miljø).

(j) Risikovurderingshandlinger – Revisjonshandlinger som er utformet og gjennomført for å identifisere og anslå risikoene for vesentlig feilinformasjon på regnskaps- og påstandsnivå, enten de skyldes misligheter eller feil.

(k) *Signifikante transaksjonsklasser, kontosaldoer eller tilleggsopplysninger* – En transaksjonsklasse, kontosaldo eller tilleggsopplysning hvor det finnes én eller flere relevante påstander.

(l) *Særskilt risiko* – En identifisert risiko for vesentlig feilinformasjon: (Jf. punkt A10)

(i) hvor vurderingen av iboende risiko er i den øvre delen av spekteret av iboende risiko, som følge av iboende risikofaktorers påvirkning på kombinasjonen av sannsynligheten for at feilinformasjon forekommer, og konsekvensen av den mulige feilinformasjonen dersom den skulle forekomme; eller

(ii) som skal behandles som en særskilt risiko i samsvar med krav i andre ISA-er.[12]

(m) *Internkontrollsystem* – Systemet som er utformet, implementert og vedlikeholdt av dem som har overordnet ansvar for styring og kontroll, ledelsen eller annet personell, for å gi rimelig sikkerhet for at enheten oppnår sine mål om pålitelig finansiell rapportering, effektiv drift og overholdelse av gjeldende lover og regler. For ISA-enes formål består internkontrollsystemet av fem komponenter som er gjensidig avhengig av hverandre:

(i) Kontrollmiljø;

(ii) Enhetens risikovurderingsprosess;

(iii) Enhetens prosess for overvåking av internkontrollsystemet;

(iv) Informasjonssystemet og kommunikasjon; og

(v) Kontrollaktiviteter.

Krav

Risikovurderingshandlinger og tilknyttede aktiviteter

13. Revisor skal utforme og gjennomføre risikovurderingshandlinger for å innhente revisjonsbevis som gir et tilstrekkelig grunnlag for å: (Jf. punkt A11–A18)

(a) Identifisere og anslå risikoer for vesentlig feilinformasjon på regnskaps- og påstandsnivå, enten de skyldes misligheter eller feil; og

(b) Utforme videre revisjonshandlinger i samsvar med ISA 330.

[12] ISA 240, punkt 27, og ISA 550 *Nærstående parter*, punkt 18

Revisor skal utforme og gjennomføre risikovurderingshandlinger på en måte som ikke tenderer mot å innhente bekreftende revisjonsbevis, eller ekskluderer revisjonsbevis som kan være motstridende. (Jf. punkt A14)

14. Risikovurderingshandlingene skal omfatte følgende handlinger: (Jf. punkt A19–A21)

    (a) Forespørsler til ledelsen og til andre relevante personer i enheten, herunder internrevisjonen (dersom enheten har en slik funksjon). (Jf. punkt A22–A26)

    (b) Analytiske handlinger. (Jf. punkt A27–A31)

    (c) Observasjon og inspeksjon. (Jf. punkt A32–A36)

Informasjon fra andre kilder

15. Ved innhenting av revisjonsbevis i samsvar med punkt 13, skal revisor vurdere informasjon fra: (Jf. punkt A37–A38)

    (a) revisors handlinger i forbindelse med vurderingen av aksept eller fortsettelse av kundeforholdet eller revisjonsoppdraget; og

    (b) der det er relevant, andre oppdrag som oppdragsansvarlig revisor har utført for enheten.

16. Når revisor har til hensikt å benytte informasjon innhentet gjennom revisors tidligere erfaring med enheten og fra revisjonshandlinger utført ved tidligere revisjoner, skal revisor vurdere hvorvidt denne informasjonen fortsatt er relevant og pålitelig som revisjonsbevis for denne revisjonen. (Jf. punkt A39–A41)

Diskusjon i revisjonsteamet

17. Oppdragsansvarlig revisor og andre sentrale medlemmer av revisjonsteamet skal diskutere anvendelsen av det gjeldende rammeverket for finansiell rapportering og i hvilken grad enhetens regnskap kan inneholde vesentlig feilinformasjon. (Jf. punkt A42–A47)

18. Dersom det er medlemmer av revisjonsteamet som ikke deltar i diskusjonen, skal oppdragsansvarlig revisor fastsette hvilke forhold som skal kommuniseres til disse medlemmene.

Opparbeidelse av forståelse av enheten og dens omgivelser, gjeldende rammeverk for finansiell rapportering og enhetens internkontrollsystem (Jf. punkt A48–A49)

Forståelse av enheten og dens omgivelser, og det gjeldende rammeverket for finansiell rapportering (Jf. punkt A50–A55)

19. Revisor skal gjennomføre risikovurderingshandlinger for å opparbeide seg en forståelse av:

    (a) følgende aspekter ved enheten og dens omgivelser:

        (i) Enhetens organisasjonsstruktur, eierskap, styring og kontroll, og forretningsmodell, herunder i hvilken grad forretningsmodellen integrerer bruken av IT; (Jf. punkt A56–A67)

        (ii) Bransjemessige, regulatoriske og andre eksterne faktorer; (Jf. punkt A68–A73) og

(iii) Parameterne som er benyttet, internt og eksternt, for å vurdere enhetens finansielle resultater; (Jf. punkt A74–A81)

(b) Det gjeldende rammeverket for finansiell rapportering, og enhetens regnskapspolicyer og årsakene til eventuelle endringer i disse; (Jf. punkt A82–A84) og

(c) Hvordan og i hvilken grad iboende risikofaktorer kan påvirke muligheten for feilinformasjon i regnskapet, knyttet til selve prosessen med å utarbeide regnskapet i samsvar med det gjeldende rammeverket for den finansielle rapporteringen, basert på forståelsen opparbeidet under (a) og (b). (Jf punkt A85-A89).

20. Revisor skal vurdere hvorvidt enhetens regnskapsprinsipper er hensiktsmessige og i samsvar med det gjeldende rammeverket for den finansielle rapporteringen.

Forståelse av komponentene i enhetens internkontrollsystem (Jf. punkt A90–A95)

Enhetens kontrollmiljø, risikovurderingsprosess og prosess for overvåking av internkontrollsystemet (Jf. punkt A96–A98)

Kontrollmiljø

<table>
<tr><td colspan="2">21. Revisor skal, gjennom utførelse av risikovurderingshandlinger, opparbeide seg en forståelse av kontrollmiljøet som er relevant for utarbeidelsen av regnskapet, ved å: (Jf. punkt A99–A100)</td></tr>
<tr><td>(a) forstå kombinasjonen av kontroller, prosesser og strukturer rettet mot: (Jf. punkt A101–A102)
(i) Hvordan ledelsen dekker sitt lederansvar, for eksempel med hensyn til enhetens kultur og ledelsens håndhevelse av integritet og etiske verdier;
(ii) Når de som har overordnet ansvar for styring og kontroll ikke er de samme som ledelsen, deres uavhengighet mot ledelsen og deres tilsyn med enhetens internkontrollsystem;
(iii) Enhetens tildeling av myndighet og ansvar;
(iv) Hvordan enheten tiltrekker seg, utvikler og beholder kompetente personer; og
(v) Hvordan enheten holder personer ansvarlige for oppgavene de er satt til å utføre for å oppfylle målene til internkontrollsystemet;</td><td>og
(b) Evaluere hvorvidt: (Jf. punkt A103–A108)
(i) Ledelsen, under oppsyn av dem som har overordnet ansvar for styring og kontroll, har utformet og opprettholdt en kultur som fremmer ærlighet og etisk atferd;
(ii) Kontrollmiljøet utgjør et hensiktsmessig grunnlag for de andre komponentene i enhetens internkontrollsystem tatt i betraktning enhetens type og kompleksitet; og
(iii) Identifiserte svakheter ved kontrollmiljøet kan undergrave de andre komponentene i enhetens internkontrollsystem.</td></tr>
</table>

Enhetens risikovurderingsprosess

22. Revisor skal, gjennom utførelse av risikovurderingshandlinger, opparbeide seg en forståelse av enhetens risikovurderingsprosess som er relevant for utarbeidelsen av regnskapet, ved å:	
(a) Forstå enhetens prosess for: (Jf. punkt A109–A110) (i) Identifisering av forretningsrisikoer som er relevante for innholdet i den finansielle rapporteringen; (Jf. punkt A62) (ii) Vurdering av betydningen av disse risikoene, herunder sannsynligheten for at de forekommer; og (iii) Håndtering av disse risikoene;	og (b) Vurdering av hvorvidt enhetens risikovurderingsprosess er hensiktsmessig ut fra enhetens omstendigheter, tatt i betraktning enhetens type og kompleksitet. (Jf. punkt A111–A113)

23. Dersom revisor identifiserer risikoer for vesentlig feilinformasjon som ledelsen ikke har identifisert, skal revisor:

(a) Fastsette hvorvidt disse risikoene er av en type som revisor forventer at enhetens risikovurderingsprosess skulle ha identifisert og, i så fall, opparbeide seg en forståelse av hvorfor enhetens risikovurderingsprosess ikke identifiserte disse risikoene for vesentlig feilinformasjon; og

(b) Vurdere innvirkningen på revisors vurdering i punkt 22(b).

Enhetens prosess for overvåking av internkontrollsystemet

24. Revisor skal, gjennom utførelse av risikovurderingshandlinger, opparbeide seg en forståelse av enhetens prosess for overvåking av internkontrollsystemet som er relevant for utarbeidelsen av regnskapet, ved å: (Jf. punkt A114–A115)	
(a) forstå de aspektene i enhetens prosess som er rettet mot: (i) Løpende og enkeltstående evalueringer for å overvåke kontrollenes effektivitet, og identifisering og utbedring av identifiserte svakheter ved intern kontrollen; (Jf. punkt A116–A117) og (ii) Enhetens internrevisjon, dersom enheten har en slik funksjon, herunder internrevisjonens type, oppgaver og plikter samt aktiviteter; (Jf. punkt A118) (b) Forstå kildene til informasjonen som er benyttet i enhetens prosess for overvåking av internkontrollsystemet, og på hvilket grunnlag	og (c) Vurdere hvorvidt enhetens prosess for overvåking av internkontrollsystemet er hensiktsmessig ut fra enhetens omstendigheter tatt i betraktning enhetens type og kompleksitet. (Jf. punkt A121–A122)

ledelsen vurderer at informasjonen er tilstrekkelig pålitelig for formålet; (Jf. punkt A119–A120)	

Informasjonssystem og kommunikasjon, og kontrollaktiviteter (Jf. punkt A123–A130)

Informasjonssystemet og kommunikasjon

25. Revisor skal gjennomføre risikovurderingshandlinger for å opparbeide seg en forståelse av enhetens informasjonssystem og kommunikasjon som er relevant for utarbeidelsen av regnskapet, ved å: (Jf. punkt A131)	
(a) Forstå enhetens aktiviteter knyttet til informasjonsbehandling, herunder data og informasjon, ressursene som benyttes for disse aktivitetene, og retningslinjene som, for signifikante transaksjonsklasser, kontosaldoer og tilleggsopplysninger, beskriver: (Jf. punkt A132–A143) (i) Hvordan informasjon flyter gjennom enhetens informasjonssystem, herunder: a. Hvordan transaksjoner initieres, og hvordan informasjon om dem registreres, behandles, eventuelt korrigeres, overføres til hovedboken og rapporteres i regnskapet; og b. Hvordan informasjon om hendelser og forhold ut over transaksjoner fanges opp, behandles og opplyses om i regnskapet; (ii) Regnskapsmaterialet, spesifikke kontoer i regnskapet og annet underliggende materiale knyttet til informasjonsflyten i informasjonssystemet; (iii) Den finansielle rapporteringsprosessen for utarbeidelsen av enhetens regnskap, herunder tilleggsopplysninger; og (iv) Enhetens ressurser, herunder IT-miljøet, som er relevante for (a)(i) til (a)(iii) ovenfor; (b) Forstå hvordan enheten kommuniserer vesentlige forhold i informasjonssystemet, som understøtter utarbeidelsen av regnskapet og relaterte rapporteringsoppgaver, og ved andre komponenter i internkontrollsystemet: (Jf. punkt A144–A145)	og (c) Vurdere hvorvidt enhetens informasjonssystem og kommunikasjon understøtter utarbeidelsen av enhetens regnskap i samsvar med det gjeldende rammeverket for finansiell rapportering, på en hensiktsmessig måte (Jf. punkt A146)

(i) Mellom personer i enheten, herunder hvordan roller og ansvar med hensyn til finansiell rapportering er kommunisert; (ii) Mellom ledelsen og dem som har overordnet ansvar for styring og kontroll; og (iii) Med eksterne parter, for eksempel kommunikasjon med tilsynsmyndigheter;	

Kontrollaktiviteter

26. Revisor skal gjennomføre risikovurderingshandlinger for å opparbeide seg en forståelse av komponenten «kontrollaktiviteter» ved å: (Jf. punkt A147–A157)	
(a) Identifisere de kontroller i kontrollaktivitetskomponenten, som håndterer risikoer for vesentlig feil på påstandsnivå: (i) Kontroller som håndterer en risiko, som er fastslått å være en særskilt risiko; (Jf. punkt A158–A159) (ii) Kontroller knyttet til posteringer, herunder ikke-standard posteringer benyttet for å registrere enkeltstående, uvanlige transaksjoner eller justeringer; (Jf. punkt A160–A161) (iii) Kontroller som revisor planlegger å teste om fungerer effektivt for å fastsette typen, tidspunktet og omfanget av substanstesting, som skal omfatte kontroller som håndterer risikoer der substanshandlinger alene ikke gir tilstrekkelig og hensiktsmessig revisjonsbevis; og (Jf. punkt A162–A164) (iv) Andre kontroller som revisor vurderer som hensiktsmessige for å kunne oppfylle målene i punkt 13 med hensyn til risikoer på påstandsnivå, basert på revisors profesjonelle skjønn; (Jf. punkt A165) (b) Basert på kontroller identifisert i (a), identifisere IT-applikasjonene og de andre aspektene ved enhetens IT-miljø som er gjenstand for risikoer som følger av bruken av IT; (Jf. punkt A166–A172) (c) For IT-applikasjonene og de andre aspektene ved IT-miljøet identifisert i (b), identifisere: (Jf. punkt A173–A174)	og (d) For hver kontroll identifisert i (a) eller (c)(ii): (Jf. punkt A175–A181) (i) Evaluere hvorvidt kontrollen er hensiktsmessig utformet for å håndtere risikoen for vesentlig feil på påstandsnivå, eller for å understøtte at andre kontroller kan fungere; og (ii) Fastslå hvorvidt kontrollen er implementert ved å utføre handlinger i tillegg til forespørsler til enhetens personell.

(i) De tilhørende risikoene som følger av bruken av IT; og (ii) Enhetens generelle IT-kontroller som håndterer slike risikoer;	

Kontrollmangler i enhetens internkontrollsystem

27. Basert på sin vurdering av hver av komponentene i enhetens internkontrollsystem, skal revisor fastslå hvorvidt det er identifisert en eller flere svakheter ved den interne kontrollen . (Jf. punkt A182–A183)

Identifisering og vurdering av risikoene for vesentlig feilinformasjon (Jf. punkt A184–A185)

Identifisering av risikoer for vesentlig feilinformasjon

28. Revisor skal identifisere risikoene for vesentlig feilinformasjon og fastslå hvorvidt de foreligger på: (Jf. punkt A186–A192)

    (a) Regnskapsnivå; (Jf. punkt A193–A200) eller

    (b) Påstandsnivå for transaksjonsklasser, kontosaldoer og tilleggsopplysninger. (Jf. punkt A201)

29. Revisor skal fastsette de relevante påstandene og de tilhørende signifikante transaksjonsklassene, kontosaldoene og tilleggsopplysningene. (Jf. punkt A202–A204)

Vurdering av risikoer for vesentlig feilinformasjon på regnskapsnivå

30. For identifiserte risikoer for vesentlig feilinformasjon på regnskapsnivå skal revisor anslå risikoene og: (Jf. punkt A193–A200)

    (a) Fastslå hvorvidt slike risikoer påvirker vurderingen av risikoer på påstandsnivå; og

    (b) Evaluere typen og omfanget av deres gjennomgripende virkning på regnskapet.

Vurdering av risikoer for vesentlig feilinformasjon på påstandsnivå

Vurdering av iboende risiko (Jf. punkt A205–A217)

31. For identifiserte risikoer for vesentlig feilinformasjon på påstandsnivå skal revisor vurdere iboende risiko ved å vurdere sannsynligheten for og betydningen av mulig feilinformasjon. I den forbindelse skal revisor ta i betraktning hvordan og i hvilken grad:

    (a) Iboende risikofaktorer påvirker eksponeringen av relevante påstander for feilinformasjon; og

    (b) Risikoene for vesentlig feilinformasjon på regnskapsnivå påvirker vurderingen av iboende risiko for risikoer for vesentlig feilinformasjon på påstandsnivå. (Jf. punkt A215–A216)

32. Revisor skal fastsette hvorvidt noen av de anslåtte risikoene for vesentlig feilinformasjon er særskilte risikoer. (Jf. punkt A218–A221)

33. For risikoene for vesentlig feilinformasjon på påstandsnivå skal revisor fastsette hvorvidt substanshandlinger alene ikke kan gi tilstrekkelig og hensiktsmessig revisjonsbevis . (Jf. punkt A222–A225)

Vurdering av kontrollrisiko

34. Dersom revisor planlegger å teste om kontroller fungerer effektivt, skal revisor vurdere kontrollrisiko. Dersom revisor ikke planlegger å teste om kontrollen fungerer effektivt, skal revisor vurdere kontrollrisiko på en slik måte at vurderingen av risikoen for vesentlig feilinformasjon er den samme som vurderingen av iboende risiko. (Jf. punkt A226–A229)

Evaluering av revisjonsbeviset innhentet gjennom risikovurderingshandlinger

35. Revisor skal evaluere hvorvidt revisjonsbeviset som er innhentet gjennom risikovurderingshandlingene, gir et hensiktsmessig grunnlag for identifiseringen og vurderingen av risikoene for vesentlig feilinformasjon. Dersom dette ikke er tilfellet, skal revisor utføre ytterligere risikovurderingshandlinger inntil revisjonsbeviset som er innhentet, gir et slikt grunnlag. Ved identifisering og vurdering av risikoene for vesentlig feilinformasjon skal revisor ta i betraktning alt revisjonsbevis som er innhentet gjennom risikovurderingshandlingene, uansett om de bekrefter eller er i strid med påstander utarbeidet av ledelsen. (Jf. punkt A230–A232)

Transaksjonsklasser, kontosaldoer og tilleggsopplysninger som ikke er signifikante, men som er vesentlige

36. For vesentlige transaksjonsklasser, kontosaldoer eller tilleggsopplysninger som ikke er vurdert til å være signifikante transaksjonsklasser, kontosaldoer eller tilleggsopplysninger, skal revisor vurdere hvorvidt revisors fastsettelse fortsatt er hensiktsmessig. (Jf. punkt A233–A235)

Oppdatering av risikovurdering

37. Dersom revisor innhenter ny informasjon som ikke er i overensstemmelse med revisjonsbeviset som revisor opprinnelig baserte identifiseringen eller vurderingen av risikoer for vesentlig feilinformasjon på, skal revisor oppdaterer identifiseringen eller vurderingen. (Jf. punkt A236)

Dokumentasjon

38. Revisor skal inkludere følgende i revisjonsdokumentasjonen:[13] (Jf. punkt A237–A241)

    (a) Diskusjonen i revisjonsteamet og de viktige beslutningene som er fattet;

    (b) Hovedelementene i revisors forståelse i samsvar med punkt 19, 21, 22, 24 og 25; informasjonskildene som revisors forståelse bygger på; og de risikovurderingshandlingene som er utført;

[13] ISA 230 *Revisjonsdokumentasjon*, punkt 8–11 og A6–A7

(c) Evalueringen av utformingen av identifiserte kontroller, og fastsettelsen av hvorvidt disse kontrollene er implementert, i samsvar med kravene i punkt 26; og

(d) De identifiserte og vurderte risikoene for vesentlig feilinformasjon på regnskapsnivå og påstandsnivå, herunder særskilte risikoer og risikoer der substanshandlinger alene ikke kan gi tilstrekkelig og hensiktsmessig revisjonsbevis, og begrunnelsen for de betydelige skjønnsmessige vurderingene som er foretatt.

Veiledning og utfyllende forklaringer

Definisjoner (Jf. punkt 12)

Påstander (Jf. punkt 12(a))

A1. Kategorier av påstander benyttes av revisorer for å vurdere de ulike typene mulig feilinformasjon som kan forekomme ved identifisering, vurdering og håndtering av risikoene for vesentlig feilinformasjon. Eksempler på disse kategoriene av påstander er beskrevet i punkt A190. Påstandene avviker fra de skriftlige uttalelsene som kreves av ISA 580,[14] for å bekrefte visse forhold eller underbygge annet revisjonsbevis.

Kontroller (Jf. punkt 12(c))

A2. Kontroller er integrert i komponentene i enhetens internkontrollsystem.

A3. Retningslinjer implementeres gjennom handlingene til personell i enheten, eller gjennom begrensninger som hindrer personell i utføre handlinger som kan være i konflikt med slike retningslinjer.

A4. Rutiner kan være pålagt, gjennom formell dokumentasjon eller annen kommunikasjon fra ledelsen eller dem som har overordnet ansvar for styring og kontroll, eller kan være et resultat av atferd som ikke er pålagt, men som i stedet er betinget av enhetens kultur. Rutiner kan håndheves gjennom handlingene som tillates av IT-applikasjonene som benyttes av enheten, eller andre aspekter ved enhetens IT-miljø.

A5. Kontroller kan være direkte eller indirekte. Direkte kontroller er kontroller som er presise nok til å håndtere risikoer for vesentlig feilinformasjon på påstandsnivå. Indirekte kontroller er kontroller som underbygger direkte kontroller.

Informasjonsbehandlingskontroller (Jf. punkt 12(e))

A6. Risikoer knyttet til informasjonens integritet oppstår som følge av mulighet for ineffektiv implementering av enhetens informasjonsretningslinjer, som er retningslinjer som definerer informasjonsflyten, registreringene og rapporteringsprosessene i enhetens informasjonssystem. Informasjonsbehandlingskontroller er rutiner som underbygger effektiv implementering av enhetens informasjonsretningslinjer. Informasjonsbehandlingskontroller kan være automatiserte (dvs. integrert

[14] ISA 580 *Skriftlige uttalelser*

i IT-applikasjoner) eller manuelle (for eksempel kontroller av inndata eller utdata) og kan bygge på andre kontroller, herunder andre informasjonsbehandlingskontroller eller generelle IT-kontroller.

Iboende risikofaktorer (Jf. punkt 12(f))

Vedlegg 2 inneholder ytterligere vurderinger knyttet til forståelsen av iboende risikofaktorer.

A7. Iboende risikofaktorer kan være kvalitative eller kvantitative, og påvirker påstanders mulighet for feilinformasjon. Kvalitative iboende risikofaktorer knyttet til utarbeidelsen av informasjon som kreves av det gjeldende rammeverket for finansiell rapportering, omfatter:

- Kompleksitet;
- Subjektivitet;
- Endring;
- Usikkerhet; eller
- Mulig feilinformasjon som følge av manglende objektivitet hos ledelsen eller andre mislighetsrisikofaktorer i den grad de påvirker iboende risiko.

A8. Andre iboende risikofaktorer som påvirker i hvilken grad en påstand om en transaksjonsklasse, kontosaldo eller tilleggsopplysning kan inneholde feilinformasjon, kan omfatte:

- Den kvantitative eller kvalitative betydningen av transaksjonsklassen, kontosaldoen eller tilleggsopplysningen; eller
- Volumet eller en mangel på ensartethet i sammensetningen av elementene som skal behandles gjennom transaksjonsklassen eller kontosaldoen, eller som skal gjenspeiles i tilleggsopplysningen.

Relevante påstander (Jf. punkt 12(h))

A9. En risiko for vesentlig feilinformasjon kan være knyttet til mer enn én påstand. Når dette er tilfellet, vil alle påstandene som risikoen er knyttet til, være relevante påstander. Dersom en påstand ikke har en identifisert risiko for vesentlig feilinformasjon, er den ikke en relevant påstand.

Særskilt risiko (Jf. punkt 12(l))

A10. Et forholds betydning avgjør om en risiko defineres som en særskilt risiko , og blir skjønnsmessig vurdert av revisor i den konteksten forholdet blir vurdert i. For iboende risiko kan betydning bli vurdert i kontekst av hvordan, og i hvilken grad, iboende risikofaktorer påvirker kombinasjonen av sannsynligheten for at feilinformasjon forekommer, og omfanget av den mulige feilinformasjonen dersom den forekommer.

Risikovurderingshandlinger og tilknyttede aktiviteter (Jf. punkt 13–18)

A11. Risikoene for vesentlig feilinformasjon som skal identifiseres og vurderes, omfatter både risikoer som skyldes misligheter og risikoer som skyldes feil, og begge dekkes av denne ISA-en. Misligheter er imidlertid av så stor betydning at ytterligere krav og veiledning til risikovurderingshandlinger og tilknyttede aktiviteter for å innhente informasjon som benyttes til å identifisere og anslå risikoer for vesentlig feilinformasjon som skyldes misligheter, er tatt inn i ISA 240.[15] I tillegg inneholder de følgende ISA-ene videre krav og veiledning til identifisering og vurdering av risikoer for vesentlig feilinformasjon knyttet til spesifikke forhold eller omstendigheter:

- ISA 540 (revidert)[16] med hensyn til regnskapsestimater;
- ISA 550[22] med hensyn til nærstående parter og transaksjoner med disse;
- ISA 570 (revidert)[17] med hensyn til fortsatt drift; og
- ISA 600[18] med hensyn til konsernregnskaper.

A12. Profesjonell skepsis er nødvendig for å kunne foreta en kritisk vurdering av revisjonsbevis som er innhentet ved gjennomføring av risikovurderingshandlingene, og hjelper revisor med å være oppmerksom på revisjonsbevis som ikke tenderer mot å bekrefte eksistensen av risikoer, eller som kan være i strid med eksistensen av risikoer. Profesjonell skepsis er en holdning som utøves når revisor foretar profesjonelle skjønnsmessige vurderinger som skal utgjøre et grunnlag for revisors handlinger. Revisor utøver profesjonelt skjønn ved fastsettelse av hvorvidt revisor har innhentet revisjonsbevis som gir et hensiktsmessig grunnlag for risikovurdering.

A13. Revisors utøvelse av profesjonell skepsis kan omfatte:

- Å stille spørsmål ved motstridende informasjon og påliteligheten av dokumenter;
- Å vurdere svar på forespørsler og annen informasjon som er innhentet fra ledelsen og dem som har overordnet ansvar for styring og kontroll;
- Å være oppmerksom på forhold som kan tyde på mulig feilinformasjon som skyldes misligheter eller feil; og
- Å vurdere hvorvidt innhentet revisjonsbevis underbygger revisors identifisering og vurdering av risikoene for vesentlig feilinformasjon i lys av enhetens type og omstendigheter.

Hvorfor det er viktig å innhente revisjonsbevis på en objektiv måte (Jf. punkt 13)

A14. Utforming og gjennomføring av risikovurderingshandlinger for å innhente revisjonsbevis som underbygger identifiseringen og vurderingen av risikoer for vesentlig feilinformasjon på en objektiv

---

15 ISA 240, punkt 12–27

16 ISA 540 (revidert) *Revisjon av regnskapsestimater og tilhørende tilleggsopplysninger*

17 ISA 570 (revidert) *Fortsatt drift*

18 ISA 600 *Særlige hensyn ved revisjon av konsernregnskaper (herunder arbeidet til revisorer i konsernenheter)*

måte, kan hjelpe revisor med å identifisere mulig motstridende informasjon, som hjelper revisor i utøvelsen av profesjonell skepsis ved identifisering og vurdering av risikoer for vesentlig feilinformasjon.

Kilder til revisjonsbevis (Jf. punkt 13)

A15. Utforming og gjennomføring av risikovurderingshandlinger for å innhente revisjonsbevis på en objektiv måte kan innebære innhenting av bevis fra flere kilder i og utenfor enheten. Revisor er imidlertid ikke pålagt å utføre et uttømmende søk for å identifisere alle mulige kilder til revisjonsbevis. I tillegg til informasjon fra andre kilder[19] kan informasjonskilder for risikovurderingshandlinger omfatte:

- Interaksjoner med ledelsen, dem som har overordnet ansvar for styring og kontroll og andre nøkkelpersonell i enheten, for eksempel interne revisorer.
- Bestemte eksterne parter som for eksempel tilsynsmyndigheter, enten informasjonen innhentes direkte eller indirekte.
- Offentlig tilgjengelig informasjon om enheten, for eksempel pressemeldinger utstedt av enheten, materiale til analytikere eller møter med investorgrupper, rapporter fra analytikere eller informasjon om handelsaktivitet.

Uavhengig av informasjonskilder vurderer revisor relevansen og påliteligheten av informasjonen som skal benyttes som revisjonsbevis i samsvar med ISA 500.[20]

Skalerbarhet (Jf. punkt 13)

A16. Typen og omfanget av risikovurderingshandlinger vil variere basert på enhetens type og omstendigheter (for eksempel formaliseringen av enhetens retningslinjer og rutiner samt prosesser og systemer). Revisor utøver profesjonelt skjønn for å fastsette typen og omfanget av risikovurderingshandlinger som skal utføres for å oppfylle kravene i denne ISA-en.

A17. Selv om formaliseringen av en enhets retningslinjer og rutiner samt prosesser og systemer kan variere, kreves det likevel at revisor opparbeider seg en forståelse i samsvar med punkt 19, 21, 22, 24, 25 og 26.

Eksempler:

Enkelte enheter, herunder mindre komplekse enheter, og særlig eierkontrollerte virksomheter, har ikke nødvendigvis etablert strukturerte prosesser og systemer (for eksempel en risikovurderingsprosess eller en prosess for overvåking av internkontrollsystemet), eller kan ha etablert prosesser eller systemer med begrenset dokumentasjon eller manglende konsistens i måten de utføres på. Når slike systemer og prosesser ikke er formaliserte, kan revisor fortsatt være i stand til å gjennomføre risikovurderingshandlinger gjennom observasjon og forespørsler.

[19] Se punkt A37 og A38.

[20] ISA 500 *Revisjonsbevis*, punkt 7

Andre enheter, typisk mer komplekse enheter, forventes å ha mer formaliserte og dokumenterte retningslinjer og rutiner. Revisor kan bruke slik dokumentasjon ved utførelse av risikovurderingshandlinger.

A18. Typen og omfanget av risikovurderingshandlinger som skal utføres ved et nytt oppdrag, kan være mer omfattende enn handlinger som utføres ved løpende oppdrag. I etterfølgende perioder kan revisor fokusere på endringer som har forekommet siden foregående periode.

Typer risikovurderingshandlinger (Jf. punkt 14)

A19. ISA 500[21] beskriver de forskjellige typene av revisjonshandlinger som kan utføres for å innhente revisjonsbevis gjennom risikovurderingshandlinger og videre revisjonshandlinger. Typen, tidspunktet og omfanget av revisjonshandlingene kan påvirkes av det faktum at enkelte regnskapsdata og annet bevis bare er tilgjengelige i elektronisk form eller på bestemte tidspunkt.[22] Revisor kan utføre substanshandlinger eller tester av kontroller, i samsvar med ISA 330, samtidig med risikovurderingshandlinger der dette er kostnadseffektivt. Innhentet revisjonsbevis som underbygger identifiseringen og vurderingen av risikoer for vesentlig feilinformasjon, kan også underbygge avdekkingen av feilinformasjon på påstandsnivå eller evalueringen av om kontroller fungerer effektivt.

A20. Selv om det kreves at revisor utfører alle risikovurderingshandlingene beskrevet i punkt 14 i løpet av opparbeidelsen av den påkrevde forståelsen av enheten og dens omgivelser, det gjeldende rammeverket for finansiell rapportering og enhetens internkontrollsystem (se punkt 19–26), kreves det ikke at revisor utfører alle handlingene for hvert enkelt aspekt ved denne forståelsen. Andre handlinger kan utføres når informasjonen som skal innhentes kan være til hjelp ved identifisering av risikoer for vesentlig feilinformasjon. Eksempler på slike handlinger kan omfatte forespørsler til enhetens eksterne juridiske rådgivere eller eksterne tilsynsmyndigheter, eller til verdsettelseseksperter enheten har benyttet.

Automatiserte verktøy og teknikker (Jf. punkt 14)

A21. Ved hjelp av automatiserte verktøy og teknikker kan revisor gjennomføre risikovurderingshandlinger på store mengder data (fra hovedboken, reskontroer eller andre driftsdata), herunder analyser, etterregninger, gjentakelser eller avstemminger.

Forespørsler til ledelsen og andre i enheten (Jf. punkt 14(a))

Hvorfor det rettes forespørsler til ledelsen og andre i enheten

A22. Informasjon innhentet av revisor for å underbygge et hensiktsmessig grunnlag for identifisering og vurdering av risikoer, og utforming av videre revisjonshandlinger, kan innhentes gjennom forespørsler til ledelsen og dem som er ansvarlige for finansiell rapportering.

---

[21] ISA 500, punkt A14–A17 og A21–A25

[22] ISA 500, punkt A12

A23. Forespørsler til ledelsen og dem som er ansvarlige for finansiell rapportering, og til andre relevante personer i enheten og andre personell på ulike ansvarsnivåer, kan gi revisor forskjellige perspektiver ved identifisering og vurdering av risikoer for vesentlig feilinformasjon.

Eksempler:

- Forespørsler rettet til dem som har overordnet ansvar for styring og kontroll, kan hjelpe revisor med å forstå omfanget av tilsynet de fører med ledelsens utarbeidelse av regnskapet. ISA 260 (revidert)[23] identifiserer viktigheten av effektiv toveiskommunikasjon for å hjelpe revisor med å innhente informasjon fra dem som har overordnet ansvar for styring og kontroll i denne sammenheng.
- Forespørsler rettet til personell som er ansvarlige for å initiere, behandle eller registrere komplekse eller uvanlige transaksjoner, kan hjelpe revisor med å evaluere om valget og anvendelsen av bestemte regnskapspolicyer er hensiktsmessig.
- Forespørsler rettet til interne juridiske rådgivere kan gi informasjon om forhold som rettstvister, overholdelse av lover og forskrifter, kjennskap til misligheter eller mistanke om misligheter som berører enheten, garantier, forpliktelser i forbindelse med serviceavtaler, samarbeid (for eksempel felleskontrollert virksomhet) med forretningspartnere og betydningen av kontraktsvilkår.
- Forespørsler rettet til markedsførings- eller salgspersonale kan gi informasjon om endringer i enhetens markedsføringsstrategier, salgstrender eller kontraktsbestemmelser med kunder.
- Forespørsler rettet til risikostyringsfunksjonen (eller til dem som utøver slike roller) kan gi informasjon om driftsmessige og regulatoriske risikoer som kan påvirke finansiell rapportering.
- Forespørsler rettet til IT-personale kan gi informasjon om systemendringer, system- eller kontrollsvikt eller andre IT-relaterte risikoer.

Særlige hensyn knyttet til enheter i offentlig sektor

A24. Når revisorer i enheter i offentlig sektor retter forespørsler til dem som kan inneha informasjon som forventes å være til hjelp ved identifisering av vesentlig feilinformasjon, kan de innhente informasjon fra flere kilder, for eksempel fra revisorer som deltar i forvaltningsrevisjon eller andre revisjoner relatert til enheten.

Forespørsler til internrevisjonsfunksjonen

Vedlegg 4 inneholder vurderinger knyttet til forståelsen av enhetens internrevisjonsfunksjon.

[23] ISA 260 (revidert) *Kommunikasjon med dem som har overordnet ansvar for styring og kontroll*, punkt 4(b)

Hvorfor det rettes forespørsler til internrevisjonsfunksjonen (dersom enheten har en slik funksjon)

A25. Dersom en enhet har en internrevisjonsfunksjon, kan forespørsler rettet til relevante personer i funksjonen hjelpe revisor med å forstå enheten og dens omgivelser, og enhetens internkontrollsystem, ved identifisering og vurdering av risikoer.

Særlige hensyn knyttet til enheter i offentlig sektor

A26. Revisorer i enheter i offentlig sektor har ofte tilleggsoppgaver knyttet til intern kontroll og overholdelse av gjeldende lover og forskrifter. Forespørsler til relevante personer i internrevisjonsfunksjonen kan hjelpe revisor med å identifisere risikoen for vesentlig manglende overholdelse av gjeldende lover og forskrifter og risikoen for kontrollmangler knyttet til finansiell rapportering.

Analytiske handlinger (Jf. punkt 14(b))

Hvorfor analytiske handlinger utføres som en risikovurderingshandling

A27. Analytiske handlinger kan bidra til å identifisere uoverensstemmelser, uvanlige transaksjoner eller hendelser samt beløp, forholdstall og trender som kan indikere at det foreligger forhold som har innvirkning på revisjonen. Uvanlige eller uventede sammenhenger som blir identifisert, kan hjelpe revisor med å identifisere risikoer for vesentlig feilinformasjon, særlig risikoer for vesentlig feilinformasjon som skyldes misligheter.

