# ISA 315 (ajourført) – Risikovurdering med fokus på **virksomhedens it-anvendelse**

Formålet med nærværende artikel, samt de øvrige artikler i dette nummer af Revision & Regnskabsvæsen om ISA 315 (ajourført 2019) *Identifikation og vurdering af risici for væsentlig fejlinformation,* er at informere om den ajourførte standard og bidrage til en ensartet og passende implementering heraf. Artiklerne kan ikke erstatte en fuldstændig gennemgang af standarden og tilhørende vejledning samt bilag som grundlag for udførelsen af en revision efter ISA.

## 1. ISA 315 (ajourført) – overordnede betragtninger

Den tidligere version af ISA 315[1] er fra 2012. IAASB har med den ajourførte standard oplagt haft som en af sine målsætninger at forbedre standarden, således at denne fremstår mere forståelig, anvendelig og opdateret til den it-teknologi, der anvendes af et stort antal virksomheder.

De oprindelige afsnit om revisors opnåelse og dokumentation af forståelse af interne kontrolsystemer har været vanskelige at omsætte i praksis. Den hastige udvikling inden for digitalisering og it, herunder betydningen af virksomhedernes it-anvendelse i forhold til regnskabsaflæggelsen og virksomhedens drift, har påkaldt et aktuelt behov for både en opdatering og modernisering af standarden. Trusler og risici ved it-anvendelsen kan medføre tab af informationer, længerevarende it-nedbrud, fx på grund af cyberangreb eller sanktioner ved manglende compliance i forhold til relevant lovgivning, herunder beskyttelse af personhenførbare data.

Formålet med ajourføringen af ISA 315 er først og fremmest udsprunget af behovet for mere konsistente og dokumenterede risikovurderinger – også i relation til vurderingen af specifikke risici forbundet med it-anvendelsen i virksomhederne. Dette vil formentlig være med til at forbedre kvaliteten af de udførte revisioner. Det skal samtidig medvirke til at synliggøre revisors udøvelse af tilstrækkelig grad af professionel skepsis og sikre en effektivitet i forhold til at indhente tilstrækkelige og egnede revisionsbeviser.

På it-området er standarden blevet mere fokuseret på at stille eksplicitte krav til revisors risikovurderingshandlinger. Revisor skal til brug herfor opnå og dokumentere sin forståelse af såvel it-miljøet, it-relaterede risici, generelle it-kontroller og informationsbehandlingskontroller, der adresserer disse risici. Revisors forståelse for de risici, der knytter sig til brugen af it, skal medvirke til at sikre identifikation af risici på regnskabsniveau og på revisionsmålsniveau, hvor it-miljøet, anvendelsen af it og virk-

*Af Hans Henrik Berthing, Verifica, medlem af Cybersikkerhedsudvalget, og Thomas Bjerrehus, Revisorgruppen Danmark, medlem af Revisionsteknisk Udvalg, FSR – danske revisorer*


somhedens generelle it-kontroller er udgangspunktet for revisors tilrettelæggelse af risikovurderingshandlingerne.

Standarden indeholder i vejledningsafsnittene uddybende forklaringer til, hvordan revisor kan udføre planlægningsaktiviteter, herunder risikovurderingshandlinger, der er rettet imod it-anvendelsen i virksomheden, hvor det absolutte fokus er rettet imod de to komponenter i det interne kontrolsystem, som benævnes henholdsvis "Informationssystemet og kommunikation" og "Kontrolaktiviteter". Såvel muligheden for at skalere kravene efter forholdene i virksomheden (mere eller mindre komplekse it-miljøer) som de konkrete eksempler i vejledningsafsnittene, som adresserer it-relaterede problemstillinger, øger anvendeligheden af standarden betragteligt. Hertil kommer to centrale bilag til standarden, henholdsvis bilag 5 og 6, som omhandler "Overvejelser vedrørende forståelse af informationsteknologi (it)