A28. Analytiske handlinger utført som risikovurderingshandlinger kan derfor bidra ved identifiseringen og vurderingen av risikoer for vesentlig feilinformasjon ved å identifisere aspekter ved enheten som revisor ikke var klar over, eller ved å gi en forståelse av hvordan iboende risikofaktorer, for eksempel endringer, påvirker påstanders mulighet for feilinformasjon.

Typer av analytiske handlinger

A29. Analytiske handlinger utført som risikovurderingshandlinger kan:

- Omfatte både finansiell og ikke-finansiell informasjon, for eksempel forholdet mellom salg og antall kvadratmeter salgsflate eller volumet av solgte varer (ikke-finansiell).
- Bruke data som er aggregert på et høyt nivå. Følgelig kan resultatene av disse analytiske handlingene gi en generell, første indikasjon på sannsynligheten for vesentlig feilinformasjon.

> **Eksempel**:
>
> Ved revisjon av en del enheter, herunder dem som har mindre komplekse forretningsmodeller og prosesser og et mindre komplekst informasjonssystem, kan revisor utføre en enkel sammenligning av informasjon, for eksempel endringen i interims- eller månedlige kontosaldoer fra foregående perioder, for å få en indikasjon på potensielt høyere risikoområder.

A30. Denne ISA-en omhandler revisors bruk av analytiske handlinger som risikovurderingshandlinger. ISA 520[24] omhandler revisors bruk av analytiske handlinger som substanshandlinger («analytiske substanshandlinger»), og revisors oppgaver med og plikter til å utføre analytiske handlinger mot slutten av revisjonen. Følgelig kreves det ikke at analytiske handlinger utført som risikovurderingshandlinger skal utføres i samsvar med kravene i ISA 520. Kravene og veiledningen i ISA 520 kan imidlertid være til nytte når revisor utfører analytiske handlinger som en del av risikovurderingshandlingene.

Automatiserte verktøy og teknikker

A31. Analytiske handlinger kan utføres ved hjelp av en rekke verktøy eller teknikker, som kan være automatiserte. Anvendelse av automatiserte analytiske handlinger på data kan refereres til som dataanalyse.

> **Eksempel**:
>
> Revisor kan bruke et regneark for å sammenligne faktiske registrerte beløp med budsjetterte beløp, eller utføre en mer avansert rutine for å trekke ut data fra enhetens informasjonssystem og deretter analysere disse dataene ved hjelp av visualiseringsteknikker for å identifisere transaksjonsklasser, kontosaldoer eller tilleggsopplysninger som kan kreve videre særskilte risikovurderingshandlinger.

Observasjon og inspeksjon (Jf. punkt 14(c))

Hvorfor observasjon og inspeksjon utføres som risikovurderingshandlinger

A32. Observasjon og inspeksjon kan underbygge, bekrefte eller motsi forespørsler rettet til ledelsen og andre, og kan også gi informasjon om enheten og dens omgivelser.

Skalerbarhet

A33. Når retningslinjer og rutiner ikke er dokumentert, eller når enheten har mindre formaliserte kontroller, kan revisor fortsatt være i stand til å innhente revisjonsbevis for å underbygge identifiseringen og vurderingen av risikoer for vesentlig feilinformasjon gjennom observasjon eller inspeksjon av gjennomføringen av kontrollen.

> **Eksempler**:
>
> - Revisor kan opparbeide seg en forståelse av kontroller knyttet til en varetelling, selv om de ikke er dokumentert av enheten, gjennom direkte observasjon.
> - Revisor kan være i stand til å observere arbeidsdelingen.
> - Revisor kan være i stand til å observere at passord tastes inn.

[24] ISA 520 *Analytiske handlinger*

Observasjon og inspeksjon som risikovurderingshandlinger

A34. Risikovurderingshandlinger kan omfatte observasjon eller inspeksjon av følgende:

- Enhetens drift.
- Interne dokumenter (for eksempel forretningsplaner og -strategier), regnskapsmateriale og håndbøker for internkontroll.
- Rapporter utarbeidet av ledelsen (for eksempel kvartalsvise ledelsesrapporter og delårsregnskap) og dem som har overordnet ansvar for styring og kontroll (for eksempel referater fra styremøter).
- Enhetens lokaler og anlegg.
- Informasjon innhentet fra eksterne kilder, for eksempel handels- og økonomiske tidsskrifter, rapporter fra analytikere, banker eller kredittopplysningsbyråer; regulatoriske eller finansielle publikasjoner; eller andre eksterne dokumenter om enhetens finansielle resultater (for eksempel dem det refereres til i punkt A79).
- Atferd og handlinger til ledelsen eller dem som har overordnet ansvar for styring og kontroll (for eksempel observasjon av et møte i revisjonsutvalget).

Automatiserte verktøy og teknikker

A35. Automatiserte verktøy eller teknikker kan også benyttes til å observere eller inspisere, særlig eiendeler, for eksempel ved bruk av fjernstyrte observasjonsverktøy (for eksempel en drone).

Særlige hensyn knyttet til enheter i offentlig sektor

A36. Risikovurderingshandlinger utført av revisorer i offentlig sektor kan også omfatte observasjon og inspeksjon av dokumenter utarbeidet av ledelsen for lovgivende myndighet, for eksempel dokumenter relatert til pålagt resultatrapportering.

Informasjon fra andre kilder (Jf. punkt 15)

Hvorfor revisor vurderer informasjon fra andre kilder

A37. Informasjon innhentet fra andre kilder kan være relevant for identifiseringen og vurderingen av risikoer for vesentlig feilinformasjon ved at den kan gi informasjon om og innsikt i:

- Typen enhet og dens forretningsrisikoer, og hva som kan være endret fra foregående perioder.
- Integriteten og de etiske verdiene til ledelsen og dem som har overordnet ansvar for styring og kontroll, som også kan være relevant for revisors forståelse av kontrollmiljøet.
- Det gjeldende rammeverket for finansiell rapportering og dens anvendelse på typen og omstendighetene ved enheten.

Andre relevante kilder

A38. Andre relevante kilder til informasjon omfatter:

- Revisors handlinger knyttet til aksept eller fortsettelse av kundeforhold eller revisjonsoppdrag i samsvar med ISA 220, herunder konklusjonene som er trukket i den sammenheng.[25]
- Andre oppdrag som oppdragsansvarlig revisor har utført for enheten. Oppdragsansvarlig revisor kan ha opparbeidet seg kunnskap som er relevant for revisjonen, herunder om enheten og dens omgivelser, ved gjennomføring av andre oppdrag for enheten. Slike oppdrag kan omfatte avtalte kontrollhandlinger eller andre revisjons- eller attestasjonsoppdrag, herunder oppdrag for å håndtere økende rapporteringskrav i jurisdiksjonen.

Informasjon fra revisors tidligere erfaring med enheten og tidligere revisjoner (Jf. punkt 16)

Hvorfor informasjon fra tidligere revisjoner er viktig for den aktuelle revisjonen

A39. Revisors tidligere erfaring med enheten og revisjonshandlinger som er utført ved tidligere revisjoner kan gi revisor informasjon som er relevant for revisors fastsettelse av typen og omfanget av risikovurderingshandlinger, og identifiseringen og vurderingen av risikoer for vesentlig feilinformasjon.

Typen informasjon fra tidligere revisjoner

A40. Revisors tidligere erfaring med enheten og revisjonshandlinger som er utført ved tidligere revisjoner kan gi revisor informasjon om forhold som:

- Tidligere feilinformasjon og hvorvidt den ble korrigert i rett tid.
- Typen enhet og dens omgivelser, og enhetens internkontrollsystem (herunder kontrollmangler).
- Betydelige endringer som enheten eller dens virksomhet kan ha vært gjenstand for siden den foregående regnskapsperioden.
- De særlige transaksjonstypene og andre hendelser eller kontosaldoer (og tilhørende tilleggsopplysninger) der revisor hadde vanskeligheter med å gjennomføre de nødvendige revisjonshandlingene, for eksempel på grunn av deres kompleksitet.

A41. Det kreves at revisor fastslår hvorvidt informasjon som er innhentet gjennom revisors tidligere erfaring med enheten og revisjonshandlinger utført ved tidligere revisjoner, fortsatt er relevant og pålitelig dersom revisor har til hensikt å bruke denne informasjonen i den aktuelle revisjonen. Dersom typen eller omstendighetene ved enheten er endret, eller det er innhentet ny informasjon, kan det være at informasjon fra tidligere perioder ikke lenger er relevant eller pålitelig for den aktuelle revisjonen. For å fastslå hvorvidt det har skjedd endringer som kan påvirke relevansen eller påliteligheten av denne informasjonen, kan revisor rette forespørsler og utføre andre hensiktsmessige revisjonshandlinger,

[25] ISA 220 *Kvalitetskontroll av revisjon av regnskaper*, punkt 12

for eksempel vugge-til-grav-tester av relevante systemer. Dersom informasjonen ikke er pålitelig, kan revisor vurdere å utføre videre handlinger som er hensiktsmessige ut fra omstendighetene.

Diskusjon i revisjonsteamet (Jf. punkt 17–18)

Hvorfor det kreves at revisjonsteamet diskuterer anvendelsen av det gjeldende rammeverket for finansiell rapportering og muligheten for at enhetens regnskap inneholder vesentlig feilinformasjon

A42. Diskusjonen i revisjonsteamet om anvendelsen av det gjeldende rammeverket for finansiell rapportering og muligheten for at enhetens regnskap inneholder vesentlig feilinformasjon:

- Gir mer erfarne medlemmer av revisjonsteamet, herunder oppdragsansvarlig revisor, mulighet til å dele den innsikt deres kjennskap til enheten gir. Deling av informasjon bidrar til å gi alle medlemmer av revisjonsteamet en bedre forståelse.
- Gjør det mulig for medlemmene av revisjonsteamet å utveksle informasjon om forretningsrisikoene som enheten er gjenstand for, hvordan iboende risikofaktorer kan påvirke i hvilken grad transaksjonsklasser, kontosaldoer og tilleggsopplysninger kan inneholde feilinformasjon, og hvordan og hvor regnskapet kan være eksponert for vesentlig feilinformasjon som skyldes misligheter eller feil.
- Bidrar til å gi medlemmene av revisjonsteamet en bedre forståelse av muligheten for vesentlig feilinformasjon i regnskapet på de særskilte områdene de har fått tildelt, og til å forstå hvordan resultatene av revisjonshandlingene de utfører kan påvirke andre aspekter ved revisjonen, herunder beslutninger om typen, tidspunktet og omfanget av videre revisjonshandlinger. Diskusjonen bidrar særlig til at medlemmer av revisjonsteamet foretar en nærmere vurdering av motstridende informasjon basert på hvert enkelt medlems egen forståelse av typen og omstendighetene ved enheten.
- Danner grunnlaget for at medlemmer av revisjonsteamet kommuniserer og deler ny informasjon som innhentes under hele revisjonen, som kan påvirke vurderingen av risikoene for vesentlig feilinformasjon eller revisjonshandlingene som utføres for å håndtere disse risikoene.

ISA 240 krever at diskusjonen i revisjonsteamet legger spesielt vekt på hvordan og hvor enhetens regnskap kan være eksponert for vesentlig feilinformasjon som skyldes misligheter, herunder hvordan misligheter kan oppstå.[26]

A43. Profesjonell skepsis er nødvendig for å kunne foreta en kritisk vurdering av revisjonsbevis, og en robust og åpen diskusjon i revisjonsteamet, herunder for gjentakende revisjoner, kan føre til en bedre identifisering og vurdering av risikoene for vesentlig feilinformasjon. Et annet utfall av diskusjonen kan være at revisor identifiserer særskilte områder ved revisjonen der utøvelse av profesjonell skepsis kan være særlig viktig, noe som kan føre til at mer erfarne medlemmer av revisjonsteamet

[26] ISA 240, punkt 16

som har de nødvendige ferdighetene deltar i gjennomføringen av revisjonshandlinger på disse områdene.

Skalerbarhet

A44. Når oppdraget utføres av en enkelt person, for eksempel en alenepraktiserende revisor (dvs. når en diskusjon i revisjonsteamet ikke er mulig), kan det likevel være nyttig for revisor å vurdere forholdene referert til i punkt A42 og A46 for å identifisere hvor det kan foreligge risikoer for vesentlig feilinformasjon.

A45. Når et oppdrag utføres av et stort revisjonsteam, for eksempel ved revisjon av konsernregnskap, er det ikke alltid nødvendig eller praktisk for diskusjonen at alle medlemmene deltar i en enkelt diskusjon (for eksempel ved en revisjon som utføres på flere steder), og det er heller ikke nødvendig at alle medlemmene av revisjonsteamet informeres om alle beslutningene som fattes under diskusjonen. Oppdragsansvarlig revisor kan diskutere forhold med sentrale medlemmer av revisjonsteamet, herunder, dersom det anses hensiktsmessig, med dem som har spesialistferdigheter eller -kunnskaper, og med dem som er ansvarlige for revisjon av konsernenheter, og samtidig delegere diskusjon med andre, i den grad kommunikasjonen mellom medlemmene av revisjonsteamet opprettholdes på det nivået som anses som nødvendig. En kommunikasjonsplan som er godkjent av oppdragsansvarlig revisor, kan være nyttig.

Diskusjon om tilleggsopplysninger i det gjeldende rammeverket for finansiell rapportering

A46. Som en del av diskusjonen i revisjonsteamet, bidrar vurderingen av opplysningskravene i det gjeldende rammeverket for finansiell rapportering til å identifisere tidlig i revisjonen hvor det kan foreligge risikoer for vesentlig feilinformasjon i forbindelse med tilleggsopplysninger, også under omstendigheter der det gjeldende rammeverket for finansiell rapportering kun krever forenklede tilleggsopplysninger. Forhold som revisjonsteamet kan diskutere, omfatter:

- Endringer i kravene til finansiell rapportering som kan føre til nye eller reviderte tilleggsopplysninger av betydning;
- Endringer i enhetens omgivelser, finansielle betingelser eller aktiviteter som kan resultere i nye eller reviderte tilleggsopplysninger av betydning, for eksempel en foretaksintegrasjon av betydning i revisjonsperioden;
- Tilleggsopplysninger som det tidligere har vært vanskelig å innhente tilstrekkelig og hensiktsmessig revisjonsbevis for; og
- Tilleggsopplysninger om komplekse forhold, herunder forhold som innebærer at ledelsen må utøve betydelig skjønn med hensyn til hvilken informasjon det skal opplyses om.

Særlige hensyn knyttet til enheter i offentlig sektor

A47. Som en del av diskusjonen i revisjonsteamet for revisorer i enheter i offentlig sektor, kan vurderingen også omfatte andre, mer generelle mål, og tilhørende risikoer, som følger av revisjonsmandatet eller forpliktelsene for enheter i offentlig sektor.

Opparbeidelse av en forståelse av enheten og dens omgivelser, det gjeldende rammeverket for finansiell rapportering og enhetens internkontrollsystem (Jf. punkt 19–27)

> **Vedlegg 1 til og med 6** inneholder ytterligere vurderinger knyttet til opparbeidelsen av en forståelse av enheten og dens omgivelser, det gjeldende rammeverket for finansiell rapportering og enhetens internkontrollsystem.

Opparbeidelse av den påkrevde forståelsen (Jf. punkt 19–27)

A48. Opparbeidelse av en forståelse av enheten og dens omgivelser, det gjeldende rammeverket for finansiell rapportering og enhetens internkontrollsystem er en dynamisk og gjentakende prosess som består av innhenting, oppdatering og analyse av informasjon gjennom hele revisjonen. Revisors forventninger kan derfor endres etter hvert som det innhentes ny informasjon.

A49. Revisors forståelse av enheten og dens omgivelser og det gjeldende rammeverket for finansiell rapportering kan også bidra til at revisor etablerer innledende forventninger om hvilke transaksjonsklasser, kontosaldoer og tilleggsopplysninger som kan være signifikante transaksjonsklasser, kontosaldoer og tilleggsopplysninger. Disse forventede signifikante transaksjonsklassene, kontosaldoene og tilleggsopplysningene danner grunnlaget for omfanget av revisors forståelse av enhetens informasjonssystem.

Hvorfor det kreves en forståelse av enheten og dens omgivelser og det gjeldende rammeverket for finansiell rapportering (Jf. punkt 19–20)

A50. Revisors forståelse av enheten og dens omgivelser og det gjeldende rammeverket for finansiell rapportering hjelper revisor med å forstå hendelsene og forholdene som er relevante for enheten, og med å identifisere hvordan iboende risikofaktorer påvirker påstanders mulighet for feilinformasjon ved utarbeidelsen av regnskapet i samsvar med det gjeldende rammeverket for finansiell rapportering, og i hvilken grad de gjør det. Slik informasjon utgjør en referanseramme for revisors arbeid med å identifisere og anslå risikoer for vesentlig feilinformasjon. Denne referanserammen hjelper også revisor med å planlegge revisjonen og utøve profesjonelt skjønn og profesjonell skepsis gjennom hele revisjonen, for eksempel når revisor:

- Identifiserer og vurderer risikoer for vesentlig feilinformasjon i regnskapet i samsvar med ISA 315 (revidert 2019) eller andre relevante standarder (for eksempel knyttet til risikoer for misligheter i samsvar med ISA 240, eller når revisor identifiserer eller vurderer risikoer knyttet til regnskapsestimater i samsvar med ISA 540 (revidert));
- Gjennomfører handlinger for å bidra til å identifisere tilfeller av manglende overholdelse av lover og forskrifter som kan ha en vesentlig virkning på regnskapet i samsvar med ISA 250;[27]

[27] ISA 250 (revidert) *Vurdering av lover og forskrifter ved revisjon av regnskaper* punkt 14

- Evaluerer hvorvidt regnskapet gir adekvate tilleggsopplysninger i samsvar med ISA 700 (revidert);[28]
- Fastsetter vesentlighet eller arbeidsvesentlighet i samsvar med ISA 320;[29] eller
- Vurderer om valget og anvendelsen av regnskapspolicyer er hensiktsmessig, og om tilleggsopplysningene i regnskapet er adekvate.

A51. Revisors forståelse av enheten og dens omgivelser og det gjeldende rammeverket for finansiell rapportering gir også informasjon om hvordan revisor planlegger og utfører videre revisjonshandlinger, for eksempel når revisor:

- Etablerer forventninger til bruk ved gjennomføring av analytiske handlinger i samsvar med ISA 520;[30]
- Utformer og utfører videre revisjonshandlinger for å innhente tilstrekkelig og hensiktsmessig revisjonsbevis i samsvar med ISA 330; og
- Evaluerer om innhentet revisjonsbevis er tilstrekkelig og hensiktsmessig (for eksempel knyttet til forutsetninger eller ledelsens muntlige og skriftlige uttalelser).

Skalerbarhet

A52. Typen og omfanget av den påkrevde forståelsen er gjenstand for revisors profesjonelle skjønn og varierer fra enhet til enhet basert på typen og omstendighetene ved enheten, herunder:

- Enhetens størrelse og kompleksitet, herunder enhetens IT-miljø;
- Revisors tidligere erfaring med enheten;
- Typen systemer og prosesser i enheten, herunder hvorvidt de er formaliserte eller ikke; og
- Typen og formen på enhetens dokumentasjon.

A53. Revisors risikovurderingshandlinger for å opparbeide seg den påkrevde forståelsen kan være mindre omfattende ved revisjoner av mindre komplekse enheter, og mer omfattende for enheter som er mer komplekse. Dybden av forståelsen som kreves av revisor forventes å være mindre enn den ledelsen har for å lede enheten.

A54. Enkelte rammeverk for finansiell rapportering tillater at mindre enheter gir enklere og mindre detaljerte tilleggsopplysninger i regnskapet. Dette fritar imidlertid ikke revisor for oppgaven med å opparbeide seg en forståelse av enheten og dens omgivelser og hvordan det gjeldende rammeverket for finansiell rapportering skal anvendes på enheten.

A55. Enhetens bruk av IT og typen og omfanget av endringer i IT-miljøet kan også påvirke de spesialiserte ferdighetene som er nødvendige for å kunne opparbeide seg den påkrevde forståelsen.

---

[28] ISA 700 (revidert) *Konklusjon og rapportering om regnskaper* , punkt 13(e)

[29] ISA 320 *Vesentlighet ved planlegging og gjennomføring av en revisjon*, punkt 10–11

[30] ISA 520, punkt 5

Enheten og dens omgivelser (Jf. punkt 19(a))

Enhetens organisasjonsstruktur, eierskap og styring og kontroll, og forretningsmodell (Jf. punkt 19(a)(i))

Enhetens organisasjonsstruktur og eierskap

A56. En forståelse av enhetens organisasjonsstruktur og eierskap kan gjøre revisor i stand til å forstå forhold som for eksempel:

- Kompleksiteten av enhetens struktur.

  Eksempel:

  Enheten kan være et enkelt foretak, eller enhetens struktur kan omfatte datterselskaper, divisjoner eller andre konsernenheter på flere steder. Videre kan den juridiske strukturen være forskjellig fra den operasjonelle strukturen. Komplekse strukturer introduserer ofte faktorer som kan gi økt mulighet for risikoer for vesentlig feilinformasjon. Slike forhold kan blant annet omfatte hvorvidt goodwill, felleskontrollert virksomhet, investeringer eller foretak med avgrenset formål (special-purpose entities) regnskapsføres på en hensiktsmessig måte, og hvorvidt det er gitt adekvate tilleggsopplysninger om slike forhold i regnskapet.

- Eierskapet, og relasjoner mellom eiere og andre personer eller enheter, herunder nærstående parter. Denne forståelsen kan bidra til å fastsette hvorvidt transaksjoner med nærstående parter er tilstrekkelig identifisert og hensyntatt samt opplyst om i regnskapet på en adekvat måte.[31]

- Skillet mellom eierne, de som har overordnet ansvar for styring og kontroll, og ledelsen.

  Eksempel:

  I mindre komplekse enheter kan eiere av enheten være involvert i ledelsen av enheten, og skillet er derfor lite eller ikke-eksisterende. På den annen side, for eksempel i enkelte børsnoterte enheter, kan det være et tydelig skille mellom ledelsen, eierne av enheten og de som har overordnet ansvar for styring og kontroll.[32]

[31] ISA 550 fastsetter krav og gir veiledning til revisors vurderinger knyttet til nærstående parter.

[32] ISA 260 (revidert), punkt A1 og A2, gir veiledning i identifiseringen av dem som har overordnet ansvar for styring og kontroll, og forklarer at i enkelte tilfeller kan noen av eller alle dem som har overordnet ansvar for styring og kontroll, være involvert i ledelsen av enheten.

- Strukturen og kompleksiteten av enhetens IT-miljø.

> **Eksempler**:
>
> En enhet kan:
>
> - Ha flere eldre IT-systemer innenfor ulike virksomhetsområder som ikke er godt integrert, noe som fører til et komplekst IT-miljø.
> - Bruke eksterne eller interne tjenesteleverandører for aspekter ved IT-miljøet (for eksempel utkontraktering av driften av IT-miljøet til en tredjepart eller bruk av et delt servicesenter for sentral styring av IT-prosesser i et konsern).

Automatiserte verktøy og teknikker

A57. Revisor kan bruke automatiserte verktøy og teknikker for å forstå transaksjonsflyt og behandling som en del av revisors handlinger for å forstå informasjonssystemet. Et utfall av disse handlingene kan være at revisor innhenter informasjon om enhetens organisasjonsstruktur eller dem som enheten driver forretninger med (for eksempel leverandører, kunder, nærstående parter).

Særlige hensyn knyttet til enheter i offentlig sektor

A58. Eierskap i en enhet i offentlig sektor har ikke nødvendigvis samme relevans som i privat sektor, ettersom beslutninger knyttet til enheten kan tas utenfor enheten som et resultat av politiske prosesser. Derfor har ikke ledelsen nødvendigvis kontroll over alle beslutningene som tas. Forhold som kan være relevante, omfatter forståelse av evnen som enheten har til å ta unilaterale beslutninger, og evnen som andre enheter i offentlig sektor har til å kontrollere eller øve innflytelse på enhetens mandat og strategiske styring.

> **Eksempel**:
>
> En enhet i offentlig sektor kan være gjenstand for lover eller andre føringer fra myndigheter som krever at parter utenfor enheten godkjenner enhetens strategi og mål før de kan implementeres. Derfor kan forhold knyttet til forståelsen av enhetens juridiske struktur omfatte gjeldende lover og forskrifter, og klassifiseringen av enheten (dvs. hvorvidt enheten er et departement, direktorat eller annen type enhet).

Styring og kontroll

Hvorfor revisor opparbeider seg en forståelse av styring og kontroll

A59. Forståelse av enhetens styring og kontroll kan hjelpe revisor med å forstå enhetens evne til å sørge for tilstrekkelig tilsyn med internkontrollsystemet. Denne forståelsen kan imidlertid også gi bevis på mangler, som kan tyde på økt mulighet for at enhetens regnskap er eksponert for risikoer for vesentlig feilinformasjon.

Forståelse av enhetens styring og kontroll

A60. Forhold som kan være relevante for revisor å vurdere ved opparbeidelsen av en forståelse av enhetens styring og kontroll, omfatter:

- Hvorvidt noen av eller alle dem som har overordnet ansvar for styring og kontroll, inngår i ledelsen av enheten.
- Eksistensen av (og skillet mellom) et ikke-utøvende styre, dersom det er relevant, og utøvende ledelse.
- Hvorvidt de som har overordnet ansvar for styring og kontroll innehar posisjoner som er en integrert del av enhetens juridiske struktur, for eksempel som styremedlemmer.
- Eksistensen av undergrupper av dem som har overordnet ansvar for styring og kontroll, for eksempel et revisjonsutvalg, og en slik gruppes oppgaver og plikter.
- Oppgavene og pliktene til dem som har ansvar for å føre tilsyn med finansiell rapportering, inkludert godkjenning av regnskapet.

Enhetens forretningsmodell

> **Vedlegg 1** inneholder ytterligere vurderinger knyttet til opparbeidelsen av en forståelse av enheten og dens forretningsmodell, så vel som ytterligere vurderinger knyttet til revisjon av foretak med avgrenset formål (special-purpose entities).

Hvorfor revisor opparbeider seg en forståelse av enhetens forretningsmodell

A61. Forståelse av enhetens mål, strategi og forretningsmodell hjelper revisor med å forstå enheten på et strategisk nivå, og hvilke forretningsrisikoer enheten tar og står overfor. En forståelse av forretningsrisikoene som har en virkning på regnskapet, bistår revisor i identifiseringen av risikoer for vesentlig feilinformasjon, ettersom de fleste forretningsrisikoer til slutt vil ha finansielle konsekvenser og dermed en virkning på regnskapet.

Eksempler:

En enhets forretningsmodell kan bygge på bruken av IT på forskjellige måter:

- Enheten selger sko fra en fysisk butikk, og bruker et avansert lager- og salgssystem for å registrere salget av sko; eller
- Enheten selger sko på nettet, slik at alle salgstransaksjoner behandles i et IT-miljø, herunder initiering av transaksjonene gjennom en nettside.

For begge disse enhetene vil forretningsrisikoene som oppstår som følge av en signifikant forskjellig forretningsmodell, være vesentlig forskjellige, selv om begge enhetene selger sko.

Forståelse av enhetens forretningsmodell

A62. Ikke alle aspekter ved forretningsmodellen er relevante for revisors forståelse. Forretningsrisikoer favner videre enn risikoene for vesentlig feilinformasjon i regnskapet, selv om forretningsrisikoer omfatter de sistnevnte. Revisor har ikke en plikt å forstå eller identifisere alle forretningsrisikoer, ettersom ikke alle forretningsrisikoer medfører risikoer for vesentlig feilinformasjon.

A63. Forretningsrisikoer som øker eksponeringen for risikoer for vesentlig feilinformasjon kan oppstå som følge av:

- Uegnede mål eller strategier, ineffektiv gjennomføring av strategier, eller endring eller kompleksitet.
- Manglende evne til å oppfatte behovet for endringer kan også medføre forretningsrisiko, for eksempel som følge av:
  - Utviklingen av nye produkter eller tjenester som kan mislykkes;
  - Et marked som til tross for en vellykket utvikling, ikke egner seg til å understøtte et produkt eller en tjeneste; eller
  - Feil ved et produkt eller en tjeneste som kan føre til erstatningskrav og omdømmerisiko.
- Incentiver og press på ledelsen, som kan føre til tilsiktet eller utilsiktet manglende objektivitet hos ledelsen, og dermed påvirke rimeligheten av viktige forutsetninger og forventningene til ledelsen eller dem som har overordnet ansvar for styring og kontroll.

A64. Eksempler på forhold som revisor kan vurdere ved opparbeidelse av en forståelse av enhetens forretningsmodell, mål, strategier og relaterte forretningsrisikoer som kan medføre risiko for vesentlig feilinformasjon i regnskapet, omfatter:

- Bransjens utvikling, for eksempel mangel på personell eller ekspertise for å håndtere endringene i bransjen;
- Nye produkter og tjenester som kan føre til økt produktansvar;
- Utvidelse av enhetens virksomhet, og etterspørselen ikke er blitt riktig vurdert;

- Nye krav til regnskapsføring, og det har vært ufullstendig eller feilaktig implementering;
- Regulatoriske krav som har ført til økt juridisk eksponering;
- Nåværende og fremtidige krav til finansiering, for eksempel tap av finansiering på grunn av at enheten ikke er i stand til å etterleve krav;
- Bruk av IT, for eksempel implementering av et nytt IT-system som vil påvirke både driftsmessig og finansiell rapportering; eller
- Virkninger av implementering av en strategi, særlig eventuelle virkninger som vil føre til nye krav til regnskapsføring.

A65. Vanligvis identifiserer ledelsen forretningsrisikoer og utarbeider tiltak for å håndtere dem. En slik risikovurderingsprosess er en del av enhetens internkontrollsystem og omtales i punkt 22 og A109–A113.

Særlige hensyn knyttet til enheter i offentlig sektor

A66. Enheter i offentlig sektor kan skape og levere verdi på andre måter enn dem som skaper avkastning for eiere, men vil fortsatt ha en «forretningsmodell» med et bestemt mål. Forhold som er relevante for enhetens forretningsmodell og som revisorer i offentlig sektor kan opparbeide seg en forståelse av, omfatter:

- Kunnskap om relevante myndighetsaktiviteter, herunder relaterte programmer.
- Programmål og -strategier, herunder elementer i offentlig politikk.

A67. Ved revisjon av enheter i offentlig sektor kan «ledelsens mål» være påvirket av krav til offentlig ansvarlighet og kan omfatte mål som skriver seg fra lov, forskrift eller andre autoritative kilder.

Bransjemessige, regulatoriske og andre eksterne faktorer (Jf. punkt 19(a)(ii))

Bransjemessige faktorer

A68. Relevante bransjemessige faktorer omfatter forhold som konkurransesituasjonen, leverandør- og kunderelasjoner og teknologisk utvikling. Forhold som revisor kan vurdere, omfatter:

- Markedet og konkurranseforholdene, herunder etterspørsel, kapasitet og priskonkurranse.
- Periodiske eller sesongavhengige aktiviteter.
- Produktteknologi forbundet med enhetens produkter.
- Energiforsyning og -kostnader.

A69. Bransjen som enheten opererer i, kan medføre særskilte risikoer for vesentlig feilinformasjon som følge av typen virksomhet eller graden av regulering.

Eksempel:

I byggebransjen kan langsiktige kontrakter innebære betydelige estimater av inntekter og kostnader som medfører risikoer for vesentlig feilinformasjon. I slike tilfeller er det viktig at revisjonsteamet har medlemmer med tilstrekkelig relevant kunnskap og erfaring.[33]

Regulatoriske faktorer

A70. Relevante regulatoriske faktorer omfatter det regulatoriske miljøet. Det regulatoriske miljøet omfatter blant annet det gjeldende rammeverket for finansiell rapportering og det juridiske og politiske miljøet, og eventuelle endringer i disse. Forhold som revisor kan vurdere, omfatter:

- Regulatorisk rammeverk for en regulert bransje, for eksempel tilsynskrav, herunder relaterte tilleggsopplysninger.
- Lov og forskrift som vesentlig påvirker enhetens virksomhet, for eksempel lover og forskrifter knyttet til arbeidsforhold.
- Lover og forskrifter knyttet til skattlegging.
- Offentlig politikk som i øyeblikket påvirker enhetens løpende drift, for eksempel pengepolitiske tiltak, herunder valutakontroll, skatt, finansielle incentiver (for eksempel statlig støtte) og toll eller handelshindringer.
- Miljøkrav som påvirker bransjen og enhetens virksomhet.

A71. ISA 250 (revidert) inneholder noen spesifikke krav knyttet til det juridiske og regulatoriske rammeverket som gjelder for enheten og bransjen eller sektoren som enheten driver i.[34]

Særlige hensyn knyttet til enheter i offentlig sektor

A72. Ved revisjon av enheter i offentlig sektor kan det finnes særskilte lover eller forskrifter som påvirker enhetens virksomhet. Slike elementer kan være viktige å vurdere når revisor opparbeider seg en forståelse av enheten og dens omgivelser.

Andre eksterne faktorer

A73. Andre eksterne faktorer som påvirker enheten og som revisor kan vurdere, omfatter den generelle økonomiske situasjonen, rentenivå og tilgjengelig finansiering samt inflasjon og valutarevaluering.

[33] ISA 220, punkt 14

[34] ISA 250 (revidert), punkt 13

Måleparametere benyttet av ledelsen for å vurdere enhetens finansielle resultater (Jf. punkt 19(a)(iii))

Hvorfor revisor opparbeider seg en forståelse av måleparametere benyttet av ledelsen

A74. En forståelse av enhetens måleparametere hjelper revisor med å vurdere hvorvidt slike måleparametere, enten de er benyttet eksternt eller internt, legger press på enheten for å nå resultatmål. Dette presset kan motivere ledelsen til å iverksette tiltak som øker muligheten for feilinformasjon som følge av ledelsens manglende objektivitet eller misligheter (for eksempel ved å forbedre enhetens resultater eller med hensikt gi feilinformasjon i regnskapet) (se ISA 240 for krav og veiledning knyttet til risikoer for misligheter).

A75. Måleparametere kan også gi revisor en indikasjon på sannsynligheten for risikoer for vesentlig feilinformasjon i informasjon tilknyttet regnskapet. Resultatmål kan for eksempel indikere at enheten har en uvanlig rask vekst eller uvanlig høy lønnsomhet sammenlignet med andre enheter i samme bransje.

Måleparametere benyttet av ledelsen

A76. Ledelsen og andre måler og gjennomgår vanligvis de forholdene de anser som viktige. Forespørsler til ledelsen kan avdekke av ledelsen bruker bestemte nøkkelindikatorer, som kan være offentlig tilgjengelige eller ikke, for å evaluere finansielle resultater og iverksette tiltak. I slike tilfeller kan revisor identifisere relevante resultatmål, som kan være interne eller eksterne, for å vurdere informasjonen som enheten bruker til å styre virksomheten. Dersom en slik forespørsel indikerer fravær av resultatmål eller gjennomgåelse, kan det foreligge økt risiko for at feilinformasjon ikke er avdekket og korrigert.

A77. Nøkkelindikatorer som benyttes til å evaluere finansielle resultater, kan omfatte:

- Viktige styringsindikatorer (finansielle og ikke-finansielle) og viktige forholdstall, trender og driftsstatistikker.
- Analyser av periodevise finansielle resultater.
- Budsjetter, prognoser, variasjonsanalyser, segmentinformasjon og resultatrapporter fra divisjoner, avdelinger eller andre nivåer.
- Resultatmål for ansatte og incentivbaserte vederlagsordninger.
- Sammenligninger av en enhets resultater med konkurrentenes.

Skalerbarhet (Jf. punkt 19(a)(iii))

A78. Handlingene som gjennomføres for å forstå enhetens måleparametere kan variere avhengig av enhetens størrelse eller kompleksitet, og i hvilken grad eiere eller de som har overordnet styring og kontroll inngår i ledelsen av enheten.

Eksempler:

- For enkelte mindre komplekse enheter kan vilkårene for enhetens banklån (dvs. lånebetingelser) være koblet til spesifikke måleparametere knyttet til enhetens resultater eller finansielle stilling (for eksempel et maksimumsbeløp for arbeidskapital). Revisors forståelse av resultatmålene som er benyttet av banken, kan bidra til å identifisere områder som har økt mulighet for risiko for vesentlig feilinformasjon.
- For enkelte enheter der typen og omstendighetene er mer komplekse, for eksempel de som driver innenfor forsikrings- eller banksektoren, kan resultater eller finansiell stilling måles mot regulatoriske krav (for eksempel krav som regulerer ansvarlig kapital og likviditetsforhold). Revisors forståelse av disse resultatmålene kan bidra til å identifisere områder som har økt mulighet for risiko for vesentlig feilinformasjon.

Andre forhold som må vurderes

A79. Eksterne parter kan også gjennomgå og analysere enhetens finansielle resultater, særlig for enheter der finansiell informasjon er offentlig tilgjengelig. Revisor kan også vurdere offentlig tilgjengelig informasjon for å skaffe seg en bedre forståelse av virksomheten eller identifisere motstridende informasjon, for eksempel informasjon fra:

- Analytikere eller kredittopplysningsbyråer.
- Nyheter og andre medier, herunder sosiale medier.
- Skattemyndigheter.
- Tilsynsmyndigheter.
- Fagforeninger.
- Tilbydere av finansiering.

Slik finansiell informasjon kan ofte innhentes fra enheten som revideres.

A80. Måling og gjennomgåelse av finansielle resultater er ikke det samme som overvåking av internkontrollsystemet (drøftet som en komponent av internkontrollsystemet i punkt A114–A122), selv om formålene kan overlappe:

- Måling og gjennomgåelse av resultater er rettet mot hvorvidt virksomhetens resultater oppfyller målene fastsatt av ledelsen (eller tredjeparter).
- Overvåking av internkontrollsystemet, derimot, omhandler overvåking av kontrollens effektivitet, herunder dem som er knyttet til ledelsens måling og gjennomgåelse av finansielle resultater.

I noen tilfeller kan imidlertid styringsindikatorer også gi informasjon som gjør det mulig for ledelsen å identifisere kontrollmangler.

Særlige hensyn knyttet til enheter i offentlig sektor

A81. I tillegg til å vurdere relevante måleparametere benyttet av en enhet i offentlig sektor for å vurdere enhetens finansielle resultater, kan revisorer i enheter i offentlig sektor også vurdere ikke-finansiell informasjon, for eksempel oppnåelse av samfunnsnyttige mål (for eksempel antall personer som får bistand gjennom et bestemt program).

Det gjeldende rammeverket for finansiell rapportering (Jf. punkt 19(b))

Forståelse av det gjeldende rammeverket for finansiell rapportering og enhetens regnskapspolicyer

A82. Forhold som revisor kan vurdere ved opparbeidelse av en forståelse av enhetens gjeldende rammeverk for finansiell rapportering, og hvordan det anvendes i kontekst av typen og omstendighetene ved enheten og dens omgivelser, omfatter:

- Enhetens finansielle rapporteringspraksis under det gjeldende rammeverket for finansiell rapportering, for eksempel:
  - Regnskapsprinsipper og bransjespesifikk praksis, herunder for bransjespesifikke signifikante transaksjonsklasser, kontosaldoer og tilhørende tilleggsopplysninger i regnskapet (for eksempel lån og investeringer for banker, eller forskning og utvikling for farmasøytiske enheter).
  - Inntektsføring.
  - Regnskapsføring av finansielle instrumenter, herunder tilhørende kredittap.
  - Eiendeler, forpliktelser og transaksjoner i utenlandsk valuta.
  - Regnskapsføring av uvanlige eller komplekse transaksjoner, herunder transaksjoner på kontroversielle eller nye områder (for eksempel regnskapsføring av kryptovaluta).
- En forståelse av enhetens valg og anvendelse av regnskapspolicyer, herunder eventuelle endringer i dem og årsakene til endringene, kan omfatte forhold som:
  - Metodene enheten bruker til å regnskapsføre, måle, presentere og opplyse om vesentlige og uvanlige transaksjoner.
  - Virkningen av vesentlige regnskapspolicyer på kontroversielle eller nye områder der det mangler autoritativ veiledning eller enighet.
  - Endringer i omgivelsene, for eksempel endringer i det gjeldende rammeverket for finansiell rapportering eller skattereformer som kan medføre en endring i enhetens regnskapspolicyer.
  - Finansielle rapporteringsstandarder og lover og forskrifter som er nye for enheten, og når og hvordan enheten vil tilpasse seg, eller overholde, disse kravene.

A83. Opparbeidelse av en forståelse av enheten og dens omgivelser kan hjelpe revisor med å identifisere hvor endringer i enhetens finansielle rapportering (for eksempel fra foregående perioder) kan forventes.

> **Eksempel**:
>
> Dersom enheten har hatt en foretaksintegrasjon av betydning i perioden, er det sannsynlig at revisor kan forvente endringer i transaksjonsklasser, kontosaldoer og tilleggsopplysninger knyttet til denne foretaksintegrasjonen. Dersom det derimot ikke har vært noen endringer av betydning i rammeverket for finansiell rapportering i perioden, kan revisors forståelse bidra til å bekrefte at forståelsen opparbeidet i foregående periode, fortsatt er gjeldende.

Særlige hensyn knyttet til enheter i offentlig sektor

A84. Det gjeldende rammeverket for finansiell rapportering i en enhet i offentlig sektor er fastsatt av de lovmessige og regulatoriske rammeverkene som er relevante for hver jurisdiksjon eller innenfor hvert geografisk område. Forhold som kan vurderes i forbindelse med enhetens anvendelse av det gjeldende rammeverket for finansiell rapportering, og hvordan det anvendes i kontekst av typen og omstendighetene ved enheten og dens omgivelser, omfatter hvorvidt enheten anvender periodiseringsprinsippet eller kontantprinsippet ved regnskapsførsel i samsvar med de internasjonale regnskapsstandardene for offentlig sektor (IPSAS), eller en hybrid.

Hvordan iboende risikofaktorer påvirker påstanders mulighet for feilinformasjon (Jf. punkt 19(c))

> **Vedlegg 2** inneholder eksempler på hendelser og forhold som kan medføre at det foreligger risikoer for vesentlig feilinformasjon, kategorisert etter iboende risikofaktor.

Hvorfor revisor opparbeider seg en forståelse av iboende risikofaktorer ved forståelse av enheten og dens omgivelser og det gjeldende rammeverket for finansiell rapportering

A85. Forståelse av enheten og dens omgivelser og det gjeldende rammeverket for finansiell rapportering hjelper revisor med å identifisere hendelser eller forhold som har særtrekk som kan påvirke muligheten for at påstander om transaksjonsklasser, kontosaldoer og tilleggsopplysninger inneholder feilinformasjon. Disse særtrekkene er iboende risikofaktorer. Iboende risikofaktorer kan påvirke påstanders mulighet for feilinformasjon ved å virke inn på sannsynligheten for at feilinformasjon forekommer eller omfanget av feilinformasjonen dersom den forekommer. Forståelse av hvordan iboende risikofaktorer påvirker påstanders mulighet for feilinformasjon, kan bidra til å gi revisor en foreløpig forståelse av sannsynligheten for eller omfanget av feilinformasjon, som hjelper revisor med å identifisere risikoer for vesentlig feilinformasjon på påstandsnivå i samsvar med punkt 28(b). Forståelse av i hvilken grad iboende risikofaktorer påvirker påstanders mulighet for feilinformasjon, hjelper også revisor med å vurdere sannsynligheten for og omfanget av mulig feilinformasjon når revisor vurderer iboende risiko i samsvar med punkt 31(a). Forståelse av de iboende risikofaktorene

kan følgelig også hjelpe revisor med å utforme og utføre videre revisjonshandlinger i samsvar med ISA 330.

A86. Revisors identifisering av risikoer for vesentlig feilinformasjon på påstandsnivå og vurdering av iboende risiko kan også være påvirket av revisjonsbevis innhentet av revisor ved gjennomføring av andre risikovurderingshandlinger, videre revisjonshandlinger eller for å oppfylle andre krav i ISA-ene (se punkt A95, A103, A111, A121, A124 og A151).

Virkningen av iboende risikofaktorer på en transaksjonsklasse, kontosaldo eller tilleggsopplysning

A87. I hvilken grad en transaksjonsklasse, kontosaldo eller tilleggsopplysning kan inneholde feilinformasjon som følge av kompleksitet eller subjektivitet, er ofte nært knyttet til i hvilken grad den er gjenstand for endring eller usikkerhet.

> **Eksempel**:
>
> Dersom enheten har et regnskapsestimat som er basert på forutsetninger, og valget av disse er gjenstand for vesentlig skjønn, er det sannsynlig at målingen av regnskapsestimatet er påvirket av både subjektivitet og usikkerhet.

A88. Jo mer en transaksjonsklasse, kontosaldo eller tilleggsopplysning er eksponert for feilinformasjon som følge av kompleksitet eller subjektivitet, desto større er behovet for at revisor utøver profesjonell skepsis. Videre, når en transaksjonsklasse, kontosaldo eller tilleggsopplysning kan inneholde feilinformasjon som følge av kompleksitet, subjektivitet, endring eller usikkerhet, kan disse iboende risikofaktorene skape mulighet for manglende objektivitet hos ledelsen, det være seg utilsiktet eller tilsiktet, og påvirke mulig feilinformasjon som følge av manglende objektivitet hos ledelsen. Revisors identifisering av risikoer for vesentlig feilinformasjon og vurdering av iboende risiko på påstandsnivå er også påvirket av iboende risikofaktorers innbyrdes forhold.

A89. Hendelser eller forhold som kan påvirke mulig feilinformasjon som følge av manglende objektivitet hos ledelsen, kan også påvirke mulig feilinformasjon som følge av andre mislighetsrisikofaktorer. Dette kan følgelig være relevant informasjon for bruk i samsvar med punkt 24 i ISA 240, som krever at revisor evaluerer hvorvidt informasjonen innhentet gjennom de andre risikovurderingshandlingene og relaterte aktivitetene tyder på at det foreligger en eller flere mislighetsrisikofaktorer.

Opparbeidelse av en forståelse av enhetens internkontrollsystem (Jf. punkt 21–27)

> **Vedlegg 3** gir en mer detaljert beskrivelse av henholdsvis typen internkontrollsystem og iboende begrensninger ved intern kontroll. Vedlegg 3 gir også en mer detaljert forklaring på komponentene i et internkontrollsystem innenfor ISA-enes formål.

A90. Revisors forståelse av enhetens internkontrollsystem innhentes gjennom risikovurderingshandlinger som utføres for å forstå og evaluere hver av komponentene i internkontrollsystemet, som fastsatt i punkt 21 til 27.

A91. Komponentene i enhetens internkontrollsystem innenfor denne ISA-ens formål, gjenspeiler ikke nødvendigvis måten en enhet utformer, implementerer og vedlikeholder sitt internkontrollsystem på, eller måten enheten klassifiserer de ulike komponentene på. Enheter kan bruke forskjellige terminologier eller rammeverk for å beskrive de ulike aspektene ved internkontrollsystemet. Innenfor rammen av en revisjon kan også revisorer bruke forskjellige terminologier eller rammeverk, forutsatt at alle komponentene som er beskrevet i denne ISA-en, tas med.

Skalerbarhet

A92. Måten enhetens internkontrollsystem utformes, implementeres og vedlikeholdes på varierer med enhetens størrelse og kompleksitet. Mindre komplekse enheter kan for eksempel bruke mindre strukturerte eller enklere kontroller (dvs. retningslinjer og rutiner) for å oppfylle sine mål.

Særlige hensyn knyttet til enheter i offentlig sektor

A93. Revisorer i enheter i offentlig sektor har ofte ytterligere oppgaver og plikter med hensyn til den interne kontrollen, for eksempel å rapportere om overholdelse av kodifisert «god skikk» eller rapportering av utgifter i forhold til budsjett. Revisorer i enheter i offentlig sektor kan også være forpliktet til å rapportere om overholdelse av lov, forskrift eller krav fra andre autoritative kilder. Deres vurderinger av internkontrollsystemet kan følgelig være videre og mer detaljerte.

Informasjonsteknologi i komponentene i enhetens internkontrollsystem

> **Vedlegg 5** gir ytterligere veiledning knyttet til forståelsen av enhetens bruk av IT i komponentene i internkontrollsystemet.

A94. Det overordnede målet og innholdet i en revisjon skiller ikke mellom hvorvidt en enhet opererer i et hovedsakelig manuelt miljø, et fullstendig automatisert miljø eller et miljø som består av en kombinasjon av manuelle og automatiserte elementer (dvs. manuelle og automatiserte kontroller og andre ressurser som benyttes i enhetens internkontrollsystem).

Forståelse av typen komponenter i enhetens internkontrollsystem

A95. Ved evaluering av effektiviteten av utformingen av kontroller og hvorvidt de er implementert (se punkt A175 til A181), gir revisors forståelse av hver av komponentene i enhetens internkontrollsystem en foreløpig forståelse av hvordan enheten identifiserer forretningsrisikoer og hvordan den håndterer dem. Den kan også virke inn på revisors identifisering og vurdering av risikoene for vesentlig feilinformasjon på forskjellige måter (se punkt A86). Dette hjelper revisor med å utforme og utføre videre revisjonshandlinger, herunder eventuelle planer om å teste om kontroller fungerer effektivt. For eksempel:

- Revisors forståelse av komponentene «kontrollmiljø», «risikovurderingsprosess» og «prosess for overvåking av kontroller» i enheten, vil ofte påvirke identifiseringen og vurderingen av risikoer for vesentlig feilinformasjon på regnskapsnivå.

- Revisors forståelse av komponentene «informasjonssystem og kommunikasjon» og «kontrollaktiviteter» i enheten, vil ofte påvirke identifiseringen og vurderingen av risikoer for vesentlig feilinformasjon på påstandsnivå.

Kontrollmiljø, enhetens risikovurderingsprosess og enhetens prosess for overvåking av internkontrollsystemet (Jf. punkt 21–24)

A96. Kontrollene i kontrollmiljøet, enhetens risikovurderingsprosess og enhetens prosess for overvåking av internkontrollsystemet er primært indirekte kontroller (dvs. kontroller som ikke er tilstrekkelig presise til å forebygge, avdekke eller korrigere feilinformasjon på påstandsnivå, men som kan underbygge andre kontroller og derfor ha en indirekte virkning på sannsynligheten for at feilinformasjon vil bli avdekket eller forebygget i rett tid). Enkelte kontroller innenfor disse komponentene kan imidlertid også være direkte kontroller.

Hvorfor det kreves at revisor forstår kontrollmiljøet, enhetens risikovurderingsprosess og enhetens prosess for overvåking av internkontrollsystemet

A97. Kontrollmiljøet gir et overordnet grunnlag for driften av de andre komponentene i internkontrollsystemet. Kontrollmiljøet verken forebygger, eller avdekker og korrigerer, feilinformasjon direkte. Det kan midlertid virke inn på kontrollens effektivitet i de andre komponentene i internkontrollsystemet. Likeledes er enhetens risikovurderingsprosess og enhetens prosess for overvåking av internkontrollsystemet utformet for å fungere på en måte som også underbygger hele internkontrollsystemet.

A98. Fordi disse komponentene er grunnleggende for enhetens internkontrollsystem, kan eventuelle mangler i driften av dem ha gjennomgripende virkninger på utarbeidelsen av regnskapet. Derfor påvirker revisors forståelse og evaluering av disse komponentene revisors identifisering og vurdering av risikoer for vesentlig feilinformasjon på regnskapsnivå, og kan også påvirke identifiseringen og vurderingen av risikoer for vesentlig feilinformasjon på påstandsnivå. Risikoer for vesentlig feilinformasjon på regnskapsnivå påvirker revisors utforming av overordnede handlinger, og har blant annet, som forklart i ISA 330, en innvirkning på typen, tidspunktet og omfanget av revisors videre handlinger.[35]

Opparbeidelse av en forståelse av kontrollmiljøet (Jf. punkt 21)

Skalerbarhet

A99. Typen kontrollmiljø i en mindre kompleks enhet er ofte forskjellig fra kontrollmiljøet i en mer kompleks enhet. Det kan for eksempel være at de som har overordnet ansvar for styring og kontroll i mindre komplekse enheter ikke har et uavhengig eller eksternt medlem, og at styrings- og kontrollrollen utøves direkte av eier-leder når det ikke finnes andre eiere. Følgelig kan enkelte vurderinger knyttet til enhetens kontrollmiljø være mindre relevante, eller ikke aktuelle i det hele tatt.

[35] ISA 330, punkt A1–A3

A100. I tillegg er det ikke alltid at revisjonsbevis for elementer i kontrollmiljøet i mindre komplekse enheter er tilgjengelige i dokumentform, særlig når kommunikasjonen mellom ledelsen og annet personell er uformell, men beviset kan fortsatt være tilstrekkelig relevant og pålitelig ut fra omstendighetene.

Eksempler:

- Organisasjonsstrukturen i en mindre kompleks enhet vil ofte være enklere, og det kan være få personell i funksjonen knyttet til finansiell rapportering.
- Dersom styrings- og kontrollrollen utøves direkte av eier-leder, kan revisor fastsette at uavhengigheten til dem som har overordnet ansvar for styring og kontroll, ikke er relevant.
- Det kan for eksempel være at mindre komplekse enheter ikke har noen skriftlige etiske regler, men i stedet utvikler en kultur som vektlegger viktigheten av integritet og etisk atferd gjennom muntlig kommunikasjon og ved at ledelsen går foran med et godt eksempel. Holdningene, bevisstheten og handlingene til ledelsen eller eier-leder er dermed av særlig betydning for revisors forståelse av kontrollmiljøet i en mindre kompleks enhet.

Forståelse av kontrollmiljøet (Jf. punkt 21(a))

A101. Revisjonsbevis for revisors forståelse av kontrollmiljøet kan innhentes gjennom en kombinasjon av forespørsler og andre risikovurderingshandlinger (dvs. bekreftende forespørsler gjennom observasjon eller inspeksjon av dokumenter).

A102. Ved vurdering av i hvilken grad ledelsen viser at den håndhever integritet og etiske verdier, kan revisor opparbeide seg en forståelse ved å rette forespørsler til ledelsen og ansatte, og ved å vurdere informasjon fra eksterne kilder, om:

- Hvordan ledelsen kommuniserer sitt syn på forretningspraksis og etisk atferd til ansatte; og ved å
- Inspisere ledelsens skriftlige etiske regler og observere hvorvidt ledelsen opptrer på en måte som underbygger disse reglene.

Evaluering av kontrollmiljøet (Jf. punkt 21(b))

Hvorfor revisor evaluerer kontrollmiljøet

A103. Revisors evaluering av hvordan enheten opptrer i samsvar med enhetens håndhevelse av integritet og etiske verdier, hvorvidt kontrollmiljøet gir et hensiktsmessig grunnlag for de andre komponentene i enhetens internkontrollsystem, og hvorvidt eventuelle identifiserte kontrollmangler undergraver de andre komponentene i internkontrollsystemet, hjelper revisor med å identifisere potensielle problemer i de andre komponentene i internkontrollsystemet. Dette er fordi kontrollmiljøet er grunnleggende for de andre komponentene i enhetens internkontrollsystem. Denne evalueringen kan også hjelpe revisor med å forstå risikoer som enheten står overfor, og dermed med å identifisere og anslå risikoene for vesentlig feilinformasjon på regnskaps- og påstandsnivå (se punkt A86).

Revisors evaluering av kontrollmiljøet

A104. Revisors evaluering av kontrollmiljøet bygger på forståelsen opparbeidet i samsvar med punkt 21(a).

A105. Enkelte enheter kan være dominert av en enkeltperson som kan utøve en god del skjønn. Handlingene og holdningene til denne personen kan ha en gjennomgripende virkning på kulturen i enheten, noe som igjen kan ha en gjennomgripende virkning på kontrollmiljøet. En slik virkning kan være positiv eller negativ.

> **Eksempel**:
>
> Direkte deltakelse av en enkeltperson kan være avgjørende for at enheten oppfyller sine vekstmål eller andre mål, og kan også i betydelig grad bidra til et effektivt internkontrollsystem. På den annen side kan slik konsentrasjon av kunnskap og autoritet også føre til økt mulig feilinformasjon som følge av ledelsens overstyring av kontroller.

A106. Revisor kan vurdere hvordan de ulike elementene i kontrollmiljøet kan være påvirket av filosofien og lederstilen til den øverste ledelsen, herunder om de som har overordnet ansvar for styring og kontroll har uavhengige medlemmer.

A107. Selv om kontrollmiljøet kan gi et hensiktsmessig grunnlag for internkontrollsystemet og kan bidra til å redusere risikoen for misligheter, er ikke et hensiktsmessig kontrollmiljø nødvendigvis en effektiv garanti mot misligheter.

> **Eksempel**:
>
> Personalpolitiske retningslinjer og rutiner rettet mot ansettelse av kompetente personell innenfor finans, regnskap og IT, kan motvirke risikoen for feil ved behandling og registrering av finansiell informasjon. Slike retningslinjer og rutiner vil imidlertid ikke nødvendigvis motvirke den øverste ledelsens overstyring av kontroller (for eksempel med hensyn til overrapportering av inntekter).

A108. Revisors evaluering av kontrollmiljøet knyttet til enhetens bruk av IT kan omfatte forhold som for eksempel:

- Hvorvidt styring og kontroll knyttet til IT står i forhold til enhetens type og kompleksitet, og forretningsoperasjonene som er muliggjort gjennom IT, herunder kompleksiteten eller modenheten til enhetens teknologiske plattform eller arkitektur og i hvilket omfang enheten bruker IT-applikasjoner for å støtte finansiell rapportering.
- Ledelsens organisasjonsstruktur knyttet til IT og ressursene som er tildelt (for eksempel hvorvidt enheten har investert i et hensiktsmessig IT-miljø og nødvendige forbedringer, eller hvorvidt det er ansatt et tilstrekkelig antall personer med de nødvendige ferdighetene, herunder når enheten bruker kommersiell programvare (med ingen eller begrensede modifikasjoner)).

Opparbeidelse av en forståelse av enhetens risikovurderingsprosess (Jf. punkt 22–23)

Forståelse av enhetens risikovurderingsprosess (Jf. punkt 22(a))

A109. Som forklart i punkt A62, er det ikke alle forretningsrisikoer som medfører risikoer for vesentlig feilinformasjon. For å forstå hvordan ledelsen og de som har overordnet ansvar for styring og kontroll har identifisert forretningsrisikoer som er relevante for utarbeidelsen av regnskapet, og besluttet hvilke tiltak som skal håndtere disse risikoene, kan revisor blant annet vurdere hvordan ledelsen eller, der det er relevant, de som har overordnet ansvar for styring og kontroll, har:

- Spesifisert enhetens mål med tilstrekkelig nøyaktighet og tydelighet til at det er mulig å identifisere og anslå risikoene knyttet til målene;
- Identifisert risikoene knyttet til oppnåelsen av enhetens mål, og analysert risikoene som grunnlag for fastsettelse av hvordan risikoene skal håndteres; og
- Vurdert potensialet for misligheter i forbindelse med vurderingen av risikoene knyttet til oppnåelsen av enhetens mål.[36]

A110. Revisor kan vurdere innvirkningen av slike forretningsrisikoer på utarbeidelsen av enhetens regnskap og andre aspekter ved enhetens internkontrollsystem.

Evaluering av enhetens risikovurderingsprosess (Jf. punkt 22(b))

Hvorfor revisor evaluerer hvorvidt enhetens risikovurderingsprosess er hensiktsmessig

A111. Revisors evaluering av enhetens risikovurderingsprosess kan hjelpe revisor med å forstå hvor enheten har identifisert risikoer som kan foreligge, og hvordan enheten har håndtert disse risikoene. Revisors evaluering av hvordan enheten identifiserer sine forretningsrisikoer, og hvordan den vurderer og håndterer disse risikoene, hjelper revisor med å forstå hvorvidt risikoene som enheten står overfor er blitt identifisert, vurdert og håndtert på en hensiktsmessig måte ut fra enhetens type og kompleksitet. Denne evalueringen kan også hjelpe revisor med å identifisere og anslå risikoer for vesentlig feilinformasjon på regnskaps- og påstandsnivå (se punkt A86).

Evaluering av hvorvidt enhetens risikovurderingsprosess er hensiktsmessig (Jf. punkt 22(b))

A112. Revisors evaluering av hvorvidt enhetens risikovurderingsprosess er hensiktsmessig, bygger på forståelsen opparbeidet i samsvar med punkt 22(a).

Skalerbarhet

A113. Hvorvidt enhetens risikovurderingsprosess er hensiktsmessig ut fra enhetens omstendigheter tatt i betraktning enhetens type og kompleksitet, er gjenstand for revisors profesjonelle skjønn.

[36] ISA 240, punkt 19

> **Eksempel**:
>
> I enkelte mindre komplekse enheter, og særlig i enheter som ledes av eier, kan en hensiktsmessig risikovurdering utføres gjennom direkte deltakelse av ledelsen eller eier (for eksempel kan daglig leder eller eier-leder rutinemessig bruke tid på å overvåke aktivitetene til konkurrenter og andre utviklinger i markedet for å identifisere nye forretningsrisikoer). Beviset for at denne risikovurderingen forekommer i denne typen enheter er ofte ikke formelt dokumentert, men det kan fremkomme av diskusjonene som revisor har med ledelsen at ledelsen faktisk utfører risikovurderingshandlinger.

Opparbeidelse av en forståelse av enhetens prosess for overvåking av enhetens internkontrollsystem (Jf. punkt 24)

Skalerbarhet

A114. I mindre komplekse enheter, og særlig i enheter som ledes av eier, er revisors forståelse av enhetens prosess for overvåking av internkontrollsystemet ofte fokusert på hvordan ledelsen eller eier-leder deltar direkte i driften, ettersom det ikke nødvendigvis finnes andre overvåkingsaktiviteter.

> **Eksempel**:
>
> Ledelsen kan motta klager fra kunder på unøyaktigheter i den månedlige kontooversikten, noe som varsler eier-leder om at det er problemer med tidspunktet for regnskapsføring av kundebetalinger.

A115. For enheter som ikke har en formell prosess for overvåking av internkontrollsystemet, kan en forståelse av prosessen for overvåking av internkontrollsystemet inkludere en forståelse av periodiske gjennomgåelser av ledelsens regnskapsinformasjon som er utarbeidet for å bidra til at enheten forebygger eller avdekker feilinformasjon.

Forståelse av enhetens prosess for overvåking av internkontrollsystemet (Jf. punkt 24(a))

A116. Forhold som kan være relevante for revisor å vurdere ved opparbeidelsen av en forståelse av hvordan enheten overvåker internkontrollsystemet, omfatter:

- Utformingen av overvåkingsaktivitetene, for eksempel hvorvidt det er periodisk eller løpende overvåking;
- Gjennomføringen og hyppigheten av overvåkingsaktivitetene;
- Evalueringen av resultatene av overvåkingsaktivitetene, i rett tid, for å fastsette hvorvidt kontrollene har vært effektive; og
- Hvordan identifiserte mangler er blitt håndtert gjennom hensiktsmessige utbedrende tiltak, herunder rettidig kommunikasjon av slike mangler til dem som er ansvarlige for å iverksette utbedrende tiltak.

A117. Revisor kan også vurdere hvordan enhetens prosess for overvåking av internkontrollsystemet håndterer overvåking av informasjonsbehandlingskontroller som innebærer bruk av IT. Dette kan for eksempel være:

- Kontroller for å overvåke komplekse IT-miljøer som:
  - Evaluerer den løpende effektiviteten av utformingen av informasjonsbehandlingskontroller og modifiserer dem, etter behov, slik at de tilpasses endrede forhold; eller
  - Evaluerer om informasjonsbehandlingskontroller fungerer effektivt.
- Kontroller som overvåker tillatelsene som benyttes i automatiserte informasjonsbehandlingskontroller for å håndheve arbeidsdelingen.
- Kontroller som overvåker hvordan feil eller kontrollmangler knyttet til automatiseringen av finansiell rapportering blir identifisert og håndtert.

Forståelse av enhetens internrevisjonsfunksjon (Jf. punkt 24(a)(ii))

> **Vedlegg 4** inneholder ytterligere vurderinger knyttet til forståelsen av enhetens internrevisjonsfunksjon.

A118. Revisors forespørsler til relevante personer i internrevisjonsfunksjonen hjelper revisor med å opparbeide seg en forståelse av internrevisjonsfunksjonens oppgaver og plikter. Dersom revisor fastslår at funksjonens oppgaver og plikter er knyttet til enhetens finansielle rapportering, kan revisor opparbeide seg en dypere forståelse av aktivitetene som er utført, eller som skal utføres, av internrevisjonsfunksjonen ved å gjennomgå internrevisjonsfunksjonens revisjonsplan for perioden, dersom en slik foreligger, og diskutere denne planen med relevante personer i funksjonen. Denne forståelsen, sammen med informasjonen innhentet gjennom revisors forespørsler, kan også gi informasjon som er direkte relevant for revisors identifisering og vurdering av risikoene for vesentlig feilinformasjon. Dersom revisor basert på sin foreløpige forståelse av internrevisjonsfunksjonen, forventer å bruke arbeidet til internrevisjonsfunksjonen for å endre typen eller tidspunktet for, eller redusere omfanget av, revisjonshandlinger som skal utføres, gjelder ISA 610 (revidert 2013)[37].

Andre informasjonskilder som er benyttet i enhetens prosess for overvåking av internkontrollsystemet

Forståelse av informasjonskilder (Jf. punkt 24(b))

A119. Ledelsens overvåkingsaktiviteter kan bruke informasjon i kommunikasjoner fra eksterne parter, for eksempel klager fra kunder eller kommentarer fra tilsynsmyndigheter, som kan indikere problemer eller synliggjøre områder der det er behov for forbedring.

[37] ISA 610 (revidert 2013) *Bruk av interne revisorers arbeid*

Hvorfor det kreves at revisor forstår informasjonskildene som er benyttet i enhetens overvåking av internkontrollsystemet

A120. Revisors forståelse av informasjonskildene som er benyttet av enheten i overvåkingen av enhetens internkontrollsystem, herunder hvorvidt informasjonen som er benyttet er relevant og pålitelig, hjelper revisor med å evaluere hvorvidt enhetens prosess for overvåking av internkontrollsystemet er hensiktsmessig. Dersom ledelsen forutsetter at informasjon som er benyttet til overvåking er relevant og pålitelig uten å ha grunnlag for denne forutsetningen, kan eventuelle feil i informasjonen potensielt føre til at ledelsen trekker feil konklusjoner basert på sine overvåkingsaktiviteter.

Evaluering av enhetens prosess for overvåking av internkontrollsystemet (Jf. Para 24(c))

Hvorfor revisor evaluerer hvorvidt enhetens prosess for overvåking av internkontrollsystemet er hensiktsmessig

A121. Revisors evaluering av hvordan enheten gjennomfører løpende og separate evalueringer for å overvåke kontrollens effektivitet, hjelper revisor med å forstå hvorvidt de andre komponentene i enhetens internkontrollsystem er til stede og fungerer, og bidrar derfor til en forståelse av de andre komponentene i enhetens internkontrollsystem. Denne evalueringen kan også hjelpe revisor med å identifisere og anslå risikoer for vesentlig feilinformasjon på regnskaps- og påstandsnivå (se punkt A86).

Evaluering av hvorvidt enhetens prosess for overvåking av internkontrollsystemet er hensiktsmessig (Jf. punkt 24(c))

A122. Revisors evaluering av hvorvidt enhetens prosess for overvåking av enhetens internkontrollsystem er hensiktsmessig, bygger på revisors forståelse av enhetens prosess for overvåking av internkontrollsystemet.

Informasjonssystem og kommunikasjon, og kontrollaktiviteter (Jf. punkt 25–26)

A123. Kontrollene i komponentene «informasjonssystem og kommunikasjon» og «kontrollaktiviteter» er primært direkte kontroller (dvs. kontroller som er tilstrekkelig presise til å forebygge, avdekke eller korrigere feilinformasjon på påstandsnivå).

Hvorfor det kreves at revisor forstår informasjonssystemet og kommunikasjonen, og kontroller i komponenten «kontrollaktiviteter»

A124. Det kreves at revisor forstår enhetens informasjonssystem og kommunikasjon fordi forståelsen av enhetens retningslinjer som definerer transaksjonsflyten og andre aspekter ved enhetens informasjonsbehandlingsaktiviteter som er relevante for utarbeidelsen av regnskapet, og evalueringen av hvorvidt komponenten på en hensiktsmessig måte underbygger utarbeidelsen av enhetens regnskap, underbygger revisors identifisering og vurdering av risikoer for vesentlig feilinformasjon på påstandsnivå. Denne forståelsen og evalueringen kan også resultere i identifiseringen av risikoer for vesentlig feilinformasjon på regnskapsnivå når resultatene av revisors handlinger ikke stemmer overens med forventninger til enhetens internkontrollsystem, som kan ha

blitt etablert basert på informasjon innhentet under vurderingen av om revisor skal påta seg eller fortsette oppdraget (se punkt A86).

A125. Det kreves at revisor identifiserer særskilte kontroller i komponenten «kontrollaktiviteter», og evaluerer utformingen og fastsetter hvorvidt kontrollene er implementert, ettersom det hjelper revisor med å forstå ledelsens tilnærming til håndteringen av visse risikoer og dermed gir grunnlag for utformingen og gjennomføringen av videre revisjonshandlinger som er tilpasset disse risikoene, som pålagt av ISA 330. Jo høyere en risiko vurderes på spekteret av iboende risiko, desto mer overbevisende må revisjonsbeviset være. Også når revisor ikke planlegger å teste om identifiserte kontroller fungerer effektivt, kan revisors forståelse fortsatt påvirke utformingen av typen, tidspunktet og omfanget av substanshandlinger som er tilpasset de relaterte risikoene for vesentlig feilinformasjon.

Det gjentakende aspektet ved revisors forståelse og evaluering av informasjonssystemet og kommunikasjonen, og kontrollaktiviteter

A126. Som forklart i punkt A49, kan revisors forståelse av enheten og dens omgivelser, og det gjeldende rammeverket for finansiell rapportering, hjelpe revisor med å etablere innledende forventninger til hvilke transaksjonsklasser, kontosaldoer og tilleggsopplysninger som kan være signifikante transaksjonsklasser, kontosaldoer og tilleggsopplysninger. Ved å opparbeide seg en forståelse av komponenten «informasjonssystem og kommunikasjon» i samsvar med punkt 25(a), kan revisor bruke disse innledende forventningene til å fastsette omfanget av forståelsen av enhetens informasjonsbehandlingsaktiviteter som skal opparbeides.

A127. Revisors forståelse av informasjonssystemet omfatter en forståelse av retningslinjene som definerer informasjonsflyten knyttet til enhetens signifikante transaksjonsklasser, kontosaldoer og tilleggsopplysninger, og andre relaterte aspekter ved enhetens informasjonsbehandlingsaktiviteter. Denne informasjonen, og informasjonen innhentet gjennom revisors evaluering av informasjonssystemet, kan bekrefte eller ytterligere virke inn på revisors forventninger til de signifikante transaksjonsklassene, kontosaldoene og tilleggsopplysningene som ble identifisert innledningsvis (se punkt A126).

A128. Ved å opparbeide seg en forståelse av hvordan informasjon knyttet til signifikante transaksjonsklasser, kontosaldoer og tilleggsopplysninger føres inn i, beveger seg gjennom og føres ut av enhetens informasjonssystem, kan revisor også identifisere kontroller i komponenten «kontrollaktiviteter» som kreves identifisert i samsvar med punkt 26(a). Revisors identifisering og evaluering av kontroller i komponenten «kontrollaktiviteter» kan i første omgang være fokusert på kontroller knyttet til posteringer, og kontroller som revisor planlegger å teste om fungerer effektivt ved utforming av typen, tidspunktet og omfanget av substanshandlinger.

A129. Revisors vurdering av iboende risiko kan også virke inn på identifiseringen av kontroller i komponenten «kontrollaktiviteter». Det kan for eksempel være at revisors identifisering av kontroller knyttet til særskilte risikoer bare lar seg gjøre når revisor har vurdert iboende risiko på påstandsnivå i samsvar med punkt 31. Videre kan det være at kontroller som håndterer risikoer der revisor har

vurdert at substanshandlinger alene ikke gir tilstrekkelig og hensiktsmessig revisjonsbevis (i samsvar med punkt 33), også bare kan identifiseres når revisors iboende risikovurderinger er gjennomført.

A130. Revisors identifisering og vurdering av risikoer for vesentlig feilinformasjon på påstandsnivå påvirkes både av revisors:

- Forståelse av enhetens retningslinjer for informasjonsbehandlingsaktiviteter i komponenten «informasjonssystem og kommunikasjon», og
- Identifisering og evaluering av kontroller i komponenten «kontrollaktiviteter».

Opparbeidelse av en forståelse av informasjonssystemet og kommunikasjonen (Jf. punkt 25)

> **Vedlegg 3**, punkt 15–19, inneholder ytterligere vurderinger knyttet til forståelsen av informasjonssystemet og kommunikasjonen.

Skalerbarhet

A131. Informasjonssystemet og tilknyttede forretningsprosesser i mindre komplekse enheter er ofte mindre avanserte enn i større enheter, og involverer ofte et mindre komplekst IT-miljø. Informasjonssystemets rolle er imidlertid like viktig. Mindre komplekse enheter der ledelsen deltar direkte i den daglige driften, har ikke nødvendigvis behov for omfattende beskrivelser av regnskapsrutiner, avanserte regnskapsposter eller skriftlige retningslinjer. Forståelsen av de relevante aspektene ved enhetens informasjonssystem kan derfor være mindre ressurskrevende ved revisjon av en mindre kompleks enhet, og kan innebære en større grad av forespørsler enn observasjon eller inspeksjon av dokumentasjon. Behovet for å opparbeide seg en forståelse er imidlertid fortsatt viktig for å gi et grunnlag for utformingen av videre revisjonshandlinger i samsvar med ISA 330, og kan videre hjelpe revisor med å identifisere eller anslå risikoer for vesentlig feilinformasjon (se punkt A86).

Opparbeidelse av en forståelse av informasjonssystemet (Jf. punkt 25(a))

A132. Enhetens internkontrollsystem omfatter aspekter som er knyttet til enhetens rapporteringsmål, herunder enhetens mål for finansiell rapportering, men kan også omfatte aspekter som er knyttet til enhetens mål for drift eller overholdelse av lover og forskrifter, når slike aspekter er relevante for finansiell rapportering. Forståelsen av hvordan enheten initierer transaksjoner og fanger opp informasjon som en del av revisors forståelse av informasjonssystemet, kan omfatte informasjon om enhetens systemer (retningslinjer) som er utformet for å håndtere mål for overholdelse og drift, fordi slik informasjon er relevant for utarbeidelsen av regnskapet. Videre kan enkelte enheter ha svært integrerte informasjonssystemer, slik at kontroller kan være utformet på en måte som bidrar til samtidig oppnåelse av mål for finansiell rapportering, overholdelse og drift, eller kombinasjoner av disse.

A133. Forståelsen av enhetens informasjonssystem omfatter også en forståelse av ressursene som skal benyttes i enhetens informasjonsbehandlingsaktiviteter. Informasjon om de menneskelige

ressursene som er involvert, som kan være relevant for å forstå risikoer knyttet til informasjonssystemets integritet, omfatter:

- Kompetansen til personene som gjennomfører arbeidet;
- Hvorvidt ressursene er adekvate; og
- Hvorvidt det er en hensiktsmessig arbeidsdeling.

A134. Forhold som revisor kan vurdere ved opparbeidelsen av en forståelse av retningslinjene som definerer informasjonsflyten knyttet til enhetens signifikante transaksjonsklasser, kontosaldoer og tilleggsopplysninger i komponenten «informasjonssystem og kommunikasjon», omfatter typen:

(a) Data eller informasjon knyttet til transaksjoner, andre hendelser og forhold som skal behandles;

(b) Informasjonsbehandling for å opprettholde integriteten til dataene eller informasjonen; og

(c) Porosesser for behandling, menneskelige og andre ressurser som er benyttet i informasjonsbehandlingsprosessen.

A135. Opparbeidelse av en forståelse av enhetens forretningsprosesser, som omfatter hvordan transaksjonene oppstår, hjelper revisor med å opparbeide seg en forståelse av enhetens informasjonssystem på en måte som er hensiktsmessig ut fra enhetens omgivelser.

A136. Revisors forståelse av informasjonssystemet kan opparbeides på forskjellige måter, og kan omfatte:

- Forespørsler til relevante personell om rutinene som benyttes til å initiere, registrere, behandle og rapportere transaksjoner, eller om enhetens finansielle rapporteringsprosess;
- Inspeksjon av håndbøker med retningslinjer eller prosesser, eller annen dokumentasjon av enhetens informasjonssystem;
- Observasjon av de ansattes praktisering av retningslinjene eller rutinene; eller
- Utvelgelse av transaksjoner og sporing av dem gjennom den relevante prosessen i informasjonssystemet (dvs. gjennomføring av en vugge-til-grav-test).

Automatiserte verktøy og teknikker

A137. Revisor kan også bruke automatiserte teknikker for å få direkte tilgang til, eller en digital nedlasting fra, databasene i enhetens informasjonssystem som lagrer regnskapsførte transaksjoner. Ved å anvende automatiserte verktøy eller teknikker på denne informasjonen kan revisor bekrefte den opparbeidede forståelsen av hvordan transaksjoner beveger seg gjennom informasjonssystemet ved å spore posteringer, eller andre digitale poster knyttet til en bestemt transaksjon, eller en hel populasjon av transaksjoner, fra initiering i regnskapssystemet til og med registrering i hovedboken. Analyse av fullstendige eller store sett med transaksjoner kan også føre til identifisering av avvik fra de normale, eller forventede, behandlingsrutinene for disse transaksjonene, noe som kan føre til identifisering av risikoer for vesentlig feilinformasjon.

Informasjon som er innhentet fra andre kilder enn hovedboken og underliggende spesifikasjoner

A138. Regnskap kan inneholde informasjon som er innhentet fra andre kilder enn hovedboken og underliggende spesifikasjoner. Eksempler på slik informasjon som revisor kan vurdere, omfatter:

- Informasjon innhentet fra leasingavtaler som er relevante for tilleggsopplysninger i regnskapet.
- Informasjon gitt i regnskapet som er produsert av en enhets risikostyringssystem.
- Informasjon om virkelig verdi som er produsert av ledelsens eksperter og opplyst om i regnskapet.
- Informasjon gitt i regnskapet som er innhentet fra modeller eller fra andre beregninger som er benyttet til å utarbeide regnskapsestimater som er innregnet eller opplyst om i regnskapet, herunder informasjon knyttet til underliggende data og forutsetninger som er benyttet i disse modellene, for eksempel:
    - Forutsetninger utviklet internt som kan påvirke en eiendels levetid; eller
    - Data som for eksempel rentesatser, som er påvirket av faktorer som ligger utenfor enhetens kontroll.
- Informasjon gitt i regnskapet om sensitivitetsanalyser avledet fra finansielle modeller, som viser at ledelsen har vurdert alternative forutsetninger.
- Informasjon innregnet eller opplyst om i regnskapet, som er hentet fra en enhets skattemelding og skattemessige registreringer.
- Informasjon gitt i regnskapet som er hentet fra analyser utarbeidet for å underbygge ledelsens vurdering av enhetens evne til fortsatt drift, for eksempel eventuelle tilleggsopplysninger knyttet til hendelser eller forhold som er blitt identifisert og som kan skape tvil av betydning om enhetens evne til fortsatt drift.[38]

A139. Visse beløp eller tilleggsopplysninger i enhetens regnskap (for eksempel tilleggsopplysninger om kredittrisiko, likviditetsrisiko og markedsrisiko) kan bygge på informasjon innhentet fra enhetens risikostyringssystem. Revisor er imidlertid ikke pålagt å forstå alle aspekter ved risikostyringssystemet, og utøver profesjonelt skjønn for å fastsette hva som er en tilstrekkelig forståelse.

Enhetens bruk av informasjonsteknologi i informasjonssystemet

Hvorfor revisor skal forstå IT-miljøet som er relevant for informasjonssystemet

A140. Revisors forståelse av informasjonssystemet omfatter IT-miljøet som er relevant for transaksjonsflyten og prosessering av informasjon, fordi enhetens bruk av IT-applikasjoner eller andre aspekter ved IT-miljøet kan medføre risikoer som følger av bruken av IT.

A141. Forståelsen av enhetens forretningsmodell og hvordan den integrerer bruken av IT, kan også gi en nyttig kontekst med hensyn til typen og omfanget av IT som kan forventes i informasjonssystemet.

[38] ISA 570 (revidert), punkt 19–20

Forståelse av enhetens bruk av IT

A142. Revisors forståelse av IT-miljøet kan være fokusert på å identifisere og forstå typen og antallet av de spesifikke IT-applikasjonene og andre aspekter ved IT-miljøet som er relevante for transaksjonsflyten og prosessering av informasjon. Endringer i transaksjonsflyten eller informasjonen i informasjonssystemet kan stamme fra programendringer i IT-applikasjoner, direkte endringer av data i databaser involvert i behandlingen, eller lagring av disse transaksjonene eller denne informasjonen.

A143. Revisor kan identifisere IT-applikasjonene og underbyggende IT-infrastruktur samtidig med at revisor opparbeider seg en forståelse av hvordan informasjon knyttet til signifikante transaksjonsklasser, kontosaldoer og tilleggsopplysninger registreres, beveger seg gjennom og føres ut av enhetens informasjonssystem.

Opparbeidelse av en forståelse av enhetens kommunikasjon (Jf. punkt 25(b))

Skalerbarhet

A144. I større, mer komplekse enheter kan informasjon som revisor kan vurdere når revisor opparbeider seg en forståelse av enhetens kommunikasjon, komme fra håndbøker med retningslinjer og håndbøker for finansiell rapportering.

A145. I mindre komplekse enheter kan kommunikasjon være mindre strukturert (for eksempel at det ikke benyttes formelle håndbøker) som følge av færre ansvarsnivåer og at ledelsen er mer synlig og tilgjengelig. Uavhengig av størrelsen på enheten, bidrar åpne kommunikasjonskanaler til å sikre at avvik rapporteres og håndteres.

Evaluering av hvorvidt de relevante aspektene ved informasjonssystemet underbygger utarbeidelsen av enhetens regnskap (Jf. punkt 25(c))

A146. Revisors evaluering av hvorvidt enhetens informasjonssystem og kommunikasjon underbygger utarbeidelsen av regnskapet på en hensiktsmessig måte, bygger på forståelsen som er opparbeidet i samsvar med punkt 25(a)–(b).

Kontrollaktiviteter (Jf. punkt 26)

Kontroller i komponenten «kontrollaktiviteter»

> **Vedlegg 3**, punkt 20 og 21, inneholder ytterligere vurderinger knyttet til kontrollaktiviteter.

A147. Komponenten «kontrollaktiviteter» omfatter kontroller som er utformet for å sikre riktig anvendelse av retningslinjer (som også er kontroller) i alle de andre komponentene i enhetens internkontrollsystem, og omfatter både direkte og indirekte kontroller.

Eksempel:

Kontrollene som en enhet har etablert for å sikre at personalet årlig teller og registrerer det fysiske varelageret på riktig måte, er direkte knyttet til risikoene for vesentlig feilinformasjon som er relevante for påstandene om eksistens og fullstendighet av saldoen på varelagerkontoen.

A148. Revisors identifisering og evaluering av kontroller i komponenten «kontrollaktiviteter» er fokusert på informasjonsbehandlingskontroller, som er kontroller anvendt under prosessering av informasjon i enhetens informasjonssystem som direkte håndterer risikoer knyttet til informasjonens integritet (dvs. fullstendigheten, nøyaktigheten og gyldigheten av transaksjoner og annen informasjon). Revisor er imidlertid ikke pålagt å identifisere og evaluere alle informasjonsbehandlingskontroller relatert til enhetens retningslinjer som definerer transaksjonsflyten og andre aspekter ved enhetens informasjonsbehandlingsaktiviteter for signifikante transaksjonsklasser, kontosaldoer og tilleggsopplysninger.

A149. Det kan også være at det finnes direkte kontroller i kontrollmiljøet, enhetens risikovurderingsprosess eller enhetens prosess for overvåking av internkontrollsystemet, som kan identifiseres i samsvar med punkt 26. Desto mer indirekte tilknytning mellom kontroller som underbygger andre kontroller og kontrollen som vurderes, desto mindre effektiv kan imidlertid denne kontrollen være for å forebygge, eller avdekke og korrigere, tilhørende feilinformasjon.

Eksempel:

En salgssjefs gjennomgåelse av regionvise salgsstatistikker for butikkene er for eksempel vanligvis bare indirekte knyttet til risikoene for vesentlig feilinformasjon som er relevante for påstanden om fullstendighet for salgsinntekter. Følgelig kan den være mindre egnet til å håndtere disse risikoene enn kontroller som er mer direkte knyttet til påstanden, for eksempel sammenligning av fraktdokumenter mot fakturaer.

A150. Punkt 26 krever også at revisor identifiserer og evaluerer generelle IT-kontroller for IT-applikasjoner og andre aspekter ved IT-miljøet som etter revisors vurdering er gjenstand for risikoer som følger av bruken av IT, ettersom generelle IT-kontroller underbygger den fortsatte effektive funksjonen av informasjonsbehandlingskontroller. En generell IT-kontroll alene er vanligvis ikke tilstrekkelig til å håndtere en risiko for vesentlig feilinformasjon på påstandsnivå.

A151. Kontrollene som revisor er pålagt å identifisere og evaluere utformingen av, og fastsette implementeringen av, i samsvar med punkt 26, er som følger:

- Kontroller som revisor planlegger å teste om fungerer effektivt av gjennom fastsettelse av typen, tidspunktet og omfanget av substanshandlinger. Evalueringen av slike kontroller gir grunnlag for revisors utforming av tester av kontroller i samsvar med ISA 330. Disse kontrollene omfatter også kontroller som håndterer risikoer der substanshandlinger alene ikke gir tilstrekkelig og hensiktsmessig revisjonsbevis.

- Kontroller inkluderer kontroller som håndterer særskilte risikoer, og kontroller knyttet til posteringer. Revisors identifisering og evaluering av slike kontroller kan også påvirke revisors forståelse av risikoene for vesentlig feilinformasjon, herunder identifiseringen av ytterligere risikoer for vesentlig feilinformasjon (se punkt A95). Denne forståelsen gir også grunnlag for revisors utforming av typen, tidspunktet og omfanget av substanshandlinger som er tilpasset de relaterte anslåtte risikoene for vesentlig feilinformasjon.
- Andre kontroller som revisor vurderer som hensiktsmessige for å kunne oppfylle målene i punkt 13 med hensyn til risikoer på påstandsnivå, basert på revisors profesjonelle skjønn.

A152. Det kreves at kontroller i komponenten «kontrollaktiviteter» identifiseres når slike kontroller oppfyller ett eller flere av kriteriene inkludert i punkt 26(a). Når flere kontroller oppfyller det samme målet, er det imidlertid unødvendig å identifisere hver kontroll som er knyttet til det aktuelle målet.

Typer kontroller i komponenten «kontrollaktiviteter» (Jf. punkt 26)

A153. Eksempler på kontroller i komponenten «kontrollaktiviteter» omfatter autorisasjoner og godkjenninger, avstemminger, verifiseringer (for eksempel redigerings- og valideringskontroller eller automatiserte beregninger), arbeidsdeling og fysiske eller logiske kontroller, herunder dem som er knyttet til sikring av eiendeler.

A154. Kontroller i komponenten «kontrollaktiviteter» kan også omfatte kontroller etablert av ledelsen for å håndtere risikoer for vesentlig feilinformasjon knyttet til tilleggsopplysninger som ikke er utarbeidet i samsvar med det gjeldende rammeverket for finansiell rapportering. Slike kontroller kan være knyttet til informasjon gitt i regnskapet som er innhentet fra andre kilder enn hovedboken og reskontroer.

A155. Uavhengig av om kontroller er innenfor IT-miljøet eller manuelle systemer, kan kontroller ha forskjellige mål og anvendes på forskjellige organisasjons- og funksjonsnivåer.

Skalerbarhet (Jf. punkt 26)

A156. Kontroller i komponenten «kontrollaktiviteter» for mindre komplekse enheter er ofte de samme som i større enheter, men graden av formalitet kan variere. Videre kan det i mindre komplekse enheter være flere kontroller som anvendes direkte av ledelsen.

> **Eksempel**:
>
> Ledelsens eksklusive myndighet til å gi kundekreditt og godkjenne vesentlige innkjøp kan gi sterk kontroll over viktige kontosaldoer og transaksjoner.

A157. Det kan være vanskeligere å etablere arbeidsdeling i mindre komplekse enheter som har færre ansatte. I en enhet som ledes av eier, kan imidlertid eier-leder være i stand til å føre mer effektivt tilsyn gjennom direkte deltakelse enn i en større enhet, noe som kan kompensere for de generelt mer begrensede mulighetene for arbeidsdeling. På den annen side, slik det også er forklart i ISA 240, kan

det at ledelsen domineres av en enkelt person være en mulig kontrollmangel, siden det utgjør en mulighet for at ledelsen overstyrer kontroller.[39]

Kontroller som håndterer risikoer for vesentlig feilinformasjon på påstandsnivå (Jf. punkt 26(a))

Kontroller som håndterer risikoer som er vurdert til å være en særskilt risiko (Jf. punkt 26(a)(i))

A158. Uavhengig av om revisor planlegger å teste om kontroller fungerer effektivt som håndterer særskilte risikoer, kan den opparbeidede forståelsen av ledelsens tilnærming til håndteringen av disse risikoene, gi grunnlag for utformingen og gjennomføringen av substanshandlinger som er tilpasset særskilte risikoer, som pålagt av ISA 330.[40] Selv om risikoer knyttet til vesentlige ikke-rutinemessige eller skjønnsmessige forhold som regel ikke er gjenstand for rutinemessige kontroller, kan ledelsen ha andre reaksjoner som er ment å håndtere slike risikoer. Revisors forståelse av hvorvidt enheten har utformet og implementert kontroller knyttet til særskilte risikoer som oppstår som følge av ikke-rutinemessige eller skjønnsmessige forhold, kan følgelig omfatte hvorvidt og hvordan ledelsen reagerer på risikoene. Slike reaksjoner kan omfatte:

- Kontroller, for eksempel den øverste ledelsens eller eksperters gjennomgåelse av forutsetninger.
- Dokumenterte prosesser for regnskapsestimater.
- Godkjenning av dem som har overordnet ansvar for styring og kontroll.

> **Eksempel**:
>
> Når engangshendelser forekommer, for eksempel mottak av varsel om en vesentlig rettssak, kan vurderingen av enhetens reaksjon blant annet omfatte forhold som hvorvidt saken er henvist til egnede eksperter (interne eller eksterne juridiske rådgivere), hvorvidt det er foretatt en vurdering av den mulige virkningen, og hvordan det er foreslått å opplyse om omstendighetene i regnskapet.

A159. ISA 240[41] krever at revisor forstår kontroller knyttet til anslåtte risikoer for vesentlig feilinformasjon som skyldes misligheter (som behandles som særskilte risikoer), og forklarer videre at det er viktig at revisor opparbeider seg en forståelse av kontrollene som ledelsen har utformet, implementert og vedlikeholdt for å forebygge og avdekke misligheter.

Kontroller knyttet til posteringer (Jf. punkt 26(a)(ii))

A160. Kontroller knyttet til posteringer er kontroller som håndterer risikoer for vesentlig feilinformasjon på påstandsnivå som forventes bli identifisert ved alle revisjoner, ettersom måten enheten fører inn informasjon fra transaksjonsbehandlingen i hovedboken på, vanligvis innebærer bruk av posteringer, uansett om de er standardiserte eller ikke-standardiserte, eller automatiserte eller manuelle. I hvilket

[39] ISA 240, punkt A28

[40] ISA 330, punkt 21

[41] ISA 240, punkt 28 og A33

omfang andre kontroller blir identifisert, kan variere avhengig av typen enhet og revisors planlagte tilnærming til videre revisjonshandlinger.

> **Eksempel**:
>
> Ved revisjon av en mindre kompleks enhet er det mulig at enhetens informasjonssystem ikke er komplekst og at revisor ikke kan planlegge å bygge på om kontroller fungerer effektivt. Videre kan det være at revisor ikke har identifisert noen særskilte risikoer eller andre risikoer for vesentlig feilinformasjon som krever at revisor evaluerer utformingen av kontroller og fastsetter at de er implementert. Ved en slik revisjon kan revisor fastslå at det ikke finnes andre identifiserte kontroller enn enhetens kontroller knyttet til posteringer.

Automatiserte verktøy og teknikker

A161. Når hovedboken føres manuelt, kan ikke-standardiserte posteringer identifiseres gjennom inspeksjon av regnskapsbøker, journaler og underliggende dokumentasjon. Når automatiserte rutiner benyttes til å føre hovedboken og utarbeide regnskap, kan det imidlertid være at disse registreringene kun finnes i elektronisk form og derfor enklere kan identifiseres ved bruk av automatiserte teknikker.

> **Eksempel**:
>
> Ved revisjon av en mindre kompleks enhet kan det være at revisor kan hente ut en fullstendig liste over alle hovedbokposteringer og overføre dem til et enkelt regneark. Det kan deretter være mulig for revisor å sortere hovedbokposteringene ved hjelp av forskjellige filtre, for eksempel valutabeløp, navn på den som har utarbeidet eller gjennomgått regnskapet, hovedbokposteringer som kun er ført i balansen og resultatregnskapet, eller å vise listen etter datoen da posteringen ble ført i hovedboken, for å hjelpe revisor med å utforme handlinger som kan håndtere de identifiserte risikoene knyttet til hovedbokposteringer.

Kontroller som revisor planlegger å teste om fungerer effektivt av (Jf. punkt 26(a)(iii))

A162. Revisor fastslår hvorvidt det foreligger risikoer for vesentlig feilinformasjon på påstandsnivå som det ikke er mulig å innhente tilstrekkelig og hensiktsmessig revisjonsbevis for gjennom substanshandlinger alene. Revisor er pålagt, i samsvar med ISA 330,[42] å utforme og utføre tester av kontroller som håndterer slike risikoer for vesentlig feilinformasjon når substanshandlinger alene ikke gir tilstrekkelig og hensiktsmessig revisjonsbevis på påstandsnivå. Når det finnes slike kontroller som håndterer disse risikoene, kreves det følgelig at de blir identifisert og evaluert.

A163. I andre tilfeller, når revisor planlegger å bygge på at kontrollene fungerer effektivitet ved fastsettelse av typen, tidspunktet og omfanget av substanshandlinger i samsvar med ISA 330, kreves det også

[42] ISA 330, punkt 8(b)

at slike kontroller blir identifisert, ettersom ISA 330[43] krever at revisor utformer og utfører tester av disse kontrollene.

Eksempler:

Revisor kan planlegge å teste om kontroller fungerer effektivt:

- Knyttet til rutinemessige transaksjonsklasser, ettersom slik testing kan være mer effektiv for store mengder ensartede transaksjoner.
- Knyttet til fullstendigheten og nøyaktigheten av informasjon produsert av enheten (for eksempel kontroller knyttet til utarbeidelsen av systemgenererte rapporter), for å fastsette påliteligheten av denne informasjonen, når revisor har til hensikt å bygge på at kontrollene fungerer effektivt ved utforming og gjennomføring av videre revisjonshandlinger.
- Knyttet til mål for drift og overholdelse av lover og forskrifter når de er relatert til data som revisor evaluerer eller bruker ved gjennomføring av revisjonshandlinger.

A164. Revisors planer om å teste om kontroller fungerer effektivt kan også være påvirket av de identifiserte risikoene for vesentlig feilinformasjon på regnskapsnivå. Dersom det for eksempel er identifisert mangler knyttet til kontrollmiljøet, kan dette påvirke revisors generelle forventninger til at direkte kontroller fungerer effektivt.

Andre kontroller som revisor vurderer som hensiktsmessige (Jf. punkt 26(a)(iv))

A165. Andre kontroller som revisor kan vurdere som hensiktsmessige å identifisere og evaluere utformingen av, og fastsette implementeringen av, kan omfatte:

- Kontroller som håndterer risikoer vurdert til å være høyere på spekteret av iboende risiko, men som ikke er vurdert til å være en særskilt risiko;
- Kontroller knyttet til avstemming av detaljerte poster mot hovedboken; eller
- Komplementære brukerenhetskontroller, dersom enheten bruker en serviceorganisasjon.[44]

Identifisering av IT-applikasjoner og andre aspekter ved IT-miljøet, risikoer som følger av bruken av IT, og generelle IT-kontroller (Jf. punkt 26(b)–(c))

Vedlegg 5 inneholder eksempler på særtrekk ved IT-applikasjoner og andre aspekter ved IT-miljøet, og en veiledning knyttet til disse særtrekkene, som kan være relevant ved identifisering av IT-applikasjoner og andre aspekter ved IT-miljøet som kan være gjenstand for risikoer som følger av bruken av IT.

[43] ISA 330, punkt 8(a)

[44] ISA 402 *Særlige hensyn ved revisjon av en enhet som bruker en serviceorganisasjon*

Identifisering av IT-applikasjoner og andre aspekter ved IT-miljøet (Jf. punkt 26(b))

Hvorfor revisor identifiserer risikoer som følger av bruken av IT, og generelle IT-kontroller knyttet til identifiserte IT-applikasjoner og andre aspekter ved IT-miljøet

A166. Forståelsen av risikoene som følger av bruken av IT, og de generelle IT-kontrollene som er implementert av enheten for å håndtere disse risikoene, kan påvirke:

- Revisors beslutning om å teste om kontroller fungerer effektivt for å håndtere risikoer for vesentlig feilinformasjon på påstandsnivå;

  Eksempel:

  Når generelle IT-kontroller ikke er effektivt utformet eller hensiktsmessig implementert for å håndtere risikoer som følger av bruken av IT (for eksempel når kontroller ikke på en hensiktsmessig måte forebygger eller avdekker uautoriserte programendringer eller uautorisert tilgang til IT-applikasjoner), kan dette påvirke revisors beslutning om å bygge på automatiserte kontroller innenfor de berørte IT-applikasjonene.

- Revisors vurdering av kontrollrisiko på påstandsnivå;

  Eksempel:

  Om en informasjonsbehandlingskontroll vedvarende fungerer effektivt kan avhenge av visse generelle IT-kontroller som forebygger eller avdekker uautoriserte programendringer i IT-informasjonsbehandlingskontrollen (for eksempel programendringskontroller knyttet til den relaterte IT-applikasjonen). Under slike omstendigheter kan den forventede måleffektiviteten (eller mangelen på en) av den generelle IT-kontrollen påvirke revisors vurdering av kontrollrisiko (for eksempel at kontrollrisiko kan være høyere når slike generelle IT-kontroller forventes å være ineffektive, eller dersom revisor ikke planlegger å teste de generelle IT-kontrollene).

- Revisors strategi for å teste informasjon produsert av enheten, som er produsert av eller inneholder informasjon fra enhetens IT-applikasjoner;

  Eksempel:

  Når informasjon produsert av enheten som skal benyttes som revisjonsbevis, er produsert av IT-applikasjoner, kan revisor bestemme seg for å teste kontroller knyttet til systemgenererte rapporter, herunder identifisering og testing av de generelle IT-kontrollene som håndterer risikoer for urettmessige eller uautoriserte programendringer eller direkte endringer av data i rapportene.

- Revisors vurdering av iboende risiko på påstandsnivå; eller

Eksempel:

Når det er foretatt vesentlige eller omfattende programmeringsendringer i en IT-applikasjon for å håndtere nye eller reviderte rapporteringskrav i det gjeldende rammeverket for finansiell rapportering, kan dette være en indikasjon på kompleksiteten av de nye kravene og deres innvirkning på enhetens regnskap. Når slike omfattende programmerings- eller dataendringer forekommer, er det også sannsynlig at IT-applikasjonen er gjenstand for risikoer som følger av bruken av IT.

- Utformingen av videre revisjonshandlinger.

Eksempel:

Dersom informasjonsbehandlingskontroller avhenger av generelle IT-kontroller, kan revisor bestemme seg for å teste måleffektiviteten av de generelle IT-kontrollene, noe som deretter vil kreve utforming av tester av kontroller for disse generelle IT-kontrollene. Dersom, under de samme forutsetningene, revisor bestemmer seg for ikke å teste måleffektiviteten av de generelle IT-kontrollene, eller de generelle IT-kontrollene forventes å være ineffektive, kan det være at de tilknyttede risikoene som følger av bruken av IT, må håndteres gjennom utformingen av substanshandlinger. Det kan imidlertid forekomme at risikoene som følger av bruken av IT, ikke kan håndteres når slike risikoer er knyttet til risikoer som substanshandlinger alene ikke gir tilstrekkelig og hensiktsmessig revisjonsbevis for. Under slike omstendigheter kan revisor bli nødt til å vurdere innvirkningen på revisors konklusjon.

Identifisering av IT-applikasjoner som er gjenstand for risikoer som følger av bruken av IT

A167. For IT-applikasjoner som er relevante for informasjonssystemet, kan en forståelse av typen og kompleksiteten av de spesifikke IT-prosessene og generelle IT-kontrollene som enheten har på plass, hjelpe revisor med å fastsette hvilke IT-applikasjoner enheten bygger på for å sikre nøyaktig behandling og opprettholdelse av informasjonens integritet i enhetens informasjonssystem. Slike IT-applikasjoner kan være gjenstand for risikoer som følger av bruken av IT.

A168. Identifisering av IT-applikasjonene som er gjenstand for risikoer som følger av bruken av IT, innebærer en vurdering av kontroller identifisert av revisor, ettersom slike kontroller kan innebære bruken av IT eller bygge på IT. Revisor kan fokusere på hvorvidt en IT-applikasjon omfatter automatiserte kontroller som ledelsen bygger på og som revisor har identifisert, herunder kontroller som håndterer risikoer som substanshandlinger alene ikke gir tilstrekkelig og hensiktsmessig revisjonsbevis for. Revisor kan også vurdere hvordan informasjon knyttet til signifikante transaksjonsklasser, kontosaldoer og tilleggsopplysninger lagres og behandles i informasjonssystemet, og hvorvidt ledelsen bygger på generelle IT-kontroller for å opprettholde integriteten til denne informasjonen.

A169. Kontrollene identifisert av revisor kan avhenge av systemgenererte rapporter. I så fall kan IT-applikasjonene som produserer disse rapportene, være gjenstand for risikoer som følger av bruken

av IT. I andre tilfeller kan det være at revisor ikke planlegger å bygge på kontroller knyttet til de systemgenererte rapportene, men planlegger å teste inn- og utdataene i slike rapporter direkte. I så fall er det mulig at revisor ikke identifiserer de tilknyttede IT-applikasjonene som gjenstand for risikoer som følger av IT.

Skalerbarhet

A170. Omfanget av revisors forståelse av IT-prosessene, herunder i hvilket omfang enheten har generelle IT-kontroller på plass, vil variere med typen og omstendighetene ved enheten og enhetens IT-miljø, og være basert på typen og omfanget av kontroller som er identifisert av revisor. Antallet IT-applikasjoner som er gjenstand for risikoer som følger av bruken av IT, vil variere basert på disse faktorene.

Eksempler:

- En enhet som bruker kommersiell programvare og som ikke har tilgang til kildekoden for å gjøre eventuelle programendringer, vil som regel ikke ha en prosess for programendringer, men en prosess eller rutiner for å konfigurere programvaren (for eksempel kontoplan, rapporteringsparametere eller terskler). I tillegg kan enheten ha en prosess eller rutiner for å håndtere tilgang til applikasjonen (for eksempel en utpekt person med administratortilgang til den kommersielle programvaren). Under slike omstendigheter vil enheten som regel ikke ha, eller ha behov for, generelle IT-kontroller.
- På den annen side kan en større enhet bygge på IT i stor grad, og IT-miljøet kan omfatte flere IT-applikasjoner og IT-prosessene som administrerer IT-miljøet kan være komplekse (for eksempel kan enheten ha en egen IT-avdeling som utvikler og implementerer programendringer og administrerer tilgangsrettigheter), herunder at enheten har implementert formaliserte generelle IT-kontroller knyttet til sine IT-prosesser.
- Når ledelsen ikke bygger på automatiserte kontroller eller generelle IT-kontroller for å behandle transaksjoner eller vedlikeholde dataene, og revisor ikke har identifisert noen automatiserte kontroller eller andre informasjonsbehandlingskontroller (eller noen som avhenger av generelle IT-kontroller), kan revisor planlegge å teste informasjon produsert av enheten ved bruk av IT direkte, og identifiserer ikke nødvendigvis IT-applikasjoner som er gjenstand for risikoer som følger av bruken av IT.
- Når ledelsen bygger på en IT-applikasjon for å behandle eller vedlikeholde data og datamengden er betydelig, og ledelsen bygger på IT-applikasjonen for å utføre automatiserte kontroller som revisor også har identifisert, er det sannsynlig at IT-applikasjonen er gjenstand for risikoer som følger av bruken av IT.

A171. Når en enhet har et IT-miljø med en høyere grad av kompleksitet, vil identifisering av IT-applikasjoner og andre aspekter ved IT-miljøet, fastsettelse av tilknyttede risikoer som følger av bruken av IT, og identifisering av generelle IT-kontroller, som regel kreve deltakelse av teammedlemmer med

spesialistferdigheter innen IT. En slik deltakelse vil som regel være avgjørende, og kan være omfattende, for komplekse IT-miljøer.

Identifisering av andre aspekter ved IT-miljøet som er gjenstand for risikoer som følger av bruken av IT

A172. De andre aspektene ved IT-miljøet som kan være gjenstand for risikoer som følger av bruken av IT, omfatter nettverket, operativsystemet og databaser og, under visse omstendigheter, grensesnitt mellom IT-applikasjoner. Andre aspekter ved IT-miljøet blir vanligvis ikke identifisert når revisor ikke identifiserer IT-applikasjoner som er gjenstand for risikoer som følger av bruken av IT. Når revisor har identifisert IT-applikasjoner som er gjenstand for risikoer som følger av IT, blir som regel andre aspekter ved IT-miljøet (for eksempel database, operativsystem, nettverk) identifisert, ettersom slike aspekter underbygger og interagerer med de identifiserte IT-applikasjonene.

Identifisering av risikoer som følger av bruken av IT, og generelle IT-kontroller (Jf. punkt 26(c))

> **Vedlegg 6** inneholder vurderinger knyttet til forståelsen av generelle IT-kontroller.

A173. Ved identifisering av risikoer som følger av bruken av IT, kan revisor vurdere typen av den identifiserte IT-applikasjonen eller andre aspekter ved IT-miljøet, og årsakene til at den er gjenstand for risikoer som følger av bruken av IT. For enkelte identifiserte IT-applikasjoner eller andre aspekter ved IT-miljøet kan revisor identifisere relevante risikoer som følger av bruken av IT som er knyttet primært til uautorisert tilgang eller uautoriserte programendringer, så vel som risikoer knyttet til urettmessige dataendringer (for eksempel risikoen for urettmessige endringer i dataene gjennom direkte databasetilgang eller muligheten for å manipulere informasjon direkte).

A174. Omfanget og typen av relevante risikoer som følger av bruken av IT, kan variere avhengig av typen og særtrekkene ved de identifiserte IT-applikasjonene og andre aspekter ved IT-miljøet. Relevante IT-risikoer kan oppstå når enheten bruker eksterne eller interne tjenesteleverandører for identifiserte aspekter ved IT-miljøet (for eksempel utkontraktering av driften av IT-miljøet til en tredjepart eller bruk av et felles driftssenter for sentral administrasjon av IT-prosesser i et konsern). Relevante risikoer som følger av bruken av IT, kan også identifiseres knyttet til cybersikkerhet. Det er mer sannsynlig at det vil foreligge flere risikoer som følger av bruken av IT, når mengden eller kompleksiteten av automatiserte applikasjonskontroller er høyere, og ledelsen i stor grad bygger på disse kontrollene for å sikre effektiv behandling av transaksjoner eller effektivt vedlikehold av den underliggende informasjonens integritet.

Evaluering av utformingen, og fastsettelse av implementeringen, av identifiserte kontroller i komponenten «kontrollaktiviteter» (Jf. punkt 26(d))

A175. Evaluering av utformingen av en identifisert kontroll innebærer at revisor vurderer hvorvidt kontrollen, individuelt eller i kombinasjon med andre kontroller, er i stand til på en effektiv måte å forebygge, eller avdekke og korrigere, vesentlig feilinformasjon (dvs. kontrollmålet).

A176. Revisor fastslår implementeringen av en identifisert kontroll ved å fastslå at kontrollen eksisterer og at enheten bruker den. Det har liten hensikt at revisor vurderer implementeringen av en kontroll som ikke er effektivt utformet. Følgelig evaluerer revisor utformingen av en kontroll først. En feilaktig utformet kontroll kan utgjøre en kontrollmangel.

A177. Risikovurderingshandlinger for å innhente revisjonsbevis for utformingen og implementeringen av identifiserte kontroller i komponenten «kontrollaktiviteter» kan omfatte:

- Forespørsler til ansatte i enheten.
- Observasjon av utførelsen av bestemte kontroller.
- Inspeksjon av dokumenter og rapporter.

Forespørsler alene er imidlertid ikke tilstrekkelig i denne sammenhengen.

A178. Det kan være at revisor, basert på erfaring fra den foregående revisjonen eller på risikovurderingshandlingene i inneværende periode, forventer at ledelsen ikke har utformet eller implementert kontroller på en effektiv måte for å håndtere en særskilt risiko. I slike tilfeller kan handlingene som utføres for å håndtere kravet i punkt 26(d), bestå av å fastsette at slike kontroller ikke er effektivt utformet eller implementert. Dersom resultatet av handlingene tyder på at kontroller nylig er utformet eller implementert, kreves det at revisor utfører handlingene i punkt 26(b)–(d) på de nylig utformede eller implementerte kontrollene.

A179. Revisor kan konkludere at det kan være hensiktsmessig å teste en kontroll som er effektivt utformet og implementert, for å vurdere om kontrollen fungerer effektivit ved utforming av substanshandlinger. Når en kontroll ikke er effektivt utformet eller implementert, har det imidlertid ingen hensikt å teste den. Når revisor planlegger å teste en kontroll, er den innhentede informasjonen om i hvilken grad kontrollen håndterer risikoene for vesentlig feilinformasjon, et bidrag til revisors kontrollrisikovurdering på påstandsnivå.

A180. Evaluering av utformingen, og fastslåelse av implementeringen, av identifiserte kontroller i komponenten «kontrollaktiviteter» er ikke tilstrekkelig til å teste om kontrollen fungerer effektivt. For automatiserte kontroller kan imidlertid revisor planlegge å teste om automatiserte kontroller fungerer effektivt ved å identifisere og teste generelle IT-kontroller som sørger for en enhetlig drift av en automatisert kontroll, i stedet for å utføre tester om de automatiserte kontrollene fungerer effektivt direkte. Innhenting av revisjonsbevis for implementeringen av en manuell kontroll på et gitt tidspunkt gir for eksempel ikke revisjonsbevis for om kontrollen fungerer effektivt på andre tidspunkter i perioden som revideres. Tester av om kontroller fungerer effektivt, herunder tester av indirekte kontroller, er ytterligere beskrevet i ISA 330.[45]

A181. Når revisor ikke planlegger å teste om identifiserte kontroller fungerer effektivt, kan revisors forståelse fortsatt være til hjelp ved utformingen av typen, tidspunktet og omfanget av substanshandlinger som er tilpasset de relaterte risikoene for vesentlig feilinformasjon.

[45] ISA 330, punkt 8–11

Eksempel:

Resultatet av disse risikovurderingshandlingene kan gi grunnlag for revisors vurdering av mulige avvik i en populasjon ved utforming av revisjonsutvalg.

Kontrollmangler i enhetens internkontrollsystem (Jf. punkt 27)

A182. Ved gjennomføring av evalueringen av hver av komponentene i enhetens internkontrollsystem[46] kan revisor fastslå at noen av enhetens retningslinjer i en komponent, ikke er hensiktsmessige ut fra typen og omstendighetene ved enheten. En slik fastslåelse kan være en indikasjon som hjelper revisor med å identifisere kontrollmangler. Dersom revisor har identifisert en eller flere kontrollmangler, kan revisor vurdere virkningen av disse kontrollmanglene på utformingen av videre revisjonshandlinger i samsvar med ISA 330.

A183. Dersom revisor har identifisert en eller flere kontrollmangler, krever ISA 265[47] at revisor fastslår hvorvidt, individuelt eller i kombinasjon, manglene utgjør en vesentlig mangel. Revisor utøver profesjonelt skjønn ved fastsettelse av hvorvidt en mangel utgjør en vesentlig kontrollmangel.[48]

Eksempler:

Omstendigheter som kan tyde på at det foreligger en vesentlig kontrollmangel, omfatter forhold som:

- Identifisering av misligheter, uansett omfang, som involverer den øverste ledelsen;
- Identifiserte interne prosesser som er utilstrekkelige når det gjelder rapportering og kommunikasjon av mangler notert ved intern revisjon;
- Tidligere kommuniserte mangler som ikke er korrigert av ledelsen i rett tid;
- Ledelsens unnlatelse av å håndtere særskilte risikoer, for eksempel ved ikke å implementere kontroller knyttet til særskilte risikoer; og
- Omarbeidelse av tidligere avgitte regnskaper.

Identifisering og vurdering av risikoene for vesentlig feilinformasjon (Jf. punkt 28–37)

Hvorfor revisor identifiserer og vurderer risikoene for vesentlig feilinformasjon

A184. Risikoer for vesentlig feilinformasjon identifiseres og vurderes av revisor for å fastsette typen, tidspunktet og omfanget av videre revisjonshandlinger som er nødvendige for å innhente tilstrekkelig

[46] Punkt 21(b), 22(b), 24(c), 25(c) og 26(d)

[47] ISA 265 *Kommunikasjon av mangler i intern kontroll til dem som har overordnet ansvar for styring og kontroll, samt ledelsen*, punkt 8

[48] ISA 265, punkt A6–A7, gir eksempler på indikasjoner på vesentlige mangler samt forhold som skal vurderes ved fastsettelse av hvorvidt en mangel, eller en kombinasjon av mangler, i intern kontroll utgjør en vesentlig mangel.

og hensiktsmessig revisjonsbevis. Dette beviset gjør det mulig for revisor å gi uttrykk for en mening om regnskapet på et akseptabelt lavt revisjonsrisikonivå.

A185. Informasjon innhentet ved å utføre risikovurderingshandlingene benyttes som revisjonsbevis for å gi grunnlag for identifisering og vurdering av risikoene for vesentlig feilinformasjon. For eksempel benyttes revisjonsbeviset som er innhentet ved å evaluere utformingen av identifiserte kontroller og fastslå hvorvidt disse kontrollene er implementert i komponenten «kontrollaktiviteter», som revisjonsbevis for å underbygge risikovurderingen. Slikt bevis gir også revisor grunnlag for å utforme overordnede handlinger for å håndtere de anslåtte risikoene for vesentlig feilinformasjon på påstandsnivå, og for å utforme og utføre videre revisjonshandlinger hvis type, tidspunkt og omfang er tilpasset de anslåtte risikoene for vesentlig feilinformasjon på påstandsnivå, i samsvar med ISA 330.

Identifisering av risikoer for vesentlig feilinformasjon (Jf. punkt 28)

A186. Identifiseringen av risikoer for vesentlig feilinformasjon utføres før vurderingen av eventuelle tilknyttede kontroller (dvs. iboende risiko), og er basert på revisors foreløpige vurdering av feilinformasjon som har en rimelig mulighet for både å forekomme og å være vesentlig dersom de forekommer.[49]

A187. Identifisering av risikoene for vesentlig feilinformasjon gir også grunnlag for revisors fastsettelse av relevante påstander, som hjelper revisor med å fastsette de signifikante transaksjonsklassene, kontosaldoene og tilleggsopplysningene.

Påstander

Hvorfor revisor bruker påstander

A188. Ved identifisering og vurdering av risikoene for vesentlig feilinformasjon bruker revisor påstander til å vurdere de ulike typene mulig feilinformasjon som kan forekomme. Påstander der revisor har identifisert tilknyttede risikoer for vesentlig feilinformasjon, er relevante påstander.

Bruken av påstander

A189. Ved identifisering og vurdering av risikoene for vesentlig feilinformasjon kan revisor bruke kategoriene av påstander som er beskrevet i punkt A190(a)–(b) nedenfor, eller uttrykke dem på en annen måte forutsatt at alle aspektene som er beskrevet nedenfor, er dekket. Revisor kan velge å kombinere påstandene om transaksjonsklasser og hendelser og tilhørende tilleggsopplysninger med påstandene om kontosaldoer og tilhørende tilleggsopplysninger.

A190. Påstander som benyttes av revisor ved vurdering av forskjellige typer mulig feilinformasjon som kan forekomme, kan falle inn under følgende kategorier:

(a) Påstander om transaksjonsklasser og hendelser og tilhørende tilleggsopplysninger i perioden som revideres:

[49] ISA 200, punkt A15a

(i) Gyldighet – transaksjoner og hendelser som er registrert eller opplyst om har forekommet, og slike transaksjoner og hendelser vedrører enheten.

(ii) Fullstendighet – alle transaksjoner og hendelser som skulle ha vært registrert, er registrert, og alle tilhørende tilleggsopplysninger som skulle ha vært med i regnskapet, er tatt med.

(iii) Nøyaktighet – beløp og andre data knyttet til registrerte transaksjoner og hendelser er riktig registrert i forhold til grunnlaget, og tilhørende tilleggsopplysninger er tilstrekkelig målt og beskrevet.

(iv) Periodisering – transaksjoner og hendelser er registrert i riktig regnskapsperiode.

(v) Klassifisering – transaksjoner og hendelser er registrert på riktige kontoer.

(vi) Presentasjon – transaksjoner og hendelser er tilstrekkelig aggregert eller disaggregert og klart beskrevet, og tilhørende tilleggsopplysninger er relevante og forståelige i kontekst av kravene i det gjeldende rammeverket for finansiell rapportering.

(b) Påstander om kontosaldoer og tilhørende tilleggsopplysninger ved regnskapsperiodens slutt:

(i) Eksistens – eiendeler, gjeld og egenkapital eksisterer.

(ii) Rettigheter og forpliktelser – enheten innehar eller kontrollerer rettighetene til eiendeler, og gjeld er enhetens forpliktelser.

(iii) Fullstendighet – alle eiendeler og all gjeld og egenkapital som skulle ha vært registrert, er registrert, og alle tilhørende tilleggsopplysninger som skulle ha vært med i regnskapet, er tatt med.

(iv) Nøyaktighet, verdsettelse og allokering – eiendeler, gjeld og egenkapital er inkludert i regnskapet med riktige beløp, og eventuelle resulterende justeringer av verdsettelse eller allokering er riktig registrert, og tilhørende tilleggsopplysninger er tilstrekkelig målt og beskrevet.

(v) Klassifisering – eiendeler, forpliktelser og egenkapitalinteresser er registrert på riktige kontoer.

(vi) Presentasjon – eiendeler, forpliktelser og egenkapitalinteresser er tilstrekkelig aggregert eller disaggregert og klart beskrevet, og tilhørende tilleggsopplysninger er relevante og forståelige i kontekst av kravene i det gjeldende rammeverket for finansiell rapportering.

A191. Påstandene beskrevet i punkt A190(a)–(b) ovenfor, anvendt på en hensiktsmessig måte, kan også benyttes av revisor ved vurdering av de ulike typene mulig feilinformasjon som kan forekomme i tilleggsopplysninger som ikke er direkte knyttet til registrerte transaksjonsklasser, hendelser eller kontosaldoer.

> **Eksempel**:
>
> Et eksempel på en slik tilleggsopplysning er når det gjeldende rammeverket for finansiell rapportering krever at enheten beskriver risikoeksponeringen knyttet til finansielle instrumenter, herunder hvordan risikoene oppstår, målene, retningslinjene og prosessene for å styre risikoene, og metodene som er benyttet for å måle risikoene.

Særlige hensyn knyttet til enheter i offentlig sektor

A192. Når det utarbeides påstander om regnskapet i offentlig sektor, kan det i tillegg til påstandene som er nevnt i punkt A190(a)–(b), ofte være at ledelsen påstår at transaksjoner og hendelser er utført i samsvar med lov, forskrift eller annen autorativ kilde. Slike påstander kan falle inn under omfanget av revisjonen av regnskapet.

Risikoer for vesentlig feilinformasjon på regnskapsnivå (Jf. punkt 28(a) og 30)

Hvorfor revisor identifiserer og vurderer risikoer for vesentlig feilinformasjon på regnskapsnivå

A193. Revisor identifiserer risikoer for vesentlig feilinformasjon på regnskapsnivå for å fastsette hvorvidt risikoene har en gjennomgripende virkning på regnskapet og dermed kan kreve overordnede handlinger i samsvar med ISA 330.[50]

A194. I tillegg kan risikoer for vesentlig feilinformasjon på regnskapsnivå påvirke individuelle påstander, og identifisering av disse risikoene kan hjelpe revisor med å anslå risikoer for vesentlig feilinformasjon på påstandsnivå, og med å utforme videre revisjonshandlinger for å håndtere de identifiserte risikoene.

Identifisering og vurdering av risikoer for vesentlig feilinformasjon på regnskapsnivå

A195. Risikoer for vesentlig feilinformasjon på regnskapsnivå refererer til risikoer som er mer gjennomgripende knyttet til regnskapet som helhet, og kan påvirke mange påstander. Slike risikoer er ikke nødvendigvis risikoer som kan knyttes til spesifikke påstander på transaksjonsklasse-, kontosaldo- eller tilleggsopplysningsnivå (for eksempel risiko for at ledelsen overstyrer kontroller). De representerer snarere omstendigheter som på en mer gjennomgripende måte kan øke risikoene for vesentlig feilinformasjon på påstandsnivå. Revisors evaluering av hvorvidt identifiserte risikoer er mer gjennomgripende knyttet til regnskapet, underbygger revisors vurdering av risikoene for vesentlig feilinformasjon på regnskapsnivå. I andre tilfeller kan flere påstander også bli identifisert som eksponert for risikoen, og kan derfor påvirke revisors risikoidentifisering og vurdering av risikoer for vesentlig feilinformasjon på påstandsnivå.

[50] ISA 330, punkt 5

Eksempel:

Enheten står overfor driftstap og likviditetsproblemer og er avhengig av finansiering som ennå ikke er sikret. Under slike omstendigheter kan revisor fastsette at forutsetningen om fortsatt drift medfører en risiko for vesentlig feilinformasjon på regnskapsnivå. I denne situasjonen kan det være behov for at rammeverket for regnskapsføring må anvendes under forutsetning om avvikling, noe som sannsynligvis vil påvirke alle påstander på en gjennomgripende måte.

A196. Revisors identifisering og vurdering av risikoer for vesentlig feilinformasjon på regnskapsnivå påvirkes av revisors forståelse av enhetens internkontrollsystem, særlig revisors forståelse av kontrollmiljøet, enhetens risikovurderingsprosess og enhetens prosess for overvåking av internkontrollsystemet, og:

- Utfallet av de tilknyttede evalueringene som kreves i punkt 21(b), 22(b), 24(c) og 25(c); og
- Eventuelle kontrollmangler identifisert i samsvar med punkt 27.

Risikoer på regnskapsnivå kan særlig oppstå som følge av mangler i kontrollmiljøet, eller som følge av eksterne hendelser eller forhold, for eksempel en generell lavkonjunktur.

A197. Risikoer for vesentlig feilinformasjon som skyldes misligheter, kan være spesielt relevant for revisors vurdering av risikoene for vesentlig feilinformasjon på regnskapsnivå.

Eksempel:

Revisor forstår ut fra forespørsler rettet til ledelsen at enhetens regnskap skal benyttes i diskusjoner med långivere for å sikre ytterligere finansiering for å opprettholde arbeidskapital. Revisor kan derfor fastsette at det er en større mulighet feilinformasjon på grunn av mislighetsrisikofaktorer som påvirker iboende risiko (dvs. regnskapets mulighet for vesentlig feilinformasjon på grunn av risikoen for uredelig finansiell rapportering, for eksempel overvurdering av eiendeler og inntekt og undervurdering av forpliktelser og kostnader for å sikre at finansiering oppnås).

A198. Revisors forståelse, herunder de tilknyttede evalueringene, av kontrollmiljøet og andre komponenter i internkontrollsystemet kan reise tvil om revisors evne til å innhente revisjonsbevis for å underbygge revisors konklusjon, eller føre til at revisor trekker seg fra oppdraget når dette er mulig etter gjeldende lov eller forskrift.

Eksempler:

- Som følge av evalueringen av enhetens kontrollmiljø, kan revisors usikkerhet vedrørende integriteten til enhetens ledelse være så stor at revisor konkluderer med at risikoen for tilsiktet feilrapportering fra ledelsen i regnskapet er så høy at en revisjon ikke kan gjennomføres.
- Som følge av evalueringen av enhetens informasjonssystem og kommunikasjon, fastslår revisor at viktige endringer i IT-miljøet er blitt dårlig styrt, med manglende oversikt fra ledelsen og dem som har overordnet ansvar for styring og kontroll. Revisor konkluderer med at det foreligger betydelig usikkerhet vedrørende tilstanden til og påliteligheten av enhetens regnskapsmateriale. Under slike omstendigheter kan revisor fastslå at det er usannsynlig at det foreligger tilstrekkelig og hensiktsmessig revisjonsbevis til å underbygge en umodifisert konklusjon om regnskapet.

A199. ISA 705 (revidert)[51] fastsetter krav og gir veiledning ved fastsettelse av hvorvidt det er behov for at revisor gir uttrykk for en konklusjon med forbehold eller en konklusjon om at revisor ikke kan uttale seg om regnskapet, eller, som det kan være påkrevd i visse tilfeller, at revisor trekker seg fra oppdraget når dette er mulig etter gjeldende lov eller forskrift.

Særlige hensyn knyttet til enheter i offentlig sektor

A200. For enheter i offentlig sektor kan identifiseringen av risikoer på regnskapsnivå omfatte vurdering av forhold som er knyttet til det politiske klimaet, offentlig interesse og programsensitivitet.

Risikoer for vesentlig feilinformasjon på påstandsnivå (Jf. punkt 28(b))

Vedlegg 2 gir eksempler, i kontekst av iboende risikofaktorer, på hendelser eller forhold som kan tyde på mulighet feilinformasjon som kan være vesentlig.

A201. Risikoer for vesentlig feilinformasjon som ikke er gjennomgripende knyttet til regnskapet, er risikoer for vesentlig feilinformasjon på påstandsnivå.

Relevante påstander og signifikante transaksjonsklasser, kontosaldoer og tilleggsopplysninger (Jf. punkt 29)

Hvorfor relevante påstander og signifikante transaksjonsklasser, kontosaldoer og tilleggsopplysninger fastsettes

A202. Fastsettelse av relevante påstander og signifikante transaksjonsklasser, kontosaldoer og tilleggsopplysninger danner grunnlaget for omfanget av revisors forståelse av enhetens informasjonssystem som revisor er pålagt å opparbeide seg i samsvar med punkt 25(a). Denne

[51] ISA 705 (revidert) *Modifikasjoner i konklusjonen i den uavhengige revisors beretning*

forståelsen kan videre hjelpe revisor med å identifisere og anslå risikoer for vesentlig feilinformasjon (se A86).

Automatiserte verktøy og teknikker

A203. Revisor kan bruke automatiserte teknikker som en hjelp i identifiseringen av signifikante transaksjonsklasser, kontosaldoer og tilleggsopplysninger.

Eksempler:

- En hel populasjon av transaksjoner kan analyseres ved hjelp av automatiserte verktøy og teknikker for å forstå typen, kilden, størrelsen og mengden. Ved å bruke automatiserte teknikker kan revisor for eksempel identifisere at en konto med null i saldo ved periodeslutt, har inneholdt en rekke motregningstransaksjoner og posteringer som har forekommet i perioden, noe som kan tyde på at kontosaldoen eller transaksjonsklassen kan være signifikant (for eksempel en oppgjørskonto for lønn). Denne samme oppgjørskontoen for lønn kan også identifisere refusjoner av utgifter til ledelsen (og andre ansatte), som kan være en signifikant tilleggsopplysning som følge av at disse utbetalingene er foretatt til nærstående parter.
- Ved å analysere flyten av en hel populasjon av inntektstransaksjoner kan det være enklere for revisor å identifisere en signifikant transaksjonsklasse som tidligere ikke har vært identifisert.

Tilleggsopplysninger som kan være signifikante

A204. Signifikante tilleggsopplysninger omfatter både kvantitative og kvalitative tilleggsopplysninger som det er knyttet en eller flere relevante påstander til. Eksempler på tilleggsopplysninger som har kvalitative aspekter og som kan ha relevante påstander og derfor kan bli vurdert som signifikante av revisor, omfatter tilleggsopplysninger om:

- Lånebetingelser knyttet til likviditets- og gjeldsgrader for en enhet i finansielle vansker.
- Hendelser eller omstendigheter som har medført innregnet tap ved verdifall på en eiendel.
- Hovedkilder til estimeringsusikkerhet, herunder forutsetninger om fremtiden.
- Arten av en endring i regnskapspraksis, eller andre relevante tilleggsopplysninger som kreves av det gjeldende rammeverket for finansiell rapportering, når det for eksempel ventes at nye finansielle rapporteringskrav vil ha en signifikant innvirkning på enhetens finansielle stilling og resultater.
- Aksjebaserte lønnsordninger, herunder informasjon om hvordan de innregnede beløpene ble fastsatt, og andre relevante tilleggsopplysninger.
- Nærstående parter og transaksjoner med nærstående parter.

- Sensitivitetsanalyser, herunder virkningene av endringer i forutsetninger benyttet i enhetens verdsettelsesteknikker i den hensikt å gjøre brukerne i stand til å forstå måleusikkerheten av et beløp som er registrert eller som det er gitt tilleggsopplysning om.

Vurdering av risikoer for vesentlig feilinformasjon på påstandsnivå

Vurdering av iboende risiko (Jf. punkt 31–33)

Vurdering av sannsynligheten for og omfanget av feilinformasjon (Jf. punkt 31)

Hvorfor revisor vurderer sannsynlighet for og konsekvensen av feilinformasjon

A205. Revisor vurderer sannsynligheten for og konsekvensen av feilinformasjon for identifiserte risikoer for vesentlig feilinformasjon, ettersom betydningen av kombinasjonen av sannsynligheten for at en feilinformasjon forekommer, og konsekvensen av den mulige feilinformasjonen dersom den forekommer, fastsetter hvor på spekteret av iboende risiko den identifiserte risikoen vurderes, noe som gir grunnlag for revisors utforming av videre revisjonshandlinger for å håndtere risikoen.

A206. Vurdering av den iboende risikoen knyttet til identifiserte risikoer for vesentlig feilinformasjon er også en hjelp for revisor ved fastsettelse av særskilte risikoer. Revisor fastsetter særskilte risikoer fordi det kreves spesifikke handlinger for å håndtere særskilte risikoer i samsvar med ISA 330 og andre ISA-er.

A207. Iboende risikofaktorer påvirker revisors vurdering av sannsynligheten for og konsekvensen av feilinformasjon for de identifiserte risikoene for vesentlig feilinformasjon på påstandsnivå. Jo mer en transaksjonsklasse, kontosaldo eller tilleggsopplysning kan inneholde feilinformasjon, desto høyere vil vurderingen av iboende risiko sannsynligvis være. Vurdering av i hvilken grad iboende risikofaktorer påvirker eksponeringen av en påstand for feilinformasjon, hjelper revisor med å foreta en hensiktsmessig vurdering av iboende risiko for risikoer for vesentlig feilinformasjon på påstandsnivå, og med å utforme en mer nøyaktig håndtering av en slik risiko.

Spekter av iboende risiko

A208. Ved vurdering av iboende risiko utøver revisor profesjonelt skjønn ved fastsettelse av betydningen av kombinasjonen av sannsynligheten for og konsekvensen av feilinformasjon.

A209. Den anslåtte iboende risikoen knyttet til en bestemt risiko for vesentlig feilinformasjon på påstandsnivå, representerer en skjønnsmessig vurdering innenfor et område, fra lav til høy, på spekteret av iboende risiko. Den skjønnsmessige vurderingen av hvor i området iboende risiko vurderes, kan variere avhengig av enhetens type, størrelse og kompleksitet, og tar i betraktning den vurderte sannsynligheten for og konsekvensen av feilinformasjonen og iboende risikofaktorer.

A210. Ved vurdering av sannsynligheten for feilinformasjon vurderer revisor muligheten for at feilinformasjon kan forekomme, basert på vurderingen av de iboende risikofaktorene.

A211. Ved vurdering av konsekvensen av en feilinformasjon vurderer revisor de kvalitative og kvantitative aspektene ved den mulige feilinformasjonen (dvs. at feilinformasjon i påstander om

transaksjonsklasser, kontosaldoer eller tilleggsopplysninger kan vurderes å være vesentlig på grunn av størrelse, type eller omstendigheter).

A212. Revisor bruker betydningen av kombinasjonen av sannsynligheten for og konsekvensen av mulig feilinformasjon for å fastsette hvor på spekteret av iboende risiko (dvs. området) iboende risiko vurderes. Jo høyere kombinasjonen av sannsynlighet og omfang er, desto høyere er vurderingen av iboende risiko. Jo lavere kombinasjonen av sannsynlighet og omfang er, desto lavere er vurderingen av iboende risiko.

A213. For at en risiko skal vurderes som høyere på spekteret av iboende risiko, er det ikke nødvendig at både konsekvensen og sannsynligheten må vurderes som høy. I stedet er det skjæringspunktet mellom konsekvensen av og sannsynligheten for vesentlig feilinformasjon på spekteret av iboende risiko som vil fastslå hvorvidt den anslåtte iboende risikoen er høyere eller lavere på spekteret av iboende risiko. En høyere iboende risikovurdering kan også oppstå som følge av forskjellige kombinasjoner av sannsynlighet og konsekvens, og en høyere iboende risikovurdering kan for eksempel være resultatet av en lavere sannsynlighet, men et svært stor konsekvens.

A214. For å utarbeide hensiktsmessige strategier for å håndtere risikoer for vesentlig feilinformasjon kan revisor kategorisere risikoer for vesentlig feilinformasjon innenfor kategorier langs spekteret av iboende risiko, basert på deres vurdering av iboende risiko. Disse kategoriene kan beskrives på forskjellige måter. Uavhengig av kategoriseringsmetoden som benyttes, er revisors vurdering av iboende risiko hensiktsmessig når utformingen og implementeringen av videre revisjonshandlinger for å håndtere de identifiserte risikoene for vesentlig feilinformasjon på påstandsnivå, er hensiktsmessig tilpasset vurderingen av iboende risiko og grunnlaget for denne vurderingen.

Gjennomgripende risikoer for vesentlig feilinformasjon på påstandsnivå (Jf. Para 31(b))

A215. Ved vurdering av de identifiserte risikoene for vesentlig feilinformasjon på påstandsnivå kan revisor konkludere med at enkelte risikoer for vesentlig feilinformasjon er mer gjennomgripende knyttet til regnskapet som helhet, og kan påvirke mange påstander. I så fall kan revisor oppdatere identifiseringen av risikoer for vesentlig feilinformasjon på regnskapsnivå.

A216. Under omstendigheter der risikoer for vesentlig feilinformasjon identifiseres som risikoer på regnskapsnivå fordi de har en gjennomgripende virkning på flere påstander, og er identifiserbare med spesifikke påstander, kreves det at revisor tar i betraktning disse risikoene ved vurdering av iboende risiko for risikoer for vesentlig feilinformasjon på påstandsnivå.

Særlige hensyn knyttet til enheter i offentlig sektor

A217. Ved utøvelse av profesjonelt skjønn i forbindelse med risikoen for vesentlig feilinformasjon, kan revisorer i enheter i offentlig sektor vurdere kompleksiteten av forskriftene og direktivene, og risikoene for manglende overholdelse av myndighetskrav.

Særskilte risikoer (Jf. punkt 32)

Hvorfor særskilte risikoer fastsettes og innvirkningen på revisjonen

A218. Fastsettelsen av særskilte risikoer gjør det mulig for revisor å rette mer oppmerksomhet mot risikoene som befinner seg i den øvre enden av spekteret av iboende risiko, ved å gjennomføre visse påkrevde handlinger, herunder:

- Kontroller som håndterer særskilte risikoer må være identifisert i samsvar med punkt 26(a)(i), og det er et krav at revisor evaluerer hvorvidt kontrollen er effektivt utformet og implementert i samsvar med punkt 26(d).
- ISA 330 krever at kontroller som håndterer særskilte risikoer skal testes i inneværende periode (når revisor har til hensikt å bygge på om disse kontrollene fungerer effektivt), og at det skal planlegges og gjennomføres substanshandlinger som er spesielt tilpasset den identifiserte særskilte risikoen.[52]
- ISA 330 krever at revisor innhenter mer overbevisende revisjonsbevis jo høyere revisor vurderer risikoen.[53]
- ISA 260 (revidert) krever kommunikasjon med dem som har overordnet ansvar for styring og kontroll om særskilte risikoer som er identifisert av revisor.[54]
- ISA 701 krever at revisor vurderer særskilte risikoer ved fastsettelse av forhold som krevde særskilt oppmerksomhet fra revisors side, som er forhold som kan være sentrale forhold ved revisjonen.[55]
- Oppdragsansvarlig revisors rettidige gjennomgåelse av revisjonsdokumentasjon på hensiktsmessige stadier under revisjonen gjør det mulig å avklare vesentlige forhold, herunder særskilte risikoer, i rett tid og til oppdragsansvarlig revisors tilfredsstillelse på eller før datoen for revisjonsberetningen.[56]
- ISA 600 krever mer deltakelse av oppdragsansvarlig revisor for konsernet dersom den særskilte risikoen er knyttet til en konsernenhet ved revisjon av et konsernregnskap, og at konsernrevisjonsteamet rettleder arbeidet som skal utføres i konsernenheten av revisor i konsernenheten.[57]

Fastsettelse av særskilte risikoer

---

[52] ISA 330, punkt 15 og 21

[53] ISA 330, punkt 7(b)

[54] ISA 260 (revidert), punkt 15

[55] ISA 701 *Omtale av sentrale forhold ved revisjonen i den uavhengige revisors beretning*, punkt 9

[56] ISA 220, punkt 17 og A19

[57] ISA 600, punkt 30 og 31

A219. Ved fastsettelse av særskilte risikoer, kan revisor først identifisere de anslåtte risikoene for vesentlig feilinformasjon som er vurdert til å være høyere på spekteret av iboende risiko, som grunnlag for vurderingen av hvilke risikoer som kan være nær den øvre enden. Å være nær den øvre enden av spekteret av iboende risiko, vil variere fra enhet til enhet og vil ikke nødvendigvis være identisk for en enhet fra én periode til en annen. Det kan avhenge av typen og omstendighetene ved enheten som risikoen vurderes.

A220. Fastsettelsen av hvilke av de anslåtte risikoene for vesentlig feilinformasjon som er nær den øvre enden av spekteret av iboende risiko, og som dermed er særskilte risikoer, er gjenstand for profesjonelt skjønn, med mindre risikoen er av en type som uttrykkelig er angitt skal behandles som en særskilt risiko i samsvar med kravene i en annen ISA. ISA 240 inneholder ytterligere krav og veiledning i forbindelse med identifiseringen og vurderingen av risikoene for vesentlig feilinformasjon som skyldes misligheter.[58]

Eksempel:

- Kontanter i en kjedebutikk vil vanligvis bli vurdert til å ha høy sannsynlighet for mulig feilinformasjon (på grunn av risikoen for at kontanter kan underslås), men konsekvensen vil vanligvis være svært lav (på grunn av det lave nivået av fysiske kontanter som håndteres i butikkene). Det er lite sannsynlig at kombinasjonen av disse to faktorene på spekteret av iboende risiko vil føre til at eksistensen av kontanter blir vurdert til å være en særskilt risiko.
- En enhet er i forhandlinger om å selge et forretningssegment. Revisor vurderer virkningen på nedskrivning av goodwill, og kan fastsette at det er en høyere sannsynlighet for mulig feilinformasjon og et større omfang på grunn av innvirkningen av iboende risikofaktorer knyttet til subjektivitet, usikkerhet og mulighet for manglende objektivitet hos ledelsen eller andre mislighetsrisikofaktorer. Dette kan føre til at nedskrivning av goodwill blir vurdert til å være en særskilt risiko.

A221. Revisor tar også i betraktning de relative virkningene av iboende risikofaktorer ved vurdering av iboende risiko. Jo lavere virkningen av iboende risikofaktorer er, desto lavere vil sannsynligvis den anslåtte risikoen være. Risikoer for vesentlig feilinformasjon som kan bli vurdert til å ha høyere iboende risiko og derfor kan bli vurdert til å være en særskilt risiko, kan oppstå som følge av forhold som:

- Transaksjoner som det finnes flere akseptable regnskapsbehandlinger for, slik at subjektivitet inngår.
- Regnskapsestimater som har høy estimeringsusikkerhet eller komplekse modeller.
- Kompleksitet ved datainnsamling og -behandling for å underbygge kontosaldoer.
- Kontosaldoer eller kvantitative tilleggsopplysninger som innebærer komplekse beregninger.

[58] ISA 240, punkt 26–28

- Regnskapsprinsipper som kan tolkes på forskjellige måter.
- Endringer i enhetens virksomhet som innebærer regnskapsendringer, for eksempel sammenslåinger og oppkjøp.

Risikoer der substanshandlinger alene ikke gir tilstrekkelig og hensiktsmessig revisjonsbevis (Jf. punkt 33)

Hvorfor det kreves at risikoer der substanshandlinger alene ikke gir tilstrekkelig og hensiktsmessig revisjonsbevis skal identifiseres

A222. Som følge av typen risiko for vesentlig feilinformasjon, og kontrollaktivitetene som håndterer denne risikoen, vil testing av om kontroller fungerer effektivt være den eneste måten å innhente tilstrekkelig og hensiktsmessig revisjonsbevis på under enkelte omstendigheter. Følgelig er det et krav at revisor identifiserer enhver slik risiko på grunn av innvirkningen på utformingen og gjennomføringen av videre revisjonshandlinger i samsvar med ISA 330 for å håndtere risikoer for vesentlig feilinformasjon på påstandsnivå.

A223. Punkt 26(a)(iii) krever også identifisering av kontroller som håndterer risikoer der substanshandlinger alene ikke kan gi tilstrekkelig og hensiktsmessig revisjonsbevis, ettersom revisor er pålagt, i samsvar med ISA 330,[59] å utforme og utføre tester av slike kontroller.

Fastsettelse av risikoer der substanshandlinger alene ikke gir tilstrekkelig og hensiktsmessig revisjonsbevis

A224. Når rutinemessige forretningstransaksjoner er gjenstand for en høy grad av automatisering med liten eller ingen manuell inngripen, vil det ikke alltid være mulig bare å utføre substanshandlinger i forbindelse med risikoen. Dette kan være tilfellet når en vesentlig del av en enhets informasjon utelukkende initieres, registreres, behandles eller rapporteres elektronisk, for eksempel i et informasjonssystem med en høy grad av integrasjon mellom IT-applikasjonene. I slike tilfeller kan:

- Revisjonsbevis foreligge utelukkende i elektronisk form, og bevisets tilstrekkelighet og hensiktsmessighet avhenger vanligvis av hvor effektiv kontrollen knyttet til bevisets nøyaktighet og fullstendighet er.
- Muligheten for at informasjon initieres eller endres på feil grunnlag, og at dette ikke oppdages, være større dersom hensiktsmessige kontroller ikke fungerer effektivt.

[59] ISA 330, punkt 8

Eksempel:

Det er vanligvis ikke mulig å innhente tilstrekkelig og hensiktsmessig revisjonsbevis knyttet til inntektene i en telekommunikasjonsenhet basert på substanshandlinger alene. Dette er fordi beviset for samtale- eller dataaktiviteten ikke eksisterer i en form som kan observeres. I stedet utføres vanligvis omfattende kontrolltesting for å fastsette at opprinnelsen til og varigheten av samtaler, og dataaktivitet, er riktig fanget opp (for eksempel minutter for en samtale eller mengde for en nedlasting) og riktig registrert i enhetens fakturasystem.

A225. ISA 540 (revidert) gir ytterligere veiledning knyttet til regnskapsestimater når det foreligger risikoer som substanshandlinger alene ikke kan gi tilstrekkelig og hensiktsmessig revisjonsbevis for.[60] I forbindelse med regnskapsestimater vil ikke dette nødvendigvis være begrenset til automatisert behandling, men kan også gjelde for komplekse modeller.

Vurdering av kontrollrisiko (Jf. punkt 34)

A226. Revisors planer om å teste om kontroller fungerer effektivt er basert på forventningen om at kontroller fungerer effektivt, og dette vil danne grunnlaget for revisors vurdering av kontrollrisiko. Den innledende forventningen til om kontroller fungerer effektivt er basert på revisors evaluering av utformingen, og fastsettelse av implementeringen, av de identifiserte kontrollene i komponenten «kontrollaktiviteter». Når revisor har testet om kontrollene fungerer effektivt i samsvar med ISA 330, vil revisor være i stand til å bekrefte den innledende forventningen til om kontroller fungerer effektivt. Dersom kontrollene ikke fungerer effektivt som forventet, må revisor revidere kontrollrisikovurderingen i samsvar med punkt 37.

A227. Revisors vurdering av kontrollrisiko kan utføres på forskjellige måter avhengig av foretrukne revisjonsteknikker eller -metodikker, og kan uttrykkes på forskjellige måter.

A228. Dersom revisor planlegger å teste om kontroller fungerer effektivt, kan det være nødvendig å teste en kombinasjon av kontroller for å bekrefte revisors forventning om at kontrollene fungerer effektivt. Revisor kan planlegge å teste både direkte og indirekte kontroller, herunder generelle IT-kontroller, og, i så fall, ta i betraktning den kombinerte forventede virkningen av kontrollene ved vurdering av kontrollrisiko. I den grad kontrollen som skal testes ikke fullt ut håndterer den anslåtte iboende risikoen, fastsetter revisor innvirkningen på utformingen av videre revisjonshandlinger for å redusere revisjonsrisiko til et akseptabelt lavt nivå.

A229. Når revisor planlegger å teste om en automatisert kontroll fungerer effektivt, kan revisor også planlegge å teste om de relevante generelle IT-kontrollene som underbygger den fortsatte funksjonen av denne automatiserte kontrollen for å håndtere risikoene som følger av bruken av IT fungerer effektivt, og for å gi grunnlag for revisors forventning om at den automatiserte kontrollen fungerte effektivt gjennom hele perioden. Når revisor forventer at tilhørende generelle IT-kontroller er ineffektive, kan denne forventningen påvirke revisors vurdering av kontrollrisiko på påstandsnivå, og

[60] ISA 540 (revidert), punkt A87–A89

det kan være behov for at revisors videre revisjonshandlinger inkluderer substanshandlinger for å håndtere de relevante risikoene som følger av bruken av IT. Ytterligere veiledning knyttet til handlingene som revisor kan utføre under slike omstendigheter, er gitt i ISA 330.[61]

Evaluering av revisjonsbeviset innhentet gjennom risikovurderingshandlinger (Jf. punkt 35)

Hvorfor revisor evaluerer revisjonsbeviset innhentet gjennom risikovurderingshandlingene

A230. Revisjonsbevis innhentet gjennom utførelse av risikovurderingshandlinger gir grunnlag for identifiseringen og vurderingen av risikoene for vesentlig feilinformasjon. Dette gir grunnlag for revisors utforming av typen, tidspunktet og omfanget av videre revisjonshandlinger som er tilpasset de anslåtte risikoene for vesentlig feilinformasjon på påstandsnivå, i samsvar med ISA 330. Revisjonsbeviset innhentet gjennom risikovurderingshandlingene gir følgelig grunnlag for identifiseringen og vurderingen av risikoer for vesentlig feilinformasjon, enten de skyldes misligheter eller feil, på regnskaps- og påstandsnivå.

Evalueringen av revisjonsbeviset

A231. Revisjonsbevis innhentet gjennom risikovurderingshandlinger omfatter både informasjon som underbygger og bekrefter ledelsens påstander, og eventuell informasjon som motsier disse påstandene.[62]

Profesjonell skepsis

A232. Ved evaluering av revisjonsbeviset innhentet gjennom risikovurderingshandlingene, vurderer revisor hvorvidt det er opparbeidet en tilstrekkelig forståelse av enheten og dens omgivelser, det gjeldende rammeverket for finansiell rapportering og enhetens internkontrollsystem til å kunne identifisere risikoene for vesentlig feilinformasjon, og hvorvidt det foreligger motstridende bevis som kan tyde på en risiko for vesentlig feilinformasjon.

Transaksjonsklasser, kontosaldoer og tilleggsopplysninger som ikke er signifikante, men som er vesentlige (Jf. punkt 36)

A233. Som forklart i ISA 320,[63] blir vesentlighet og revisjonsrisiko vurdert ved identifisering og vurdering av risikoene for vesentlig feilinformasjon i transaksjonsklasser, kontosaldoer og tilleggsopplysninger. Revisors fastsettelse av vesentlighet er gjenstand for profesjonelt skjønn, og påvirkes av revisors oppfatning av hvilke behov for finansiell informasjon brukerne av regnskapet har.[64] For formålet med denne ISA-en og punkt 18 i ISA 330 er transaksjonsklasser, kontosaldoer eller tilleggsopplysninger vesentlige dersom det faktum at informasjon om dem utelates, feilrapporteres eller tilsløres, rimelig

[61] ISA 330, punkt A29–A30

[62] ISA 500, punkt A1

[63] ISA 320, punkt A1

[64] ISA 320, punkt 4

kan forventes å påvirke de økonomiske beslutningene som treffes av brukerne på grunnlag av regnskapet sett under ett.

A234. Det kan være at det finnes transaksjonsklasser, kontosaldoer eller tilleggsopplysninger som er vesentlige, men som ikke er vurdert til å være signifikante transaksjonsklasser, kontosaldoer eller tilleggsopplysninger (dvs. at ingen relevante påstander er identifisert).

> **Eksempel**:
>
> Enheten kan ha en tilleggsopplysning om godtgjørelse til ledelsen der revisor ikke har identifisert en risiko for vesentlig feilinformasjon. Revisor kan imidlertid fastsette at denne tilleggsopplysningen er vesentlig basert på vurderingene i punkt A233.

A235. Revisjonshandlinger som skal håndtere transaksjonsklasser, kontosaldoer eller tilleggsopplysninger som er vesentlige, men som ikke er vurdert til å være signifikante, er beskrevet i ISA 330.[65] Når en transaksjonsklasse, kontosaldo eller tilleggsopplysning er vurdert til å være signifikant i samsvar med punkt 29, er transaksjonsklassen, kontosaldoen eller tilleggsopplysningen også en vesentlig transaksjonsklasse, kontosaldo eller tilleggsopplysning for formålene i punkt 18 i ISA 330.

Revidering av risikovurdering (Jf. punkt 37)

A236. Under revisjonen kan revisor bli oppmerksom på ny eller annen informasjon som avviker vesentlig fra den informasjonen som ligger til grunn for risikovurderingen.

> **Eksempel**:
>
> Enhetens risikovurdering kan være basert på en forventning om at bestemte kontroller fungerer effektivt. Ved gjennomføring av tester av disse kontrollene kan revisor innhente revisjonsbevis for at kontrollene ikke fungerte effektivt på relevante tidspunkter i løpet av revisjonen. Tilsvarende kan revisor ved gjennomføring av substanshandlinger avdekke feilinformasjon som er mer omfattende eller hyppigere enn det som er i samsvar med revisors risikovurderinger. Under slike omstendigheter kan det være at risikovurderingen ikke gjenspeiler de faktiske omstendighetene i enheten på en tilfredsstillende måte, og at de planlagte videre revisjonshandlingene ikke er hensiktsmessige for å avdekke vesentlig feilinformasjon. Punkt 16 og 17 i ISA 330 gir ytterligere veiledning knyttet til evaluering av om kontroller fungerer effektivt.

Dokumentasjon (Jf. punkt 38)

A237. Ved løpende revisjonsoppdrag kan deler av dokumentasjonen overføres og oppdateres etter behov for å gjenspeile endringer i enhetens forretningsvirksomhet eller prosesser.

A238. ISA 230 angir blant annet at selv om det ikke finnes en enkelt måte å dokumentere revisors utøvelse av profesjonell skepsis på, kan revisjonsdokumentasjonen likevel gi bevis for revisors utøvelse av

[65] ISA 330, punkt 18

profesjonell skepsis.[66] For eksempel, når revisjonsbeviset innhentet gjennom risikovurderingshandlinger omfatter bevis som både bekrefter og motsier ledelsens påstander, kan dokumentasjonen inkludere hvordan revisor har evaluert dette beviset, herunder de profesjonelle skjønnsmessige vurderingene som er foretatt for å evaluere hvorvidt revisjonsbeviset gir et hensiktsmessig grunnlag for revisors identifisering og vurdering av risikoene for vesentlig feilinformasjon. Eksempler på andre krav i denne ISA-en der dokumentasjon kan gi bevis for revisors utøvelse av profesjonell skepsis, inkluderer:

- Punkt 13, som krever at revisor utformer og utfører risikovurderingshandlinger på en måte som ikke tenderer mot å innhente revisjonsbevis som kan bekrefte eksistensen av risikoer, eller mot å ekskludere revisjonsbevis som kan motsi eksistensen av risikoer;
- Punkt 17, som krever en diskusjon blant sentrale medlemmer av revisjonsteamet om anvendelsen av det gjeldende rammeverket for finansiell rapportering og eksponeringen av enhetens regnskap for vesentlig feilinformasjon;
- Punkt 19(b) og 20, som krever at revisor opparbeider seg en forståelse av årsakene til eventuelle endringer i enhetens regnskapspolicyer, og evaluerer hvorvidt enhetens regnskapspolicyer er hensiktsmessige og overensstemmende med det gjeldende rammeverket for finansiell rapportering;
- Punkt 21(b), 22(b), 23(b), 24(c), 25(c), 26(d) og 27, som krever at revisor evaluerer, basert på den påkrevde forståelsen som er opparbeidet, hvorvidt komponentene i enhetens internkontrollsystem er hensiktsmessige ut fra enhetens omstendigheter tatt i betraktning enhetens type og kompleksitet, og fastsetter hvorvidt en eller flere kontrollmangler er identifisert;
- Punkt 35, som krever at revisor tar i betraktning alt revisjonsbevis som er innhentet gjennom risikovurderingshandlingene, uansett om det bekrefter eller motsier påstander fra ledelsen, og evaluerer hvorvidt revisjonsbeviset innhentet gjennom risikovurderingshandlingene gir et hensiktsmessig grunnlag for identifiseringen og vurderingen av risikoene for vesentlig feilinformasjon; og
- Punkt 36, som krever at revisor evaluerer, der det er relevant, hvorvidt revisors fastsettelse av at det ikke foreligger noen risikoer for vesentlig feilinformasjon for en vesentlig transaksjonsklasse, kontosaldo eller tilleggsopplysning, fortsatt er hensiktsmessig.

Skalerbarhet

A239. På hvilken måte kravene i punkt 38 dokumenteres, fastsettes av revisor ved anvendelse av profesjonelt skjønn.

A240. Mer detaljert dokumentasjon, som er tilstrekkelig til at en erfaren revisor som ikke har noen tidligere tilknytning til revisjonsoppdraget forstår typen, tidspunktet og omfanget av de utførte

[66] ISA 230, punkt A7

revisjonshandlingene, kan være nødvendig for å underbygge begrunnelsen for vanskelige skjønnsmessige vurderinger som er foretatt.

A241. Ved revisjon av mindre komplekse enheter kan dokumentasjonen være mindre omfattende og ha en enkel og relativt kortfattet form. Formen på og omfanget av revisors dokumentasjon påvirkes av typen, størrelsen og kompleksiteten av enheten og dens internkontrollsystem, tilgjengeligheten av informasjon fra enheten og revisjonsmetodologien og -teknologien som benyttes under revisjonen. Det er ikke nødvendig å dokumentere hele revisors forståelse av enheten og tilknyttede forhold. Viktige elementer[67] i forståelsen som dokumenteres av revisor, omfatter de elementene som revisor har lagt til grunn for vurderingen av risikoene for vesentlig feilinformasjon. Det kreves imidlertid ikke at revisor dokumenterer hver iboende risikofaktor som er tatt i betraktning ved identifiseringen og vurderingen av risikoene for vesentlig feilinformasjon på påstandsnivå.

Eksempel:

Ved revisjon av mindre komplekse enheter kan revisjonsdokumentasjonen integreres i revisors dokumentasjon av den overordnede strategien og revisjonsplanen.[68] Likeledes kan for eksempel resultatene av risikovurderingen dokumenteres separat, eller som en del av revisors dokumentasjon av videre revisjonshandlinger.[69]

[67] ISA 230, punkt 8

[68] ISA 300 *Planlegging av revisjon av et regnskap*, punkt 7, 9 og A11

[69] ISA 330, punkt 28

Vedlegg 1

(Jf. punkt A61–A67)

Vurderinger knyttet til forståelsen av enheten og dens forretningsmodell

Dette vedlegget forklarer målene og omfanget av enhetens forretningsmodell og gir eksempler på forhold som revisor kan vurdere ved forståelse av enhetens aktiviteter som kan være inkludert i forretningsmodellen. Revisors forståelse av enhetens forretningsmodell, og hvordan den påvirkes av enhetens forretningsstrategi og forretningsmål, kan hjelpe revisor med å identifisere forretningsrisikoer som kan ha en virkning på regnskapet. I tillegg kan det hjelpe revisor med å identifisere risikoer for vesentlig feilinformasjon.

Mål og omfang av en enhets forretningsmodell

1. En enhets forretningsmodell beskriver hvordan en enhet vurderer for eksempel sin organisasjonsstruktur, drift eller omfang av aktiviteter, forretningsområder (herunder konkurrenter og deres kunder), prosesser, vekstmuligheter, globalisering, regulatoriske krav og teknologier. Enhetens forretningsmodell beskriver hvordan enheten skaper, bevarer og realiserer finansiell eller annen videre verdi for sine interessegrupper.

2. Strategier er metodene som ledelsen bruker for å nå enhetens mål, herunder hvordan enheten planlegger å håndtere risikoene og mulighetene den står overfor. En enhets strategier endres over tid av ledelsen for å svare på endringer i målene og i de interne og eksterne omstendighetene som enheten opererer i.

3. En beskrivelse av en forretningsmodell omfatter vanligvis:

   - Omfanget av enhetens aktiviteter, og hvorfor enheten utfører dem.
   - Enhetens struktur og skala for virksomheten.
   - Markedene eller de geografiske eller demografiske områdene, og deler av verdikjeden, som den opererer i, hvordan den er involvert i disse markedene eller områdene (hovedprodukter, kundesegmenter og distribusjonsmetoder), og på hvilket grunnlag den konkurrerer.
   - Enhetens forretnings- eller driftsprosesser (for eksempel investerings-, finansierings- eller driftsprosesser) som benyttes i forbindelse med gjennomføringen av aktivitetene, med fokus på de delene av forretningsprosessene som er viktige for å skape, bevare eller realisere verdi.
   - Ressursene (for eksempel finansielle, menneskelige, intellektuelle, miljømessige og teknologiske) og andre inngangsfaktorer og relasjoner (for eksempel kunder, konkurrenter, leverandører og ansatte) som er nødvendige eller viktige for enhetens suksess.
   - Hvordan enhetens forretningsmodell integrerer bruken av IT i sine interaksjoner med kunder, leverandører, långivere og andre interessegrupper gjennom IT-grensesnitt og andre teknologier.

4. En forretningsrisiko kan ha en umiddelbar konsekvens for risikoen for vesentlig feilinformasjon for transaksjonsklasser, kontosaldoer og tilleggsopplysninger på påstandsnivå eller regnskapsnivå. For eksempel, forretningsrisikoen som oppstår som følge av et betydelig fall i prisene på eiendomsmarkedet, kan øke risikoen for vesentlig feilinformasjon forbundet med verdsettelsespåstanden for en långiver av lån med sikkerhet i eiendom på middels lang sikt. Den samme risikoen, særlig i kombinasjon med en alvorlig økonomisk nedgang som samtidig øker den underliggende risikoen for livsvarig kredittap på sine lån, kan imidlertid også ha en konsekvens på lengre sikt. Den resulterende nettoeksponeringen for kredittap kan skape tvil av betydning om enhetens evne til fortsatt drift. I så fall vil dette kunne ha en innvirkning på ledelsens, og revisors, konklusjon om hensiktsmessigheten ved enhetens bruk av forutsetningen om fortsatt drift, og fastsettelse av hvorvidt det foreligger en vesentlig usikkerhet. Hvorvidt en forretningsrisiko kan medføre en risiko for vesentlig feilinformasjon blir derfor vurdert i lys av enhetens omstendigheter. Eksempler på hendelser og forhold som kan føre til eksistensen av risikoer for vesentlig feilinformasjon, er beskrevet i **Vedlegg 2**.

Enhetens aktiviteter

5. Eksempler på forhold som revisor kan vurdere når revisor opparbeider seg en forståelse av enhetens aktiviteter (inkludert i enhetens forretningsmodell), omfatter:

   (a) Forretningsvirksomhet – for eksempel:

   - Typen inntektskilder, produkter eller tjenester, og markeder, herunder deltakelse i elektronisk handel, for eksempel salg- og markedsføringsaktiviteter på Internett.
   - Gjennomføring av driften (for eksempel produksjonstrinn og -metoder, eller aktivitetkan inneholde miljørisikoer).
   - Allianser, felleskontrollert virksomhet og utkontrakteringsaktiviteter.
   - Geografisk spredning og bransjemessig segmentering.
   - Lokalisering av produksjonsanlegg, lagre og kontorer, og lokalisering av og størrelse på varelager.
   - Viktige kunder og viktige leverandører av varer og tjenester, ansettelsesforhold (herunder eksistens av fagforeningsavtaler, pensjonsordninger, opsjons- eller bonusordninger og statlige regulativer knyttet til ansettelsesforhold).
   - Forsknings- og utviklingsaktiviteter og tilknyttede kostnader.
   - Transaksjoner med nærstående parter.

   (b) Investeringer og investeringsaktiviteter – for eksempel:

   - Planlagte eller nylig gjennomførte oppkjøp eller salg av virksomhet.
   - Investeringer i og salg av verdipapirer og lån.
   - Investeringer i varige driftsmidler.

- Investeringer i ikke-konsoliderte enheter, herunder ikke-kontrollerte partnerskap, felleskontrollert virksomhet og ikke-kontrollerte enheter med avgrenset formål.

(c) Finansiering og finansieringsaktiviteter – for eksempel:

- Eierstruktur for viktige datterselskaper og tilknyttede enheter, herunder konsoliderte og ikke-konsoliderte strukturer.
- Gjeldsstruktur og tilknyttede vilkår, herunder ikke-balanseførte finansieringsordninger og leasingavtaler.
- Eiere med rett til utbytte (for eksempel lokale, utenlandske, renommé og erfaring i bransjen) og nærstående parter.
- Bruk av finansielle derivater.

Egenskaper ved enheter med avgrenset formål

6. En enhet med avgrenset formål (noen ganger referert til som et spesialforetak) er en enhet som vanligvis opprettes for et smalt og klart definert formål, for eksempel for å gjennomføre utleie eller verdipapirisering av finansielle eiendeler, eller for å utføre forsknings- og utviklingsaktiviteter. Den kan opprettes i form av et selskap, en stiftelse, et forretningsfellesskap eller et ansvarlig selskap eller annet formalisert samarbeid. Enheten som enheten med avgrenset formål er opprettet på vegne av, kan ofte overføre eiendeler til sistnevnte (for eksempel som et ledd i fraregning av finansielle eiendeler i balansen), ha rett til å bruke sistnevntes eiendeler eller utføre tjenester for sistnevnte, mens andre parter kan sørge for finansiering av sistnevnte. Som angitt i ISA 550, kan en enhet med avgrenset formål under enkelte omstendigheter være en nærstående part til enheten.[70]

7. Rammeverk for finansiell rapportering spesifiserer ofte detaljert hvilke forhold som anses å utgjøre kontroll, eller under hvilke omstendigheter det bør vurderes å konsolidere enheten med avgrenset formål. Tolkningen av kravene i disse rammeverkene krever ofte inngående kjennskap til de relevante avtalene som gjelder for enheten med avgrenset formål.

[70] ISA 550, punkt A7

Vedlegg 2

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

Forståelse av iboende risikofaktorer

Dette vedlegget gir en ytterligere beskrivelse av de iboende risikofaktorene samt forhold som revisor kan vurdere når revisor opparbeider seg en forståelse av og anvender de iboende risikofaktorene ved identifisering og vurdering av risikoene for vesentlig feilinformasjon på påstandsnivå.

De iboende risikofaktorene

1. Iboende risikofaktorer er særtrekk ved hendelser eller forhold som påvirker i hvilken grad en påstand om en transaksjonsklasse, kontosaldo eller tilleggsopplysning kan inneholde feilinformasjon, enten det skyldes misligheter eller feil, før kontroller tas i betraktning. Slike faktorer kan være kvalitative eller kvantitative, og omfatter kompleksitet, subjektivitet, endring, usikkerhet eller mulig feilinformasjon som følge av manglende objektivitet hos ledelsen eller andre mislighetsrisikofaktorer[71] i den grad de påvirker iboende risiko. Ved opparbeidelsen av en forståelse av enheten og dens omgivelser, og det gjeldende rammeverket for finansiell rapportering og enhetens regnskapspolicyer, i samsvar med punkt 19(a)–(b), opparbeider revisor seg også en forståelse av hvordan iboende risikofaktorer påvirker påstanders mulighet for feilinformasjon ved utarbeidelsen av regnskapet.

2. Iboende risikofaktorer knyttet til utarbeidelsen av informasjon som kreves av det gjeldende rammeverket for finansiell rapportering (referert til i dette punktet som «nødvendig informasjon»), omfatter:

   - *Kompleksitet* – oppstår som følge av enten typen informasjon eller måten den nødvendige informasjonen er utarbeidet på, herunder når slike utarbeidelsesprosesser er mer iboende vanskelige å anvende. Kompleksitet kan for eksempel oppstå:

     - Ved beregning av avsetninger for leverandørrabatt, ettersom det kan være nødvendig å ta i betraktning forskjellige forretningsvilkår med mange forskjellige leverandører, eller mange innbyrdes forhold mellom forretningsvilkårene som alle er relevante ved beregning av rabattene som er gitt; eller

     - Når det er mange potensielle datakilder, og forskjellige særtrekk er benyttet ved utarbeidelsen av et regnskapsestimat, omfatter behandlingen av disse dataene mange trinn som er innbyrdes forbundet, og dataene er derfor iboende mer vanskelige å identifisere, fange opp, få tilgang til, forstå eller behandle.

   - *Subjektivitet* – oppstår som følge av iboende begrensninger i evnen til å utarbeide nødvendig informasjon på en objektiv måte, som følge av begrensninger i tilgjengeligheten av kunnskap eller informasjon, slik at ledelsen kan bli nødt til å foreta et valg eller en subjektiv vurdering av hvilken tilnærming de skal velge og hvilken resulterende informasjon som skal tas med i

[71] ISA 240, punkt A24–A27

regnskapet. På grunn av forskjellige tilnærminger til utarbeidelsen av den nødvendige informasjonen, kan utfallene bli forskjellige selv om anvendelsen av kravene i det gjeldende rammeverket for finansiell rapportering er riktig. Etter hvert som begrensninger i kunnskap eller data øker, vil også subjektiviteten i de skjønnsmessige vurderingene som kan bli foretatt av rimelig kunnskapsrike og uavhengige personer, og ulikheten i vurderingenes mulige utfall, øke.

- *Endringer* – følger av hendelser eller forhold som over tid påvirker enhetens virksomhet eller de økonomiske, regnskapsmessige, regulatoriske, bransjemessige eller andre aspektene ved omgivelsene som enheten opererer i, når virkningene av disse hendelsene eller forholdene gjenspeiles i den nødvendige informasjonen. Slike hendelser eller forhold kan forekomme i løpet av, eller mellom, perioder for finansiell rapportering. Endringer kan for eksempel følge av en utvikling av kravene i det gjeldende rammeverket for finansiell rapportering, eller av enheten og dens forretningsmodell, eller av miljøet som enheten opererer i. Slike endringer kan påvirke ledelsens forutsetninger og skjønnsmessige vurderinger, herunder i forhold til ledelsens valg av regnskapspolicyer eller hvordan regnskapsestimater er utarbeidet eller tilhørende tilleggsopplysninger er fastsatt.
- *Usikkerhet* – oppstår når den nødvendige informasjonen ikke kan utarbeides utelukkende basert på tilstrekkelig presise og omfattende data som kan verifiseres gjennom direkte observasjon. Under disse omstendighetene kan det være behov for å velge en tilnærming som anvender den tilgjengelige kunnskapen for å utarbeide informasjonen ved bruk av tilstrekkelig presise og omfattende observerbare data, i den utstrekning de er tilgjengelige, og rimelige forutsetninger som underbygges av de mest hensiktsmessige dataene som er tilgjengelige, når dette ikke er tilfellet. Begrensninger i tilgjengeligheten av kunnskap eller data som er utenfor ledelsens kontroll (gjenstand for kostnadsbegrensninger der det er relevant), er kilder til usikkerhet, og deres virkning på utarbeidelsen av den nødvendige informasjonen kan ikke elimineres. For eksempel oppstår estimeringsusikkerhet når et nødvendig pengebeløp ikke kan fastsettes med presisjon, og utfallet av estimatet ikke er kjent før datoen for sluttføring av regnskapet.
- *Mulig feilinformasjon som følge av manglende objektivitet hos ledelsen eller andre mislighetsrisikofaktorer i den grad de påvirker iboende risiko* – mulig manglende objektivitet hos ledelsen følger av forhold som gir mulighet for at ledelsen, tilsiktet eller utilsiktet, ikke opprettholder nøytralitet ved utarbeidelsen av informasjonen. Manglende objektivitet hos ledelsen er ofte knyttet til visse forhold som har potensialet til å medføre at ledelsen ikke opprettholder nøytralitet ved utøvelse av skjønn (indikatorer for potensiell manglende objektivitet hos ledelsen), som kan føre til vesentlig feilinformasjon i informasjonen som ville ha vært uredelig dersom den var tilsiktet. Slike indikatorer omfatter incentiver eller press i den grad de påvirker iboende risiko (for eksempel som følge av motivasjonen for å oppnå et ønsket profittmål eller kapitalforhold), og mulighet for ikke å opprettholde nøytralitet. Faktorer som er relevante for eksponeringen for feilinformasjon som følge av misligheter i form av uredelig finansiell rapportering eller underslag av eiendeler, er beskrevet i punkt A1 til A5 i ISA 240.

3. Når kompleksitet er en iboende risikofaktor, kan det være et iboende behov for mer komplekse prosesser ved utarbeidelse av informasjonen, og slike prosesser kan være iboende mer vanskelige å anvende. Som følge av dette kan anvendelsen av dem kreve spesialistferdigheter eller -kunnskaper, og kan kreve bruk av en ledelsens ekspert.

4. Når ledelsens skjønn er mer subjektivt, kan også eksponeringen for feilinformasjon som følge av manglende objektivitet hos ledelsen, enten den er tilsiktet eller utilsiktet, øke. Ledelsen kan for eksempel ha anvendt betydelig skjønn ved utarbeidelsen av regnskapsestimater som er identifisert til å ha høy estimeringsusikkerhet, og konklusjoner om metoder, data og forutsetninger kan utilsiktet eller tilsiktet gjenspeile ledelsens skjønn.

Eksempler på hendelser og forhold som kan medføre at det foreligger risikoer for vesentlig feilinformasjon

5. Nedenfor følger eksempler på hendelser (herunder transaksjoner) og forhold som kan tyde på at det foreligger risikoer for vesentlig feilinformasjon i regnskapet på regnskapsnivå eller påstandsnivå. Eksemplene er gitt etter iboende risikofaktor og dekker et bredt spekter av hendelser og forhold. Det er imidlertid ikke alle hendelser og forhold som er relevante for alle revisjonsoppdrag, og listen med eksempler er ikke nødvendigvis uttømmende. Hendelsene og forholdene er kategorisert etter den iboende risikofaktoren som kan ha størst virkning under omstendighetene. Et annet viktig poeng er at, som følge av de innbyrdes forholdene mellom iboende risikofaktorer, vil også eksemplene på hendelser og forhold være gjenstand for, eller påvirket av, andre iboende risikofaktorer i varierende grad.

Relevant iboende risikofaktor:	Eksempler på hendelser og forhold som kan tyde på at det foreligger risikoer for vesentlig feilinformasjon på påstandsnivå:
Kompleksitet	Regulatorisk: • Virksomhet som er underlagt et svært komplekst regelverk. Forretningsmodell: • Eksistens av komplekse allianser og felleskontrollert virksomhet. Gjeldende rammeverk for finansiell rapportering: • Regnskapsmessige målinger basert på komplekse prosesser. Transaksjoner: • Anvendelse av finansiering utenom balansen (off-balance-sheet), enheter med avgrenset formål og andre komplekse finansieringsordninger.
Subjektivitet	Gjeldende rammeverk for finansiell rapportering:

Relevant iboende risikofaktor:	Eksempler på hendelser og forhold som kan tyde på at det foreligger risikoer for vesentlig feilinformasjon på påstandsnivå:
	• Et bredt utvalg av mulige målingskriterier for et regnskapsestimat. For eksempel, ledelsens innregning av avskrivning eller inntekter og utgifter knyttet til bygging. • Ledelsens valg av en verdsettelsesteknikk eller -modell for et anleggsmiddel, for eksempel investeringseiendommer.
Endringer	Økonomiske forhold: • Virksomhet i regioner som er økonomisk ustabile, for eksempel land med betydelig valutadevaluering eller høy inflasjon. Markeder: • Virksomhet i volatile markeder, for eksempel terminhandel. Kundetap: • Forhold vedrørende forutsetning om fortsatt drift og likviditetsproblemer, herunder tap av viktige kunder. Bransjemodell: • Endringer i bransjen enheten opererer i. Forretningsmodell: • Endringer i leverandørkjeden. • Utvikling eller salg av nye produkter eller tjenester, eller inntreden i nye forretningsområder. Geografi: • Utvidelse av virksomheten til nye geografiske områder. Enhetsstruktur: • Endringer i enheten, for eksempel store oppkjøp eller omorganiseringer eller andre uvanlige hendelser. • Sannsynlighet for salg av enheter eller forretningssegmenter. HR-kompetanse: • Utskifting av nøkkelpersonell, herunder sentrale ledere. IT: • Endringer i IT-miljøet.

Relevant iboende risikofaktor:	Eksempler på hendelser og forhold som kan tyde på at det foreligger risikoer for vesentlig feilinformasjon på påstandsnivå:
	• Innføring av vesentlige nye IT-systemer knyttet til finansiell rapportering. Gjeldende rammeverk for finansiell rapportering: • Anvendelse av nye regnskapsregler. Kapital: • Nye begrensninger på tilgangen på kapital og kreditt. Regulatorisk: • Tilsyns- eller andre offentlige myndigheters undersøkelse av enhetens drift eller finansielle resultater. • Konsekvenser av ny lovgivning knyttet til miljøbeskyttelse.
Usikkerhet	Rapportering: • Hendelser eller transaksjoner som involverer vesentlig målingsusikkerhet, herunder regnskapsestimater, og tilhørende tilleggsopplysninger. • Pågående rettssaker og betingede forpliktelser, for eksempel salgsgarantier, finansielle garantier og miljøtiltak.
Mulig feilinformasjon som følge av manglende objektivitet hos ledelsen eller andre mislighetsrisikofaktorer i den grad de påvirker iboende risiko	Rapportering: • Muligheter for ledelse og ansatte til å delta i uredelig finansiell rapportering, herunder utelatelse, eller tilsløring, av informasjon av betydning i tilleggsopplysninger. Transaksjoner: • Vesentlige transaksjoner med nærstående parter. • Vesentlig mengde ikke-rutinemessige eller ikke-systematiske transaksjoner, herunder konserninterne transaksjoner og store inntektstransaksjoner ved regnskapsperiodens slutt. • Transaksjoner som er registrert basert på ledelsens intensjon, for eksempel refinansiering av gjeld, eiendeler som skal selges og klassifisering av omsettelige verdipapirer.

Andre hendelser og forhold som kan tyde på risikoer for vesentlig feilinformasjon på regnskapsnivå:

- Mangel på personell med tilstrekkelige ferdigheter innenfor regnskap og finansiell rapportering.

- Kontrollmangler – særlig i kontrollmiljøet, risikovurderingsprosessen og prosessen for overvåking, og særlig de som ikke håndteres av ledelsen.
- Tidligere feilinformasjon, tidligere feil eller en vesentlig mengde justeringer ved regnskapsperiodens slutt.

Vedlegg 3

(Jf. punkt 12(m), 21–26, A90–A181)

Forståelse av enhetens internkontrollsystem

1. Enhetens internkontrollsystem kan gjenspeiles i håndbøker med retningslinjer og rutiner, systemer og skjemaer, og informasjonen i dem, og er utarbeidet av mennesker. Enhetens internkontrollsystem implementeres av ledelsen, dem som har overordnet ansvar for styring og kontroll og annet personale basert enhetens struktur. Enhetens internkontrollsystem kan, basert på beslutningene til ledelsen, dem som har overordnet ansvar for styring og kontroll eller annet personale, og i kontekst av juridiske eller regulatoriske krav, anvendes på enhetens forretningsmodell, enhetens juridiske struktur, eller en kombinasjon av de to.

2. Dette vedlegget gir en mer detaljert beskrivelse av komponentene, så vel som begrensningene, i enhetens internkontrollsystem, som angitt i punkt 12(m), 21–26 og A90–A181, i forhold til revisjon av regnskaper.

3. Enhetens internkontrollsystem omfatter aspekter som er knyttet til enhetens rapporteringsmål, herunder enhetens mål for finansiell rapportering, men kan også omfatte aspekter som er knyttet til enhetens mål for drift eller overholdelse av lover og forskrifter, når slike aspekter er relevante for finansiell rapportering.

> **Eksempel**:
>
> Kontroller knyttet til overholdelse av lover og forskrifter kan være relevante for finansiell rapportering når disse kontrollene er relevante for enhetens utarbeidelse av tilleggsopplysninger om latente forhold i regnskapet.

Komponenter i enhetens internkontrollsystem

Kontrollmiljø

4. Kontrollmiljøet omfatter styrings-, kontroll- og ledelsesfunksjoner samt holdningene, bevisstheten og handlingene til dem som har overordnet ansvar for styring og kontroll samt ledelsen med hensyn til enhetens internkontrollsystem og dets betydning i enheten. Kontrollmiljøet setter tonen i en organisasjon og påvirker personells kontrollbevissthet, og gir et overordnet grunnlag for driften av de andre komponentene i enhetens internkontrollsystem.

5. En enhets kontrollbevissthet påvirkes av dem som har overordnet ansvar for styring og kontroll, ettersom en av deres oppgaver er å balansere presset på ledelsen i forbindelse med finansiell rapportering som kan oppstå som følge av markedskrav eller godtgjørelsesordninger. Hvor effektivt utformingen av kontrollmiljøet fungerer i forhold til deltakelsen av dem som har overordnet ansvar for styring og kontroll, påvirkes derfor av forhold som for eksempel:

- Deres uavhengighet fra ledelsen og deres evne til å evaluere ledelsens handlinger.
- Hvorvidt de forstår enhetens forretningstransaksjoner.
- I hvilken grad de evaluerer om regnskapet er utarbeidet i samsvar med det gjeldende rammeverket for finansiell rapportering, herunder hvorvidt regnskapet inneholder adekvate tilleggsopplysninger.

6. Kontrollmiljøet omfatter følgende elementer:

(a) *Hvordan ledelsens oppgaver og plikter utføres, for eksempel hvordan ledelsen oppretter og vedlikeholder enhetens kultur og viser at den håndhever integritet og etiske verdier*. Kontrollens effektivitet kan ikke bli bedre enn integriteten og de etiske verdiene til de personene som utarbeider, administrerer og overvåker kontrollene. Integritet og etisk atferd er et resultat av enhetens standarder for etisk atferd eller regler for «god skikk», hvordan disse kommuniseres (for eksempel gjennom prinsipperklæringer) og hvordan de iverksettes (for eksempel gjennom ledelsens handlinger for å fjerne eller redusere motiver og fristelser som kan medføre at personell deltar i uærlige, ulovlige eller uetiske handlinger). Kommunikasjon av enhetens retningslinjer for integritet og etiske verdier kan omfatte kommunikasjon av etiske standarder til personell gjennom prinsipperklæringer, regler for «god skikk» og ved å gå foran med et godt eksempel.

(b) *Når de som har overordnet ansvar for styring og kontroll er atskilt fra ledelsen, hvordan de som har overordnet ansvar for styring og kontroll viser uavhengighet fra ledelsen og fører tilsyn med enhetens internkontrollsystem*. En enhets kontrollbevissthet påvirkes av dem som har overordnet ansvar for styring og kontroll. Vurderinger kan omfatte hvorvidt det er et tilstrekkelig antall personer som er uavhengige av ledelsen og objektive i sine evalueringer og beslutningstaking, hvordan de som har overordnet ansvar for styring og kontroll identifiserer og aksepterer tilsynsoppgaver, og hvorvidt de som har overordnet ansvar for styring og kontroll fører tilsyn med ledelsens utforming, implementering og gjennomføring av enhetens internkontrollsystem. Viktigheten av oppgavene og pliktene til dem som har overordnet ansvar for styring og kontroll, fremgår av regler for «god skikk» og andre lover og forskrifter eller veiledninger utarbeidet for dem som har overordnet ansvar for styring og kontroll. Øvrige oppgaver og plikter til dem som har overordnet ansvar for styring og kontroll, omfatter tilsyn med utformingen og måleffektiviteten av rutiner for varsling.

(c) *Hvordan enheten tildeler myndighet og ansvar for å oppfylle sine mål.* Dette kan omfatte vurderinger knyttet til:

- Viktige myndighets- og ansvarsområder og hensiktsmessige rapporteringskanaler;
- Retningslinjer for ansvarlig forretningspraksis, kunnskaper og erfaringer hos nøkkelpersonell og hvilke ressurser som stilles til rådighet for å utføre oppgaver; og
- Retningslinjer og kommunikasjon for å sikre at alle personell forstår enhetens mål, vet hvordan deres handlinger henger sammen med og bidrar til å oppfylle disse målene, og kjenner til hvordan og for hva de vil bli holdt ansvarlig.

(d) *Hvordan enheten tiltrekker, utvikler og beholder kompetente personer i tråd med sine mål.* Dette omfatter hvordan enheten sikrer at personene har de kunnskapene og ferdighetene som er nødvendige for å utføre de oppgavene som hører inn under en persons arbeidsoppgaver, for eksempel:

- Standarder for rekruttering av de best kvalifiserte personene – med vekt på utdanning, arbeidserfaring, tidligere oppnådde resultater og bevis på integritet og etisk atferd.
- Retningslinjer for opplæring som kommuniserer kommende oppgaver og ansvar, herunder kurs og seminarer som illustrerer forventninger til prestasjon og atferd; og
- Utvikling styrt av periodiske prestasjonsvurderinger som viser at enheten er opptatt av å utvikle kvalifiserte personell til høyere ansvarsnivåer.

(e) *Hvordan enheten holder personer ansvarlige for oppgaver de er tildelt for å oppfylle målene for enhetens internkontrollsystem.* Dette kan oppnås ved hjelp av for eksempel:

- Mekanismer for å kommunisere og holde personer ansvarlige for oppgaver knyttet til gjennomføring av kontroller, og implementere korrigerende tiltak når det er nødvendig;
- Etablere resultatmål, incentiver og belønninger for dem som er ansvarlige for enhetens internkontrollsystem, herunder hvordan måleparametrene evalueres og opprettholder sin relevans;
- Hvordan press forbundet med oppnåelsen av kontrollmål påvirker personens oppgaver og resultatmål; og
- Hvilke disiplinære reaksjoner som gis til personer når det er nødvendig.

Hvor hensiktsmessige de ovennevnte forholdene er, vil variere fra enhet til enhet, avhengig av enhetens størrelse, strukturens kompleksitet og typen aktiviteter.

Enhetens risikovurderingsprosess

7. Enhetens risikovurderingsprosess er en gjentakende prosess for å identifisere og analysere risikoer knyttet til oppnåelsen av enhetens mål, og danner grunnlaget for hvordan ledelsen eller dem som har overordnet ansvar for styring og kontroll fastsetter risikoene som skal håndteres.

8. Når det gjelder finansiell rapportering, omfatter enhetens risikovurderingsprosess hvordan ledelsen identifiserer forretningsrisikoer som er relevante for utarbeidelsen av regnskap i samsvar med enhetens gjeldende rammeverk for finansiell rapportering, anslår deres betydning, vurderer sannsynligheten for at de forekommer, og fastsetter tiltak for å håndtere dem og resultatene av dem. Enhetens risikovurderingsprosess kan for eksempel være rettet mot hvordan enheten vurderer muligheten for uregistrerte transaksjoner eller identifiserer og analyserer vesentlige estimater i regnskapet.

9. Risikoer som er relevante for den pålitelige finansielle rapporteringen, omfatter eksterne og interne hendelser, transaksjoner eller omstendigheter som kan forekomme og ha en negativ innvirkning på en enhets evne til å initiere, registrere, behandle og rapportere finansiell informasjon i

overensstemmelse med ledelsens påstander i regnskapet. Ledelsen kan initiere planer, programmer eller tiltak for å håndtere bestemte risikoer, eller den kan beslutte å akseptere en risiko av kostnadshensyn eller av andre grunner. Risikoer kan oppstå eller endres som følge av omstendigheter som nevnt nedenfor:

- *Endringer i enhetens omgivelser* Endringer i de regulatoriske, økonomiske eller driftsmessige omgivelsene kan føre til endringer i konkurransesituasjonen og et vesentlig endret risikobilde.
- *Nye personell*. Nye personell kan ha en annen vinkling på eller forståelse av enhetens internkontrollsystem.
- *Nytt eller oppdatert informasjonssystem*. Betydelige og raske endringer i informasjonssystemet kan endre risikoen knyttet til enhetens internkontrollsystem.
- *Rask vekst*. Betydelig og rask utvidelse av virksomheten kan overbelaste kontroller og øke risikoen for at kontrollene bryter sammen.
- *Ny teknologi*. Innføring av ny teknologi i produksjonsprosesser eller informasjonssystemet kan endre risikoen som er forbundet med enhetens internkontrollsystem.
- *Nye forretningsmodeller, produkter eller aktiviteter*. Nye forretningsområder eller transaksjoner som enheten har liten erfaring med, kan medføre nye risikoer forbundet med enhetens internkontrollsystem.
- *Restruktureringer*. Restruktureringer kan medføre reduksjon i antall personell og endringer i tilsyn og arbeidsdeling som kan endre risikoen forbundet med enhetens internkontrollsystem.
- *Utvidet virksomhet i utlandet*. Utvidelse eller oppkjøp av virksomhet i utlandet medfører nye og ofte unike risikoer som kan påvirke den interne kontrollen, for eksempel nye eller endrede risikoer i forbindelse med valutatransaksjoner.
- *Nye regnskapsregler*. Innføring av nye regnskapsprinsipper eller endringer i regnskapsprinsipper kan påvirke risikoer i forbindelse med utarbeidelse av regnskap.
- *Bruk av IT*. Risikoer knyttet til:
    - Vedlikehold av dataintegritet og informasjonsbehandling;
    - Risikoer for enhetens forretningsstrategi som oppstår dersom enhetens IT-strategi ikke underbygger enhetens forretningsstrategi på en effektiv måte; eller
    - Endringer eller forstyrrelser i enhetens IT-miljø eller utskifting av IT-personale, eller når enheten ikke gjør de nødvendige oppdateringene i IT-miljøet, eller disse oppdateringene ikke skjer i rett tid.

Enhetens prosess for overvåking av internkontrollsystemet

10. Enhetens prosess for overvåking av internkontrollsystemet er en kontinuerlig prosess for å evaluere effektiviteten av enhetens internkontrollsystem og iverksette nødvendige korrigerende tiltak i rett tid. Enhetens prosess for overvåking av enhetens internkontrollsystem kan bestå av løpende aktiviteter,

separate evalueringer (som gjennomføres regelmessig), eller en kombinasjon av de to. Løpende overvåkingsaktiviteter er ofte integrert i de normale rutinemessige aktivitetene i en enhet, og kan omfatte regelmessige ledelses- og tilsynsaktiviteter. Enhetens prosess vil ofte variere i omfang og hyppighet, avhengig av enhetens vurdering av risikoene.

11. Målene og ansvarsområdet til en internrevisjonsfunksjon omfatter vanligvis aktiviteter som er utformet for å evaluere eller overvåke effektiviteten av enhetens internkontrollsystem.[72] Enhetens prosess for overvåking av enhetens internkontrollsystem kan omfatte aktiviteter som for eksempel ledelsens gjennomgåelse av hvorvidt bankavstemminger utarbeides i rett tid, interne revisorers evaluering av salgspersonells overholdelse av enhetens retningslinjer for vilkår i salgskontrakter, og en juridisk avdelings tilsyn med at enhetens regler for etisk atferd eller ansvarlig forretningspraksis overholdes. Overvåking utføres også for å sikre at kontroller fungerer effektivt over tid. Dersom for eksempel bankavstemmingenes tidsriktighet og nøyaktighet ikke overvåkes, er det mulig at personell vil slutte å utarbeide dem.

12. Kontroller knyttet til enhetens prosess for overvåking av enhetens internkontrollsystem, herunder de som overvåker underliggende automatiserte kontroller, kan være automatiserte eller manuelle, eller en kombinasjon av de to. En enhet kan for eksempel bruke automatiserte overvåkingskontroller knyttet til tilgang til en bestemt teknologi med automatiserte rapporter av uvanlig aktivitet til ledelsen, som manuelt undersøker identifiserte uregelmessigheter.

13. Når man skiller mellom en overvåkingsaktivitet og en kontroll knyttet til informasjonssystemet, vurderer man aktivitetens underliggende detaljer, særlig når aktiviteten involverer et eller annet nivå av tilsynsgjennomgang. Tilsynsgjennomganger blir ikke automatisk klassifisert som overvåkingsaktiviteter, og det kan være et spørsmål om skjønn hvorvidt en gjennomgang blir klassifisert som en kontroll knyttet til informasjonssystemet eller en overvåkingsaktivitet. For eksempel vil formålet med en månedlig fullstendighetskontroll være å påvise og korrigere feil, mens en overvåkingsaktivitet vil stille spørsmål om hvorfor feil forekommer og gi ledelsen i oppgave å utbedre prosessen for å forebygge fremtidige feil. Litt forenklet kan man si at en kontroll knyttet til informasjonssystemet håndterer en bestemt risiko, mens en overvåkingsaktivitet vurderer hvorvidt kontroller innenfor hver av de fem komponentene i enhetens interne kontroll fungerer som tiltenkt.

14. Overvåkingsaktiviteter kan omfatte bruk av informasjon i kommunikasjoner fra eksterne parter som kan indikere problemer eller synliggjøre områder der det er behov for forbedring. Kunder gir indirekte bekreftelse på faktureringsdata ved å betale sine fakturaer eller klage på faktureringsbeløpet. I tillegg kan tilsynsmyndigheter kommunisere med enheten om forhold som påvirker funksjonen av enhetens internkontrollsystem, for eksempel i forbindelse med undersøkelser utført av banktilsynsmyndigheter. Ledelsen kan også ved gjennomføring av overvåkingsaktiviteter vurdere kommunikasjon fra eksterne revisorer vedrørende enhetens internkontrollsystem.

Informasjonssystemet og kommunikasjon

[72] ISA 610 (revidert 2013) og vedlegg 4 i denne ISA-en gir ytterligere veiledning knyttet til intern revisjon.

15. Informasjonssystemet som er relevant for utarbeidelsen av regnskapet, består av aktiviteter og retningslinjer samt regnskapsmateriale og underbyggende materiale som er utformet og etablert for å:

    - Initiere, registrere og behandle enhetens transaksjoner (samt fange opp, behandle og gi informasjon om hendelser og forhold ut over transaksjoner), og holde kontroll med tilknyttede eiendeler, forpliktelser og egenkapital;
    - Håndtere uriktig behandling av transaksjoner, for eksempel automatiserte ventefiler og rutiner som følges for å sikre at avviksposter avklares i rett tid;
    - Behandle og registrere overstyring eller omgåelse av kontroller;
    - Overføre informasjon fra transaksjonsbehandling til hovedboken (for eksempel overføre akkumulerte transaksjoner fra en reskontro);
    - Fange opp og behandle informasjon som er relevant for utarbeidelsen av regnskapet knyttet til hendelser og forhold ut over transaksjoner, for eksempel avskrivning og amortisering av eiendeler og endringer i kundefordringers erholdelighet; og
    - Sikre at informasjon som det er påkrevd å opplyse om i henhold til det gjeldende rammeverket for finansiell rapportering, samles inn, registreres, behandles, summeres og rapporteres på en tilfredsstillende måte i regnskapet.

16. En enhets forretningsprosesser omfatter de aktivitetene som er utformet for å:

    - Utvikle, kjøpe, produsere, selge og distribuere en enhets produkter og tjenester;
    - Sikre overholdelse av lover og forskrifter; og
    - Registrere informasjon, herunder informasjon forbundet med regnskap og finansiell rapportering.

    Forretningsprosesser resulterer i transaksjoner som registreres, behandles og rapporteres av informasjonssystemet.

17. Kvaliteten på informasjon påvirker ledelsens evne til å ta hensiktsmessige beslutninger i forbindelse med styring og kontroll av enhetens aktiviteter, og til å utarbeide pålitelige finansielle rapporter.

18. Kommunikasjon, som innebærer å formidle en forståelse av individuelle roller og ansvar som er relevante for enhetens internkontrollsystem, kan skje i form av håndbøker med retningslinjer, håndbøker for regnskap og finansiell rapportering samt notater. Kommunikasjon kan også skje elektronisk, muntlig og gjennom ledelsens handlinger.

19. Enhetens kommunikasjon av roller og ansvar knyttet til finansiell rapportering, og av vesentlige forhold knyttet til finansiell rapportering, innebærer å opparbeide seg en forståelse av individuelle roller og ansvar knyttet til enhetens internkontrollsystem som er relevant for finansiell rapportering. Det kan omfatte forhold som i hvilken grad ansatte forstår hvordan deres arbeidsoppgaver innenfor informasjonssystemet henger sammen med andres arbeidsoppgaver, og hva som er fremgangsmåten for å rapportere avvik til riktig overordnet instans i enheten.

Kontrollaktiviteter

20. Kontroller i komponenten «kontrollaktiviteter» identifiseres i samsvar med punkt 26. Slike kontroller omfatter informasjonsbehandlingskontroller og generelle IT-kontroller, som begge kan være manuelle eller automatiserte av natur. Jo større omfang av automatiserte kontroller, eller kontroller som involverer automatiserte aspekter, ledelsen bruker og bygger på i forbindelse med finansiell rapportering, desto viktigere kan det være for enheten å implementere generelle IT-kontroller som er rettet mot den fortsatte funksjonen av de automatiserte aspektene ved informasjonsbehandlingskontroller. Kontroller i komponenten «kontrollaktiviteter» kan være knyttet til følgende:

- *Autorisasjon og godkjenninger*. En autorisasjon bekrefter at en transaksjon er gyldig (dvs. at den representerer en faktisk økonomisk hendelse eller er innenfor en enhets retningslinjer). En autorisasjon skjer vanligvis i form av en godkjenning på et høyere ledelsesnivå, eller av en verifisering og en bekreftelse dersom transaksjonen er gyldig. En overordnet kan for eksempel godkjenne en utgiftsrapport etter gjennomgåelse av hvorvidt utgiftene virker rimelige og er innenfor retningslinjene. Et eksempel på en automatisert godkjenning er når en fakturert enhetskostnad automatisk sammenlignes med den tilhørende enhetskostnaden på innkjøpsordren innenfor et forhåndsdefinert toleransenivå. Fakturaer innenfor toleransenivået godkjennes automatisk og legges til betaling. Fakturaer utenfor toleransenivået flagges med sikte på ytterligere undersøkelse.
- *Avstemminger* – Avstemminger sammenligner to eller flere dataelementer. Dersom avvik identifiseres, iverksettes det tiltak for å bringe dataene i samsvar. Avstemminger er vanligvis rettet mot fullstendigheten og nøyaktigheten av behandling av transaksjoner.
- *Verifiseringer* – Verifiseringer sammenligner to eller flere elementer med hverandre, eller et element med en retningslinje, og involverer som regel et oppfølgingstiltak når to elementer ikke stemmer overens eller når elementet ikke er i henhold til retningslinjen. Verifiseringer er vanligvis rettet mot fullstendigheten, nøyaktigheten eller gyldigheten av behandling av transaksjoner.
- *Fysiske eller logiske kontroller, herunder de som er rettet mot sikring av eiendeler mot uautorisert tilgang, anskaffelse, bruk eller avhending.* Kontroller som omfatter:
    - Fysisk sikring av eiendeler, herunder egnede sikringstiltak, for eksempel begrensning av fysisk adgang til eiendeler og regnskapsmateriale.
    - Autorisasjon for tilgang til dataprogrammer og datafiler (dvs. logisk tilgang).
    - Periodisk telling og sammenligning med beløp i registre (for eksempel sammenligning av resultatet av telling av kontanter, verdipapirer og varelagre med regnskapsmaterialet).

  I hvilken grad fysiske kontroller for å forhindre tyveri av eiendeler er relevante for påliteligheten av utarbeidelsen av regnskap, avhenger av omstendighetene, for eksempel når eiendeler er særlig eksponert for urettmessig tilegnelse.

- *Arbeidsdeling.* Tildeling av ansvar til ulike personer for autorisasjon av transaksjoner, registrering av transaksjoner og kontroll over eiendeler. Hensikten med arbeidsdeling er å redusere en persons mulighet til å begå og deretter skjule feil eller misligheter ved utøvelsen av personens oppgaver.

  For eksempel, en leder som autoriserer kredittsalg er ikke ansvarlig for å regnskapsføre kundefordringer eller håndtere kvitteringer. Dersom én person kan utføre alle disse aktivitetene, vil personen for eksempel kunne opprette et fiktivt salg som ikke nødvendigvis blir avdekket. Likeledes bør ikke selgere ha mulighet til å endre produktprisfiler eller provisjonssatser.

  Noen ganger er arbeidsdeling verken praktisk, kostnadseffektivt eller gjennomførbart. Små og mindre komplekse enheter har for eksempel ikke alltid tilstrekkelige ressurser til å oppnå en ideell arbeidsdeling, og kostnader knyttet til innleie av ekstra personell kan være for høye. I slike situasjoner kan ledelsen etablere alternative kontroller. Dersom selgeren i eksempelet ovenfor kan endre produktprisfiler, kan det etableres en undersøkende kontrollaktivitet, der personale som ikke er knyttet til salgsfunksjonen regelmessig gjennomgår hvorvidt eller under hvilke omstendigheter selgeren har endret priser.

21. Visse kontroller kan avhenge av om det foreligger hensiktsmessige tilsynskontroller etablert av ledelsen eller dem som har overordnet ansvar for styring og kontroll. Autorisasjonskontroller kan for eksempel være delegert i henhold til fastsatte retningslinjer, for eksempel investeringskriterier fastsatt av dem som har overordnet ansvar for styring og kontroll, eller det kan være at ikke-rutinemessige transaksjoner, som store kjøp eller salg, krever særskilt godkjenning på høyere nivå, noen ganger også fra aksjonærene.

Begrensninger i den interne kontrollen

22. Enhetens internkontrollsystem, uansett hvor effektivt det er, kan bare gi rimelig sikkerhet for at enheten oppfyller sine mål for finansiell rapportering. Sannsynligheten for at målene oppfylles, påvirkes av de iboende begrensningene i den interne kontrollen. Disse omfatter det faktum at menneskelig skjønn ved beslutningstaking kan være mangelfullt, og at feil i enhetens internkontrollsystem kan forekomme på grunn av menneskelig svikt. Det kan for eksempel forekomme feil i forbindelse med utformingen eller endringen av en kontroll. Likeledes kan det forekomme at driften av en kontroll ikke er effektiv, for eksempel når informasjon som produseres for bruk i enhetens internkontrollsystem (for eksempel en avviksrapport), ikke anvendes effektivt fordi personen som er ansvarlig for gjennomgåelsen av informasjonen ikke forstår formålet med den eller unnlater å iverksette de nødvendige tiltakene.

23. I tillegg kan kontroller omgås gjennom fordekt samarbeid mellom to eller flere personer, eller gjennom utilbørlig overstyring av kontroller på ledelsesnivå. Ledelsen kan for eksempel inngå sideavtaler med kunder som endrer vilkårene i enhetens standard salgsavtaler, noe som kan føre til uriktig inntektsføring. Også redigeringskontroller i en IT-applikasjon som er utformet for å identifisere og rapportere transaksjoner som overskrider angitte kredittgrenser, kan overstyres eller deaktiveres.

24. Videre kan ledelsen ved utformingen og implementeringen av kontroller foreta skjønnsmessige vurderinger knyttet til typen og omfanget av de kontrollene den velger å implementere, og typen og omfanget av de risikoene den velger å legge til grunn.

Vedlegg 4

(Jf. punkt 14(a), 24(a)(ii), A25–A28, A118)

Vurderinger knyttet til forståelsen av en enhets internrevisjonsfunksjon

Dette vedlegget inneholder ytterligere vurderinger knyttet til forståelsen av enhetens internrevisjonsfunksjon når enheten har en slik funksjon.

Internrevisjonsfunksjonens mål og ansvarsområde

1. Målene og ansvarsområdet til en internrevisjonsfunksjon, og typen oppgaver og organisatoriske plassering, herunder funksjonens myndighet og ansvar, varierer betydelig, og avhenger av enhetens størrelse, kompleksitet og struktur samt krav fra ledelsen, og der det er aktuelt, dem som har overordnet ansvar for styring og kontroll. Disse forholdene kan beskrives i et internrevisjonsmandat eller annet tilsvarende dokument.

2. En internrevisjonsfunksjons oppgaver kan omfatte å utføre handlinger og evaluere resultatene for å gi sikkerhet til ledelsen og dem som har overordnet ansvar for styring og kontroll, om utformingen og effektiviteten av risikostyring, enhetens internkontrollsystem og styringsprosesser. I så fall kan internrevisjonsfunksjonen spille en viktig rolle i enhetens prosess for overvåking av enhetens internkontrollsystem. Internrevisjonsfunksjonens oppgaver kan imidlertid være fokusert på å evaluere økonomien, kostnadseffektiviteten og måleffektiviteten av driften, og i så fall kan funksjonens arbeid ikke nødvendigvis knyttes direkte til enhetens finansielle rapportering.

Forespørsler til internrevisjonsfunksjonen

3. Dersom en enhet har en internrevisjonsfunskjon, kan forespørsler til de relevante personene i funksjonen gi informasjon som er nyttig for revisors opparbeidelse av en forståelse av enheten og dens omgivelser, det gjeldende rammeverket for finansiell rapportering og enhetens internkontrollsystem, og for å identifisere og anslå risikoer for vesentlig feilinformasjon på regnskaps- og påstandsnivå. Under sitt arbeid får internrevisjonsfunksjonen sannsynligvis innsikt i enhetens drift og forretningsrisikoer, og kan gjøre funn basert på sitt arbeid, slik som identifiserte kontrollmangler eller risikoer, som kan gi verdifulle bidrag til revisors forståelse av enheten og dens omgivelser, det gjeldende rammeverket for finansiell rapportering, enhetens internkontrollsystem, revisors risikovurderinger eller andre aspekter ved revisjonen. Revisors forespørsler gjennomføres derfor uansett om revisor forventer å bruke internrevisjonsfunksjonens arbeid for å endre typen eller tidspunktet for, eller redusere omfanget av, revisjonshandlinger som skal utføres.[73] Forespørsler av særlig relevans kan gjelde forhold som internrevisjonsfunksjonen har tatt opp med dem som har overordnet ansvar for styring og kontroll, og utfallene av funksjonens egen risikovurderingsprosess.

4. Dersom det ut fra svar på revisors forespørsler viser seg at det er funn som kan være relevante for enhetens finansielle rapportering og for revisjonen av regnskapet, kan revisor vurdere det

[73] De relevante kravene er beskrevet i ISA 610 (revidert 2013).

hensiktsmessig å lese relevante rapporter fra internrevisjonsfunksjonen. Eksempler på rapporter fra internrevisjonsfunksjonen som kan være relevante, omfatter internrevisjonsfunksjonens strategi- og planleggingsdokumenter og rapporter som er utarbeidet for ledelsen eller dem som har overordnet ansvar for styring og kontroll, og som beskriver funnene fra internrevisjonsfunksjonens undersøkelser.

5. I tillegg, i samsvar med ISA 240,[74] dersom internrevisjonsfunksjonen fremskaffer informasjon til revisor om eventuelle faktiske, mistenkte eller påståtte misligheter, tar revisor dette i betraktning ved sin identifisering av risiko for vesentlig feilinformasjon som skyldes misligheter.

6. Relevante personer i internrevisjonsfunksjonen som forespørsler rettes til, er de som, etter revisors skjønn, har hensiktsmessig kunnskap, erfaring og autoritet, for eksempel leder for internrevisjonen eller, avhengig av omstendighetene, andre personell i funksjonen. Revisor kan også vurdere det hensiktsmessig å ha regelmessige møter med disse personene.

Vurdering av internrevisjonsfunksjonen gjennom forståelse av kontrollmiljøet

7. Ved opparbeidelse av en forståelse av kontrollmiljøet kan revisor vurdere hvordan ledelsen har respondert på funn og anbefalinger fra internrevisjonsfunksjonen vedrørende identifiserte kontrollmangler som er relevante for utarbeidelsen av regnskapet, herunder hvorvidt og hvordan tiltak er blitt implementert, og hvorvidt de i ettertid er blitt evaluert av internrevisjonsfunksjonen.

Forståelse av internrevisjonsfunksjonens rolle i enhetens prosess for overvåking av internkontrollsystemet

8. Dersom internrevisjonsfunksjonens oppgaver, ansvarsområder og revisjonsaktiviteter er knyttet til enhetens finansielle rapportering, kan revisor også bruke internrevisjonsfunksjonens arbeid til å endre typen eller tidspunktet for, eller redusere omfanget av, revisjonshandlinger som skal utføres direkte av revisor for å innhente revisjonsbevis. Det er mer sannsynlig at revisor kan bruke arbeidet til en enhets internrevisjonsfunksjon når det viser seg, for eksempel basert på erfaring fra tidligere revisjoner eller revisors risikovurderingshandlinger, at enheten har en internrevisjonsfunksjon som har adekvate og hensiktsmessige ressurser i forhold til enhetens kompleksitet og typen virksomhet, og har et direkte rapporteringsforhold til dem som har overordnet ansvar for styring og kontroll.

9. Dersom revisor basert på sin foreløpige forståelse av internrevisjonsfunksjonen, forventer å bruke internrevisjonsfunksjonens arbeid for å endre typen eller tidspunktet for, eller redusere omfanget av, revisjonshandlinger som skal utføres, gjelder ISA 610 (revidert 2013).

10. Som videre drøftet i ISA 610 (revidert 2013), skiller aktivitetene til en internrevisjonsfunksjon seg fra andre overvåkingskontroller som kan være relevante for finansiell rapportering, for eksempel gjennomgåelser av ledelsens regnskapsinformasjon som er utformet for å bidra til at enheten forebygger eller oppdager feilinformasjon.

[74] ISA 240, punkt 19

11. Ved å etablere kommunikasjon med de relevante personene i en enhets internrevisjonsfunksjon tidlig i oppdraget, og opprettholde kommunikasjonen gjennom hele oppdraget, kan det legges til rette for effektiv informasjonsdeling. Det skaper et miljø der revisor kan bli informert om vesentlige forhold som internrevisjonsfunksjonen kan bli oppmerksom på, når slike forhold kan påvirke revisors arbeid. ISA 200 drøfter viktigheten av at revisor planlegger og utfører revisjonen med profesjonell skepsis,[75] herunder at revisor er oppmerksom på informasjon som gir grunn til stille spørsmål ved påliteligheten av dokumenter og svar på forespørsler som skal benyttes som revisjonsbevis. Følgelig kan kommunikasjon med internrevisjonsfunksjonen gjennom hele oppdraget gi interne revisorer muligheter til å gjøre revisor oppmerksom på slik informasjon. Revisor er da i stand til å ta slik informasjon i betraktning når revisor identifiserer og vurderer risikoer for vesentlig feilinformasjon.

[75] ISA 200, punkt 7

Vedlegg 5

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

Vurderinger knyttet til forståelsen av informasjonsteknologi (IT)

Dette vedlegget beskriver ytterligere forhold som revisor kan vurdere ved opparbeidelsen av en forståelse av enhetens bruk av IT i sitt internkontrollsystem.

Forståelse av enhetens bruk av informasjonsteknologi i komponentene i enhetens internkontrollsystem

1. En enhets internkontrollsystem omfatter manuelle elementer og automatiserte elementer (dvs. manuelle og automatiserte kontroller og andre ressurser som benyttes i enhetens internkontrollsystem). En enhets blanding av manuelle og automatiserte elementer varierer avhengig av typen og kompleksiteten av enhetens bruk av IT. En enhets bruk av IT påvirker måten informasjonen som er relevant for utarbeidelsen av regnskapet i samsvar med det gjeldende rammeverket for finansiell rapportering, behandles, lagres og kommuniseres på, og påvirker derfor måten enhetens internkontrollsystem er utformet og implementert på. Hver komponent i enhetens internkontrollsystem kan bruke en viss grad av IT.

   Generelt er IT en fordel for en enhets internkontrollsystem, ettersom den gjør det mulig for enheten å:

   - Anvende forhåndsdefinerte forretningsregler på en ensartet måte og utføre komplekse beregninger ved behandling av store mengder transaksjoner eller data;
   - Forbedre informasjonens aktualitet, tilgjengelighet og nøyaktighet;
   - Forenkle videre analyse av informasjon;
   - Forbedre muligheten til å overvåke resultatet av enhetens aktiviteter, retningslinjer og rutiner;
   - Redusere risikoen for at kontroller omgås; og
   - Forbedre muligheten til å oppnå en effektiv arbeidsdeling ved å innføre sikkerhetskontroller i IT-applikasjoner, databaser og operativsystemer.

2. Særtrekkene ved manuelle eller automatiserte elementer er relevante for revisors identifisering og vurdering av risikoene for vesentlig feilinformasjon, og videre revisjonshandlinger som bygger på dette grunnlaget. Automatiserte kontroller kan være mer pålitelige enn manuelle kontroller, ettersom de ikke så enkelt kan omgås, ignoreres eller overstyres, og de er også mindre utsatt for enkle feil. Automatiserte kontroller kan være mer effektive enn manuelle kontroller under følgende omstendigheter:

   - Stort volum av gjentakende transaksjoner, eller situasjoner der feil som kan forventes eller forutsies, kan forebygges, eller avdekkes og korrigeres, gjennom automatisering.

- Kontroller der de spesifikke måtene kontrollen skal utføres på, kan utformes og automatiseres på en hensiktsmessig måte.

Forståelse av enhetens bruk av informasjonsteknologi i informasjonssystemet (Jf. punkt 25(a))

3. Enhetens informasjonssystem kan omfatte bruk av manuelle og automatiserte elementer, som også påvirker måten transaksjoner initieres, registreres, behandles og rapporteres på. Særlig rutiner for å initiere, registrere, behandle og rapportere transaksjoner kan styres av IT-applikasjonene som benyttes av enheten, og måten enheten har konfigurert disse applikasjonene på. I tillegg kan registreringer i form av digital informasjon erstatte eller supplere registreringer i form av papirdokumenter.

4. Ved opparbeidelsen av en forståelse av IT-miljøet som er relevant for transaksjonsflyten og prosessering av informasjon i informasjonssystemet, samler revisor inn informasjon om typen og særtrekkene ved IT-applikasjonene som benyttes, så vel som den støttende it-infrastrukturen og IT. Følgende tabell inneholder eksempler på forhold som revisor kan vurdere ved opparbeidelsen av en forståelse av IT-miljøet, og omfatter eksempler på typiske særtrekk ved IT-miljøer basert på kompleksiteten av IT-applikasjoner som benyttes i enhetens informasjonssystem. Disse særtrekkene er imidlertid veiledende, og kan variere avhengig av den spesifikke typen IT-applikasjoner som benyttes av en enhet.

	Eksempler på typiske særtrekk ved:		
	Ikke-komplekse kommersielle programvarer	Middels store og middels komplekse kommersielle programvarer eller IT-applikasjoner	Store eller komplekse IT-applikasjoner (f.eks. ERP-systemer)
Forhold knyttet til omfang av automatisering og bruk av data:			
• Omfanget av automatiserte rutiner for behandling, og kompleksiteten av disse rutinene, herunder hvorvidt det er høy grad av automatisert, papirløs behandling.	Ikke relevant	Ikke relevant	Omfattende og ofte komplekse automatiserte rutiner

	Eksempler på typiske særtrekk ved:		
	Ikke-komplekse kommersielle programvarer	Middels store og middels komplekse kommersielle programvarer eller IT-applikasjoner	Store eller komplekse IT-applikasjoner (f.eks. ERP-systemer)
• I hvilken grad enheten bygger på systemgenererte rapporter i behandlingen av informasjon.	Enkel automatisert rapportlogikk	Enkel relevant automatisert rapportlogikk	Kompleks automatisert rapportlogikk; rapportgenerator
• Hvordan data registreres (dvs. manuelt, av kunde eller leverandør, eller ved filnedlasting).	Manuelle dataregistreringer	Få dataregistreringer eller enkle grensesnitt	Mange dataregistreringer eller komplekse grensesnitt
• Hvordan IT fremmer kommunikasjon mellom applikasjoner, databaser og andre aspekter ved IT-miljøet, internt og eksternt, avhengig av hva som er relevant, gjennom systemgrensesnitt.	Ingen automatiserte grensesnitt (kun manuelle registreringer)	Få dataregistreringer eller enkle grensesnitt	Mange dataregistreringer eller komplekse grensesnitt
• Mengden og kompleksiteten av data i digital form	Liten datamengde eller enkle data som kan	Liten datamengde eller enkle data	Stor datamengde eller komplekse data; datavarehus;[76] bruk av

[76] Et datavarehus blir vanligvis beskrevet som et sentralt lager av integrerte data fra én eller flere forskjellige kilder (for eksempel flere databaser) som benyttesbenyttesbenyttesbenyttes til å generere rapporter, eller som kan benyttesbenyttesbenyttesbenyttes av enheten til andre dataanalyseaktiviteter. En rapportgenerator er en IT-applikasjon som benyttesbenyttesbenyttesbenyttes til

	Eksempler på typiske særtrekk ved:		
	Ikke-komplekse kommersielle programvarer	Middels store og middels komplekse kommersielle programvarer eller IT-applikasjoner	Store eller komplekse IT-applikasjoner (f.eks. ERP-systemer)
som behandles av informasjonssystemet, herunder hvorvidt regnskapsmateriale eller annen informasjon er lagret digitalt og plasseringen av lagrede data.	verifiseres manuelt; data tilgjengelig lokalt		interne eller eksterne leverandører av IT-tjenester (for eksempel lagring eller drifting av data av tredjepart)
Forhold knyttet til IT-applikasjoner og IT-infrastruktur:			
• Typen applikasjon (f.eks. en kommersiell applikasjon med liten eller ingen tilpassing, eller en svært tilpasset eller integrert applikasjon som kan ha blitt kjøpt og tilpasset, eller utviklet internt).	Kjøpt applikasjon med liten eller ingen tilpassing	Kjøpt applikasjon eller enkle, eldre eller rimelige ERP-applikasjoner med liten eller ingen tilpassing	Kundeutviklede applikasjoner eller mer komplekse ERP-er med betydelig tilpassing

å trekke ut data fra en eller flere kilder (for eksempel et datavarehus, en database eller en IT-applikasjon) og presentere dataene i et angitt format.

	Eksempler på typiske særtrekk ved:		
	Ikke-komplekse kommersielle programvarer	Middels store og middels komplekse kommersielle programvarer eller IT-applikasjoner	Store eller komplekse IT-applikasjoner (f.eks. ERP-systemer)
• Kompleksiteten av typen IT-applikasjoner og støttende it-infrastruktur.	Liten, enkel bærbar datamaskin eller klientserverbasert løsning	Moden og stabil stormaskin, liten eller enkel klientserver, programvare som skytjeneste	Kompleks stormaskin, stor eller kompleks klientserver, Internett-rettet, infrastruktur som skytjeneste
• Hvorvidt det forekommer tredjepartsdrift eller utkontraktering av IT.	Dersom utkontraktert, kompetent, moden, erfaren leverandør (for eksempel skyleverandør)	Dersom utkontraktert, kompetent, moden, erfaren leverandør (for eksempel skyleverandør)	Kompetent, moden, erfaren leverandør for visse applikasjoner, og nye eller oppstartsleverandører for andre
• Hvorvidt enheten bruker nye teknologier som påvirker enhetens finansielle rapportering.	Ingen bruk av nye teknologier	Begrenset bruk av nye teknologier i enkelte applikasjoner	Blandet bruk av nye teknologier på tvers av plattformer
Forhold knyttet til IT-prosesser:			
• Personell som arbeider med vedlikehold av IT-miljøet (antall personell og ferdighetsnivå på IT-ressurser som håndterer sikkerhet og endringer i IT-miljøet).	Få personell med begrenset IT-kunnskap som behandler leverandøroppgraderinger og administrerer tilgang	Begrenset antall personell med IT-ferdigheter/som kun arbeider med IT	Egne IT-avdelinger med kompetente personell, herunder programmeringsferdigheter
• Kompleksiteten av prosesser for å	Én person med administratortilgang	Få personer med administratortilgang	Komplekse prosesser for tilgangsrettigheter

	Eksempler på typiske særtrekk ved:		
	Ikke-komplekse kommersielle programvarer	Middels store og middels komplekse kommersielle programvarer eller IT-applikasjoner	Store eller komplekse IT-applikasjoner (f.eks. ERP-systemer)
administrere tilgangsrettigheter.	administrerer tilgangsrettigheter	administrerer tilgangsrettigheter	som administreres av IT-avdeling
• Kompleksiteten av sikkerheten knyttet til IT-miljøet, herunder sårbarheten til IT-applikasjoner, databaser og andre aspekter ved IT-miljøet i forhold til cyberrisikoer, særlig når det er nettbaserte transaksjoner eller transaksjoner som involverer eksterne grensesnitt.	Enkel lokal tilgang uten eksterne Internett-rettede elementer	Noen nettbaserte applikasjoner med hovedsakelig enkel, rollebasert sikkerhet	Flere plattformer med nettbasert tilgang og komplekse sikkerhetsmodeller
• Hvorvidt det er utført programendringer i måten informasjonen behandles på, og omfanget av slike endringer i løpet av perioden.	Kommersielle programvarer uten kildekode installert	Noen kommersielle applikasjoner uten kildekode og andre modne applikasjoner med et lite antall eller enkle endringer; livssyklus for utvikling av tradisjonelle systemer	Nye eller et stort antall eller komplekse endringer, flere utviklingssykluser hvert år
• Omfanget av endringer i IT-miljøet (f.eks. nye aspekter ved IT-	Endringer begrenset til versjonsoppgraderinger av kommersielle programvarer	Endringer består av kommersielle programvareoppgraderinger, ERP-	Nye eller et stort antall eller komplekse endringer, flere utviklingssykluser hvert

	Eksempler på typiske særtrekk ved:		
	Ikke-komplekse kommersielle programvarer	Middels store og middels komplekse kommersielle programvarer eller IT-applikasjoner	Store eller komplekse IT-applikasjoner (f.eks. ERP-systemer)
miljøet eller vesentlige endringer i IT-applikasjonene eller støttende it-infrastruktur).		versjonsoppgraderinger eller forbedringer av eldre versjoner	år, omfattende ERP-tilpassing
• Hvorvidt det har vært en omfattende datakonvertering i løpet av perioden og i så fall, typen og betydningen av endringene som er foretatt, og hvordan konverteringen er utført.	Programvareoppgraderinger fra leverandør; ingen datakonverteringsfunksjoner for oppgradering	Mindre versjonsoppgraderinger for kommersielle programvareapplikasjoner med begrenset data som er konvertert	Stor versjonsoppgradering, ny utgave, endring av plattform

Nye teknologier

5. Enheter kan bruke nye teknologier (for eksempel blokkjede, robotikk eller kunstig intelligens), ettersom slike teknologier kan gi spesifikke muligheter for å øke den driftsmessige effektiviteten eller forbedre den finansielle rapporteringen. Når det benyttes nye teknologier i enhetens informasjonssystem som er relevant for utarbeidelsen av regnskapet, kan revisor inkludere disse teknologiene ved identifiseringen av IT-applikasjoner og andre aspekter ved IT-miljøet som er gjenstand for risikoer som følger av bruken av IT. Selv om nye teknologier kan bli ansett å være mer sofistikerte eller mer komplekse sammenlignet med eksisterende teknologier, forblir revisors oppgaver og plikter knyttet til IT-applikasjoner og identifiserte generelle IT-kontroller i samsvar med punkt 26(b)–(c), uendret.

Skalerbarhet

6. Det kan være enklere å opparbeide seg en forståelse av enhetens IT-miljø for en mindre kompleks enhet som bruker kommersielle programvarer, og når enheten ikke har tilgang til kildekoden for å

foreta programendringer. Slike enheter har ikke nødvendigvis dedikerte IT-ressurser, men kan ha en person som har fått tildelt en administratorrolle med det formål å gi tilgang til ansatte eller installere leverandøroppdateringer av IT-applikasjonene. Spesifikke forhold som revisor kan vurdere ved opparbeidelsen av en forståelse av typen kommersiell programvarepakke for regnskap, som kan være en enkelt IT-applikasjon som benyttes av en mindre kompleks enhet i sitt informasjonssystem, kan omfatte:

- I hvilken grad programvaren er godt etablert og har ord på seg for å være pålitelig;
- I hvilken grad det er mulig for enheten å endre programvarens kildekode for å inkludere ytterligere moduler (dvs. tillegg) i den grunnleggende programvaren, eller å endre dataene direkte;
- Typen og omfanget av modifikasjoner som er foretatt i programvaren. Selv om en enhet ikke nødvendigvis kan modifisere programvarens kildekode, er det mange programvarepakker som tillater konfigurasjon (for eksempel innstilling eller endring av rapporteringsparametere). Disse involverer vanligvis ikke modifikasjoner i kildekoden. Revisor kan imidlertid vurdere i hvilken grad enheten er i stand til å konfigurere programvaren i forbindelse med revisors vurdering av fullstendigheten og nøyaktigheten av informasjon produsert av programvaren som benyttes som revisjonsbevis; og
- I hvilken grad det er mulig å få direkte tilgang til data relatert til utarbeidelsen av regnskapet (dvs. direkte tilgang til databasen uten å bruke IT-applikasjonen), og datamengden som behandles. Jo større datamengden er, desto mer sannsynlig er det at enheten har behov for kontroller som er rettet mot opprettholdelse av integriteten til dataene, som kan omfatte generelle IT-kontroller knyttet til uautorisert tilgang og endringer i dataene.

7. Komplekse IT-miljøer kan omfatte svært tilpassede eller svært integrerte IT-applikasjoner, og kan derfor kreve større innsats for å opparbeide seg en forståelse av dem. Prosesser eller IT-applikasjoner for finansiell rapportering kan være integrert i andre IT-applikasjoner. En slik integrasjon kan involvere IT-applikasjoner som benyttes i enhetens forretningsvirksomhet, og som formidler informasjon til IT-applikasjonene som er relevante for transaksjonsflyten og prosessering av informasjon i enhetens informasjonssystem. Under slike omstendigheter kan visse IT-applikasjoner som benyttes i enhetens forretningsvirksomhet, også være relevante for utarbeidelsen av regnskapet. Komplekse IT-miljøer kan også kreve egne IT-avdelinger som har strukturerte IT-prosesser som støttes av personell som har ferdigheter innenfor programvareutvikling og vedlikehold av IT-miljøer. I andre tilfeller kan enheten bruke interne eller eksterne tjenesteleverandører til å administrere visse aspekter ved, eller IT-prosesser i, enhetens IT-miljø (for eksempel tredjepartsdrift).

Identifisering av IT-applikasjoner som er gjenstand for risikoer som følger av bruken av IT

8. Gjennom en forståelse av typen og kompleksiteten av enhetens IT-miljø, herunder typen og omfanget av informasjonsbehandlingskontroller, kan revisor fastsette hvilke IT- applikasjoner enheten bygger på for å sikre nøyaktig behandling og opprettholdelse av integriteten til finansiell informasjon. Identifiseringen av IT-applikasjoner som enheten bygger på, kan påvirke revisors beslutning om å

teste de automatiserte kontrollene innenfor slike IT-applikasjoner, forutsatt at slike automatiserte kontroller håndterer identifiserte risikoer for vesentlig feilinformasjon. På den annen side, dersom enheten ikke bygger på en IT-applikasjon, er det lite sannsynlig at de automatiserte kontrollene innenfor en slik IT-applikasjon vil være hensiktsmessige eller tilstrekkelig presise ut fra formålet med tester av måleffektiviteten. Automatiserte kontroller som kan identifiseres i samsvar med punkt 26(b), kan for eksempel omfatte automatiserte beregninger eller kontroller knyttet til inndata, behandling og utdata, for eksempel en treveis sammenligning av en innkjøpsordre, et fraktdokument og en leverandørfaktura. Når automatiserte kontroller identifiseres av revisor, og revisor fastsetter gjennom forståelsen av IT-miljøet at enheten bygger på IT-applikasjonen som omfatter disse automatiserte kontrollene, kan det være mer sannsynlig at revisor identifiserer IT-applikasjonen som en applikasjon som er gjenstand for risikoer som følger av bruken av IT.

9. Ved vurdering av hvorvidt IT-applikasjonene som revisor har identifisert automatiserte kontroller for, er gjenstand for risikoer som følger av bruken av IT, er det sannsynlig at revisor vurderer hvorvidt, og i hvilket omfang, enheten kan ha tilgang til kildekode som gjør det mulig for ledelsen å foreta programendringer i slike kontroller eller i IT-applikasjonene. I hvilket omfang enheten foretar program- eller konfigurasjonsendringer, og i hvilket omfang IT-prosessene knyttet til slike endringer er formalisert, kan også være relevante vurderinger. Det er også sannsynlig at revisor vurderer risikoen for urettmessig tilgang til eller endringer i data.

10. Systemgenererte rapporter som revisor kan ha til hensikt å bruke som revisjonsbevis, kan for eksempel omfatte en rapport som viser kundefordringer sortert etter alder, eller en verdsettelsesrapport for varelager. For slike rapporter kan revisor innhente revisjonsbevis for fullstendigheten og nøyaktigheten av rapportene ved å substansteste inn- og utdataene i rapporten. I andre tilfeller kan revisor planlegge å teste måleffektiviteten av kontrollene knyttet til utarbeidelsen og vedlikeholdet av rapporten. I så fall kan IT-applikasjonen som rapporten er produsert fra, være gjenstand for risikoer som følger av bruken av IT. I tillegg til å teste fullstendigheten og nøyaktigheten av rapporten, kan revisor planlegge å teste måleffektiviteten av generelle IT-kontroller som håndterer risikoer knyttet til urettmessige eller uautoriserte programendringer knyttet til, eller dataendringer i, rapporten.

11. Noen IT-applikasjoner kan inneholde en rapportgeneratorfunksjon, mens noen enheter også kan bruke egne rapportgeneratorapplikasjoner (dvs. rapportgeneratorer). I slike tilfeller kan det bli nødvendig for revisor å identifisere kildene til systemgenererte rapporter (dvs. applikasjonen som utarbeider rapporten og datakildene som er benyttet av rapporten) for å fastsette om IT-applikasjonene er gjenstand for risikoer som følger av bruken av IT.

12. Datakildene som benyttes av IT-applikasjoner kan være databaser som det for eksempel bare er mulig å få tilgang til gjennom IT-applikasjonen, eller som bare IT-personale med databaseadministratorrettigheter har tilgang til. I andre tilfeller kan datakilden være et datavarehus som selv kan bli vurdert til å være en IT-applikasjon som er gjenstand for risikoer som følger av bruken av IT.

13. Revisor kan ha identifisert en risiko der substanshandlinger alene ikke er tilstrekkelig på grunn av enhetens bruk av svært automatisert og papirløs behandling av transaksjoner, som kan involvere flere integrerte IT-applikasjoner. Under slike omstendigheter vil kontrollene identifisert av revisor ofte inkludere automatiserte kontroller. Videre kan enheten bygge på generelle IT-kontroller for å vedlikeholde integriteten til transaksjonene som behandles og annen informasjon som benyttes under behandlingen. I slike tilfeller vil IT-applikasjonene som er involvert i behandlingen og lagringen av informasjonen, ofte være gjenstand for risikoer som følger av bruken av IT.

Sluttbrukerberegning

14. Selv om revisjonsbevis også kan foreligge i form av systemgenererte utdata som benyttes i en beregning utført i et beregningsverktøy for sluttbrukere (for eksempel et regnearkprogram eller enkle databaser), blir slike verktøy vanligvis ikke identifisert som IT-applikasjoner innenfor rammen av punkt 26 (b). Utforming og implementering av kontroller knyttet til tilgang og endring i beregningsverktøy for sluttbrukere kan være utfordrende, og slike kontroller er sjelden ekvivalente med, eller like effektive som, generelle IT-kontroller. I stedet kan revisor vurdere en kombinasjon av informasjonsbehandlingskontroller, som tar i betraktning formålet med og kompleksiteten av sluttbrukerberegningen som er involvert, for eksempel:

    - Informasjonsbehandlingskontroller knyttet til initieringen og behandlingen av kildedataene, herunder relevante automatiserte kontroller eller grensesnittkontroller frem til punktet der dataene trekkes ut (dvs. datavarehuset);
    - Kontroller for å kontrollere at logikken fungerer som tiltenkt, for eksempel kontroller som «beviser» uttrekkingen av data, som avstemming av rapporten mot dataene den bygger på, sammenligning av individuelle data fra rapporten med kilden, og omvendt, og kontroller som kontrollerer formlene eller makroene; eller
    - Bruk av programvareverktøy for validering, som systematisk kontrollerer formler eller makroer, for eksempel verktøy som kontrollerer integriteten til regneark.

Skalerbarhet

15. Enhetens evne til å opprettholde integriteten til informasjon som lagres og behandles i informasjonssystemet kan variere basert på kompleksiteten og mengden av de relaterte transaksjonene og annen informasjon. Jo større kompleksiteten og mengden av data som underbygger en signifikant transaksjonsklasse, kontosaldo eller tilleggsopplysning er, desto mindre sannsynlig er det at enheten opprettholder integriteten til denne informasjonen gjennom informasjonsbehandlingskontroller alene (dvs. inn- og utdatakontroller eller gjennomgåelseskontroller). Det er også mindre sannsynlig at revisor vil være i stand til å innhente revisjonsbevis for fullstendigheten og nøyaktigheten av slik informasjon gjennom substanstester alene, når slik informasjon benyttes som revisjonsbevis. Under enkelte omstendigheter, når mengden og kompleksiteten av transaksjoner er mindre, kan ledelsen ha en informasjonsbehandlingskontroll som er tilstrekkelig til å verifisere nøyaktigheten og fullstendigheten av dataene (for eksempel kan individuelle salgsordre som er behandlet og fakturert, avstemmes med papirkopien som opprinnelig

ble registrert i IT-applikasjonen). Når enheten bygger på generelle IT-kontroller for å opprettholde integriteten til bestemt informasjon som benyttes av IT-applikasjoner, kan revisor fastsette at IT-applikasjonene som vedlikeholder denne informasjonen, er gjenstand for risikoer som følger av bruken av IT.

Eksempler på særtrekk ved en IT-applikasjon som sannsynligvis ikke er gjenstand for risikoer som følger av IT	Eksempler på særtrekk ved en IT-applikasjon som sannsynligvis er gjenstand for risikoer som følger av IT
• Frittstående applikasjoner. • Datamengden (transaksjoner) er ikke betydelig. • Applikasjonens funksjonalitet er ikke kompleks. • Hver transaksjon underbygges av original dokumentasjon i papir.	• Applikasjoner er forbundet gjennom grensesnitt. • Datamengden (transaksjoner) er betydelig. • Applikasjonens funksjonalitet er kompleks, ettersom: – Applikasjonen automatisk initierer transaksjoner; og – Det er en rekke komplekse beregninger som ligger til grunn for automatiserte registreringer.
IT-applikasjon er sannsynligvis ikke gjenstand for risikoer som følger av IT fordi: • Datamengden er ikke betydelig, og ledelsen bygger derfor ikke på generelle IT-kontroller for å behandle eller vedlikeholde dataene. • Ledelsen bygger ikke på automatiserte kontroller eller annen automatisert funksjonalitet. Revisor har ikke identifisert automatiserte kontroller i samsvar med punkt 26(a). • Selv om ledelsen bruker systemgenererte rapporter i sine kontroller, bygger den ikke på disse rapportene. I stedet avstemmer den rapportene med dokumentasjonen i papir og verifiserer beregningene i rapportene. • Revisor vil teste informasjon produsert av enheten som benyttes som revisjonsbevis, direkte.	IT-applikasjon er sannsynligvis gjenstand for risikoer som følger av IT fordi: • Ledelsen bygger på et applikasjonssystem for å behandle eller vedlikeholde data, ettersom datamengden er betydelig. • Ledelsen bygger på applikasjonssystemet for å utføre bestemte automatiserte kontroller som revisor også har identifisert.

Andre aspekter ved IT-miljøet som er gjenstand for risikoer som følger av bruken av IT

16. Når revisor identifiserer IT-applikasjoner som er gjenstand for risikoer som følger av bruken av IT, vil andre aspekter ved IT-miljøet vanligvis også være gjenstand for risikoer som følger av bruken av IT. IT-infrastrukturen omfatter databasene, operativsystemet og nettverket. Databaser lagrer dataene som benyttes av IT-applikasjoner, og kan bestå av mange datatabeller som er innbyrdes forbundet. Det kan også være mulig for IT-personalet og annet personale med databaseadministratorrettigheter å få direkte tilgang til data i databaser gjennom databaseadministrasjonssystemer. Operativsystemet er ansvarlig for å administrere kommunikasjon mellom maskinvare, IT-applikasjoner og annen programvare som benyttes i nettverket. Det kan dermed være mulig å få direkte tilgang til IT-applikasjoner og databaser gjennom operativsystemet. Et nettverk benyttes i IT-infrastrukturen til å overføre data og dele informasjon, ressurser og tjenester gjennom en felles kommunikasjonsforbindelse. Nettverket etablerer også vanligvis et lag med logisk sikkerhet (aktivert gjennom operativsystemet) for å få tilgang til underliggende ressurser.

17. Når revisor identifiserer IT-applikasjoner som er gjenstand for risikoer som følger av IT, blir databasene som lagrer dataene som behandles av en identifisert IT-applikasjon, vanligvis også identifisert. Likeledes, fordi en IT-applikasjons evne til å fungere ofte avhenger av operativsystemet, og det kan være mulig å få direkte tilgang til IT-applikasjoner og databaser fra operativsystemet, er operativsystemet vanligvis gjenstand for risikoer som følger av bruken av IT. Nettverket kan bli identifisert når det er et sentralt tilgangspunkt for de identifiserte IT-applikasjonene og tilhørende databaser, eller når en IT-applikasjon interagerer med leverandører eller eksterne parter gjennom Internett, eller når Internett-rettede IT-applikasjoner identifiseres av revisor.

Identifisering av risikoer som følger av bruken av IT og generelle IT-kontroller

18. Eksempler på risikoer som følger av bruken av IT, omfatter risikoer knyttet til for stor tillit til IT-applikasjoner som behandler data unøyaktig, behandler unøyaktige data, eller begge deler, for eksempel:

    - Uautorisert tilgang til data som kan føre til ødeleggelse eller urettmessige endringer av data, herunder registrering av uautoriserte eller ikke-eksisterende transaksjoner, eller unøyaktig registrering av transaksjoner. Særlige risikoer kan oppstå når flere brukere har tilgang til en felles database.
    - Mulighet for at IT-personell får tilgangsrettigheter ut over de som er nødvendige for å utføre oppgavene de er tildelt, noe som bryter ned arbeidsdelingen.
    - Uautoriserte endringer av data i hovedfiler.
    - Uautoriserte endringer i IT-applikasjoner eller andre aspekter ved IT-miljøet.
    - Unnlatelse av å foreta nødvendige endringer i IT-applikasjoner eller andre aspekter ved IT-miljøet.
    - Urettmessige manuelle inngrep.

- Mulig tap av data eller manglende tilgang til nødvendige data.

19. Revisors vurdering av uautorisert tilgang kan omfatte risikoer knyttet til uautorisert tilgang fra interne eller eksterne parter (ofte referert til som cybersikkerhetsrisikoer). Slike risikoer påvirker ikke nødvendigvis finansiell rapportering, ettersom en enhets IT-miljø også kan omfatte IT-applikasjoner og tilknyttede data som er rettet mot driftsmessige krav eller krav til overholdelse av lover og forskrifter. Det er viktig å være oppmerksom på at cyberhendelser vanligvis først forekommer gjennom perimeternettverket og interne nettverkslag, som har en tendens til være et stykke unna IT-applikasjons-, database- og operativsystemene som påvirker utarbeidelsen av regnskapet. Følgelig, dersom informasjon om et sikkerhetsbrudd er blitt identifisert, vurderer revisor vanligvis i hvilket omfang et slikt brudd kan påvirke finansiell rapportering. Dersom finansiell rapportering kan være påvirket, kan revisor beslutte å opparbeide seg en forståelse av, og teste de tilknyttede kontrollene for å fastsette den mulige innvirkningen eller omfanget av mulig feilinformasjon i regnskapet, eller revisor kan fastsette at enheten har gitt adekvate tilleggsopplysninger i forhold til et slikt sikkerhetsbrudd.

20. I tillegg kan lover og forskrifter som kan ha en direkte eller indirekte virkning på enhetens regnskap, inkludere bestemmelser om databeskyttelse. Vurdering av en enhets overholdelse av slike lover eller forskrifter, i samsvar med ISA 250 (revidert),[77] kan innebære opparbeidelse av en forståelse av enhetens IT-prosesser og generelle IT-kontroller som enheten har implementert for å rette seg etter de relevante lovene eller forskriftene.

21. Generelle IT-kontroller implementeres for å håndtere risikoer som følger av bruken av IT. Revisor bruker følgelig den opparbeidede forståelsen av de identifiserte IT-applikasjonene og andre aspekter ved IT-miljøet og de gjeldende risikoene som følger av bruken av IT, ved fastsettelsen av hvilke generelle IT-kontroller som skal identifiseres. I enkelte tilfeller kan enheten bruke felles IT-prosesser på tvers av IT-miljøet eller på tvers av bestemte IT-applikasjoner. I så fall kan felles risikoer som følger av bruken av IT og felles generelle IT-kontroller bli identifisert.

22. Det er generelt sett sannsynlig at det identifiseres flere generelle IT-kontroller knyttet til IT-applikasjoner og databaser enn for andre aspekter ved IT-miljøet. Det er fordi disse aspektene er nærmest knyttet til prosessering av informasjon og lagringen av informasjon i enhetens informasjonssystem. Ved identifisering av generelle IT-kontroller kan revisor vurdere kontroller knyttet til handlinger hos både sluttbrukere og enhetens IT-personale eller IT-tjenesteleverandører.

23. **Vedlegg 6** gir en ytterligere beskrivelse av typen generelle IT-kontroller som vanligvis er implementert for forskjellige aspekter ved IT-miljøet. I tillegg gir vedlegget eksempler på generelle IT-kontroller for forskjellige IT-prosesser.

[77] ISA 250 (revidert)

Vedlegg 6

(Jf. punkt 25(c)(ii), A173–A174)

Vurderinger knyttet til forståelsen av generelle IT-kontroller

Dette vedlegget beskriver ytterligere forhold som revisor kan vurdere ved opparbeidelsen av en forståelse av generelle IT-kontroller.

1. Typen generelle IT-kontroller som vanligvis er implementert for hvert av aspektene ved IT-miljøet:

   (a) Applikasjoner

   Generelle IT-kontroller ved IT-applikasjonslaget vil korrelere med typen og omfanget av applikasjonsfunksjonalitet og tilgangsbanene som tillates av teknologien. Flere kontroller vil for eksempel være relevante for svært integrerte IT-applikasjoner med komplekse sikkerhetsalternativer enn for en eldre IT-applikasjon som støtter et lite antall kontosaldoer med tilgangsmetoder gjennom transaksjoner alene.

   (b) Database

   Generelle IT-kontroller ved databaselaget er vanligvis rettet mot risikoer som følger av bruken av IT knyttet til uautoriserte oppdateringer av finansiell rapporteringsinformasjon i databasen gjennom direkte databasetilgang eller kjøring av et skript eller et program.

   (c) Operativsystem

   Generelle IT-kontroller ved operativsystemlaget er vanligvis rettet mot risikoer som følger av bruken av IT knyttet til administratortilgang, som kan legge til rette for overstyring av andre kontroller. Dette omfatter handlinger som for eksempel å kompromittere en annen brukers legitimasjon, legge til nye, uautoriserte brukere, laste inn skadelig programvare eller kjøre skripter eller andre uautoriserte programmer.

   (d) Nettverk

   Generelle IT-kontroller ved nettverkslaget er vanligvis rettet mot risikoer som følger av bruken av IT knyttet til nettverkssegmentering, ekstern tilgang og autentisering. Nettverkskontroller kan være relevante når en enhet har Internett-rettede applikasjoner som benyttes ved finansiell rapportering. Nettverkskontroller kan også være relevante når enheten har betydelige forretningspartnerrelasjoner eller utkontraktering til tredjepart, noe som kan øke dataoverføringer og behovet for ekstern tilgang.

2. Eksempler på generelle IT-kontroller som kan forekomme, organisert etter IT-prosess, omfatter:

   (a) Prosess for å administrere tilgang:

   - *Autentisering*

     Kontroller som sikrer at en bruker med tilgang til IT-applikasjonen eller andre aspekter ved IT-miljøet bruker sin egen legitimasjon til pålogging (dvs. brukeren bruker ikke en annen brukers legitimasjon).

- *Autorisasjon*

  Kontroller som gir brukere tilgang til informasjonen som er nødvendig for at de skal kunne utføre arbeidet sitt, og ingenting annet, noe som legger til rette for hensiktsmessig arbeidsdeling.

- *Klargjøring*

  Kontroller for å autorisere nye brukere og modifikasjoner i eksisterende brukeres tilgangsrettigheter.

- *Oppheving av klargjøring*

  Kontroller for å fjerne brukertilgang etter avslutning eller overføring.

- *Privilegert tilgang*

  Kontroller knyttet til administratortilgang eller tilgang for privilegerte brukere.

- *Gjennomgåelser av brukertilgang*

  Kontroller for å bekrefte på nytt eller evaluere brukertilgang for løpende autorisasjon over tid.

- *Sikkerhetskonfigurasjonskontroller*

  Hver teknologi har vanligvis hovedkonfigurasjonsinnstillinger som bidrar til å begrense tilgang til miljøet.

- *Fysisk tilgang*

  Kontroller knyttet til fysisk tilgang til datasenteret og maskinvaren, ettersom slik tilgang kan benyttes til å overstyre andre kontroller.

(b) Prosess for å administrere programmering eller andre endringer i IT-miljøet:

- *Prosess for endringsadministrasjon*

  Kontroller knyttet til prosessen for å utforme, programmere, teste og overføre endringer i et produksjonsmiljø (dvs. et sluttbrukermiljø).

- *Arbeidsdeling ved endringsoverføring*

  Kontroller som fordeler tilgang for å foreta eller overføre endringer til et produksjonsmiljø.

- *Systemutvikling eller innkjøp eller implementering*

  Kontroller knyttet til utvikling eller implementering av IT-applikasjon (eller i forhold til andre aspekter ved IT-miljøet).

- *Datakonvertering*

  Kontroller knyttet til konverteringen av data under utvikling, implementering eller oppgraderinger av IT-miljøet.

(c) Prosess for å administrere IT-drift

- *Jobbplanlegging*

  Kontroller knyttet til tilgang for å planlegge og initiere jobber eller programmer som kan påvirke finansiell rapportering.

- *Jobbovervåking*

  Kontroller for å overvåke at jobber eller programmer knyttet til finansiell rapportering utføres riktig.

- *Sikkerhetskopiering og gjenoppretting*

  Kontroller for å sikre at sikkerhetskopiering av finansielle rapporteringsdata skjer som planlagt, at disse dataene er tilgjengelige, og at det er mulig å få tilgang til dem for rask gjenoppretting i tilfelle avbrudd eller angrep.

- *Inntrengingsoppdagelse*

  Kontroller for å overvåke sårbarheter og/eller inntrenginger i IT-miljøet.

Tabellen nedenfor inneholder eksempler på generelle IT-kontroller som er rettet mot eksempler på risikoer som følger av bruken av IT, herunder forskjellige IT-applikasjoner basert på typen.

Prosess	**Risikoer**	**Kontroller**	**IT-applikasjoner**		
IT-prosess	**Eksempler på risikoer som følger av bruken av IT**	**Eksempler på generelle IT-kontroller**	**Ikke-komplekse kommersielle programvarer – Relevant (ja/nei)**	**Middels store og middels komplekse kommersielle programvarer eller IT-applikasjoner – Relevant (ja/nei)**	**Store eller komplekse IT-applikasjoner (f.eks. ERP-systemer) – Relevant (ja/nei)**
Administrere tilgang	Tilgangsrettigheter: Brukere har tilgangsrettigheter ut over de som er nødvendige	Ledelsen godkjenner typen og omfanget av tilgangsrettigheter for ny og modifisert brukertilgang,	Ja – i stedet for gjennomgåelser av brukertilgang notert nedenfor	Ja	Ja

Prosess	Risikoer	Kontroller	IT-applikasjoner		
IT-prosess	**Eksempler på risikoer som følger av bruken av IT**	**Eksempler på generelle IT-kontroller**	**Ikke-komplekse kommersielle programvarer – Relevant (ja/nei)**	**Middels store og middels komplekse kommersielle programvarer eller IT-applikasjoner – Relevant (ja/nei)**	**Store eller komplekse IT-applikasjoner (f.eks. ERP-systemer) – Relevant (ja/nei)**
	for å utføre de oppgavene de er tildelt, noe som kan skape en utilstrekkelig arbeidsdeling.	herunder standard applikasjonsprofiler/-roller, kritiske transaksjoner for finansiell rapportering og arbeidsdeling			
		Tilgang for avsluttede eller overførte brukere er fjernet eller modifisert i rett tid	Ja – i stedet for gjennomgåelser av brukertilgang nedenfor	Ja	Ja
		Brukertilgang gjennomgås regelmessig	Ja – i stedet for klargjørings-/ opphevingskontroller ovenfor	Ja – for bestemte applikasjoner	Ja
		Arbeidsdeling overvåkes, og motstridende tilgang blir enten fjernet eller tilordnet motvirkende kontroller, som er	Ikke relevant – ingen systemaktivert arbeidsdeling	Ja – for bestemte applikasjoner	Ja

Prosess	**Risikoer**	**Kontroller**	**IT-applikasjoner**		
IT-prosess	**Eksempler på risikoer som følger av bruken av IT**	**Eksempler på generelle IT-kontroller**	**Ikke-komplekse kommersielle programvarer – Relevant (ja/nei)**	**Middels store og middels komplekse kommersielle programvarer eller IT-applikasjoner – Relevant (ja/nei)**	**Store eller komplekse IT-applikasjoner (f.eks. ERP-systemer) – Relevant (ja/nei)**
		dokumentert og testet			
		Tilgang på privilegert nivå (f.eks. konfigurasjons-, data- og sikkerhetsadministratorer) er autorisert og tilstrekkelig begrenset	Ja – sannsynligvis kun ved IT-applikasjonslag	Ja – ved IT-applikasjon og bestemte lag i IT-miljø for plattform	Ja – ved alle lag i IT-miljø for plattform
Administrere tilgang	Direkte datatilgang: Urettmessige endringer foretas direkte i finansielle data gjennom andre metoder enn applikasjonstransaksjoner.	Tilgang til applikasjonsdatafiler eller databaseobjekter/-tabeller/-data er begrenset til autoriserte personell basert på deres arbeidsoppgaver og tildelte rolle, og slik tilgang er godkjent av ledelsen	Ikke relevant	Ja – for bestemte applikasjoner og databaser	Ja

Prosess	**Risikoer**	**Kontroller**	**IT-applikasjoner**		
IT-prosess	**Eksempler på risikoer som følger av bruken av IT**	**Eksempler på generelle IT-kontroller**	**Ikke-komplekse kommersielle programvarer – Relevant (ja/nei)**	**Middels store og middels komplekse kommersielle programvarer eller IT-applikasjoner – Relevant (ja/nei)**	**Store eller komplekse IT-applikasjoner (f.eks. ERP-systemer) – Relevant (ja/nei)**
Administrere tilgang	Systeminnstillinger: Systemer er ikke adekvat konfigurert eller oppdatert for å begrense systemtilgang til riktig autoriserte og rettmessige brukere.	Tilgang godkjennes gjennom unike bruker-ID-er og passord eller andre metoder som en mekanisme for å validere at brukere er autorisert til å få tilgang til systemet. Passordparametere oppfyller selskaps- eller bransjestandarder (dvs. minimum passordlengde og kompleksitet, utløp, låsing av konto).	Ja – kun passordgodkjenning	Ja – blanding av passord- og flerfaktorgodkjenning	Ja
		Nøkkelattributtene for sikkerhetskonfigurasjon er riktig implementert	Ikke relevant – det finnes ingen tekniske sikkerhetskonfigurasjoner	Ja – for bestemte applikasjoner og databaser	Ja

Prosess	**Risikoer**	**Kontroller**	**IT-applikasjoner**		
IT-prosess	**Eksempler på risikoer som følger av bruken av IT**	**Eksempler på generelle IT-kontroller**	**Ikke-komplekse kommersielle programvarer – Relevant (ja/nei)**	**Middels store og middels komplekse kommersielle programvarer eller IT-applikasjoner – Relevant (ja/nei)**	**Store eller komplekse IT-applikasjoner (f.eks. ERP-systemer) – Relevant (ja/nei)**
Administrere endringer	Applikasjonsendringer: Urettmessige endringer foretas i applikasjonssystemer eller programmer som inneholder relevante automatiserte kontroller (dvs. konfigurerbare innstillinger, automatiserte algoritmer, automatiserte beregninger og automatisert datauttrekking) eller rapportlogikk.	Applikasjonsendringer er tilstrekkelig testet og godkjent før overføring til produksjonsmiljøet	Ikke relevant – kunne verifisere at ingen kildekode er installert	Ja – for ikke-kommersielle programvarer	Ja
		Tilgang til å implementere endringer i applikasjonsproduksjonsmiljøet er tilstrekkelig begrenset og atskilt fra utviklingsmiljøet	Ikke relevant	Ja – for ikke-kommersielle programvarer	Ja

Prosess	**Risikoer**	**Kontroller**	**IT-applikasjoner**		
IT-prosess	**Eksempler på risikoer som følger av bruken av IT**	**Eksempler på generelle IT-kontroller**	**Ikke-komplekse kommersielle programvarer – Relevant (ja/nei)**	**Middels store og middels komplekse kommersielle programvarer eller IT-applikasjoner – Relevant (ja/nei)**	**Store eller komplekse IT-applikasjoner (f.eks. ERP-systemer) – Relevant (ja/nei)**
Administrere endringer	Databaseendringer: Urettmessige endringer foretas i databasestrukturen og relasjoner mellom dataene.	Databaseendringer er tilstrekkelig testet og godkjent før overføring til produksjonsmiljøet	Ikke relevant – ingen databaseendringer foretatt hos enhet	Ja – for ikke-kommersielle programvarer	Ja
Administrere endringer	Endringer i systemprogramvare: Urettmessige endringer foretas i systemprogramvaren (f.eks. operativsystem, nettverk, programvare for endringsadministrasjon, programvare for tilgangskontroll).	Endringer i systemprogramvare er tilstrekkelig testet og godkjent før overføring til produksjon	Ikke relevant – ingen endringer i systemprogramvare foretatt hos enhet	Ja	Ja

Prosess	**Risikoer**	**Kontroller**	**IT-applikasjoner**		
IT-prosess	**Eksempler på risikoer som følger av bruken av IT**	**Eksempler på generelle IT-kontroller**	**Ikke-komplekse kommersielle programvarer – Relevant (ja/nei)**	**Middels store og middels komplekse kommersielle programvarer eller IT-applikasjoner – Relevant (ja/nei)**	**Store eller komplekse IT-applikasjoner (f.eks. ERP-systemer) – Relevant (ja/nei)**
Administrere endringer	Datakonvertering: Data konvertert fra eldre systemer eller tidligere versjoner introduserer datafeil dersom konverteringen overfører ufullstendige, overflødige, utdaterte eller unøyaktige data.	Ledelsen godkjenner resultatene av datakonverteringen (f.eks. balanse- eller avstemmingsaktiviteter) fra det gamle applikasjonssystemet eller den gamle datastrukturen til det nye applikasjonssystemet eller den nye datastrukturen og overvåker at konverteringen er utført i samsvar med etablerte retningslinjer og rutiner for konvertering	Ikke relevant – håndtert gjennom manuelle kontroller	Ja	Ja
IT-drift	Nettverk: Nettverket hindrer ikke i tilstrekkelig grad	Tilgang godkjennes gjennom unike bruker-ID-er og passord eller andre	Ikke relevant – det finnes ingen separat nettverksautentifiseringsmetode	Ja	Ja

Prosess	Risikoer	Kontroller	IT-applikasjoner		
IT-prosess	**Eksempler på risikoer som følger av bruken av IT**	**Eksempler på generelle IT-kontroller**	**Ikke-komplekse kommersielle programvarer – Relevant (ja/nei)**	**Middels store og middels komplekse kommersielle programvarer eller IT-applikasjoner – Relevant (ja/nei)**	**Store eller komplekse IT-applikasjoner (f.eks. ERP-systemer) – Relevant (ja/nei)**
	at uautoriserte brukere får urettmessig tilgang til informasjonssystemer.	metoder som en mekanisme for å validere at brukere er autorisert til å få tilgang til systemet. Passordparametere oppfyller selskapets eller bransjens faglige retningslinjer og standarder (dvs. minimum passordlengde og kompleksitet, utløp, låsing av konto)			
		Nettverk er bygd for å segmentere Internett-rettede applikasjoner fra det interne nettverket, der tilgangen til ICFR-relevante applikasjoner er	Ikke relevant – nettverkssegmentering benyttes ikke	Ja – med skjønn	Ja – med skjønn
		Sårbarhetsskanninger av	Ikke relevant	Ja – med skjønn	Ja – med skjønn

Prosess	Risikoer	Kontroller	IT-applikasjoner		
IT-prosess	**Eksempler på risikoer som følger av bruken av IT**	**Eksempler på generelle IT-kontroller**	**Ikke-komplekse kommersielle programvarer – Relevant (ja/nei)**	**Middels store og middels komplekse kommersielle programvarer eller IT-applikasjoner – Relevant (ja/nei)**	**Store eller komplekse IT-applikasjoner (f.eks. ERP-systemer) – Relevant (ja/nei)**
		perimeternettverket utføres regelmessig av nettverksadministrasjonsteamet, som også undersøker potensielle sårbarhetsrisikoer			
		Varsler genereres regelmessig for å informere om trusler identifisert av systemene for inntrengingsoppdagelse. Disse truslene undersøkes av nettverksadministrasjonsteamet	Ikke relevant	Ja – med skjønn	Ja – med skjønn
		Kontroller er implementert for å begrense VPN-tilgang til autoriserte og rettmessige brukere	Ikke relevant – ingen VPN	Ja – med skjønn	Ja – med skjønn

Prosess	**Risikoer**	**Kontroller**	**IT-applikasjoner**		
IT-prosess	**Eksempler på risikoer som følger av bruken av IT**	**Eksempler på generelle IT-kontroller**	**Ikke-komplekse kommersielle programvarer – Relevant (ja/nei)**	**Middels store og middels komplekse kommersielle programvarer eller IT-applikasjoner – Relevant (ja/nei)**	**Store eller komplekse IT-applikasjoner (f.eks. ERP-systemer) – Relevant (ja/nei)**
IT-drift	Sikkerhetskopiering og gjenoppretting av data: Det er ikke mulig å gjenopprette eller få tilgang til finansielle data raskt ved datatap.	Finansielle data sikkerhetskopieres regelmessig i samsvar med en etablert plan og frekvens	Ikke relevant – bygger på manuelle sikkerhetskopieringer utført av finansteam	Ja	Ja
IT-drift	Jobbplanlegging: Produksjonssystemer, programmer eller jobber resulterer i unøyaktig, ufullstendig eller uautorisert behandling av data.	Kun autoriserte brukere har tilgang til å oppdatere satsvise jobber (herunder grensesnittjobber) i programvaren for jobbplanlegging	Ikke relevant – ingen satsvise jobber	Ja – for bestemte applikasjoner	Ja
		Kritiske systemer, programmer eller jobber overvåkes, og behandlingsfeil korrigeres for å sikre	Ikke relevant – ingen jobbovervåking	Ja – for bestemte applikasjoner	Ja

Prosess	Risikoer	Kontroller	IT-applikasjoner		
IT-prosess	**Eksempler på risikoer som følger av bruken av IT**	**Eksempler på generelle IT-kontroller**	**Ikke-komplekse kommersielle programvarer – Relevant (ja/nei)**	**Middels store og middels komplekse kommersielle programvarer eller IT-applikasjoner – Relevant (ja/nei)**	**Store eller komplekse IT-applikasjoner (f.eks. ERP-systemer) – Relevant (ja/nei)**
		korrekt gjennomføring.			

Strukturene og prosessene som støtter virksomheten til IAASB, er tilrettelagt av International Federation of Accountants® eller IFAC®.

IAASB og IFAC påtar seg ikke noe ansvar for tap som skyldes utføring av handlinger eller unnlatelse av å utføre handlinger på grunnlag av innholdet i denne publikasjonen, uaktet om dette tapet er en følge av uaktsomhet eller er oppstått på annen måte.

Internasjonale revisjonsstandarder, internasjonale standarder for attestasjonsoppdrag, internasjonale standarder for forenklet revisorkontroll, internasjonale standarder for beslektede tjenester, internasjonale standarder for kvalitetskontroll, internasjonale revisjonspraksisnotater, høringsutkast, diskusjonsnotater og andre publikasjoner fra IAASB utgis av og tilhører opphavsrettslig IFAC.

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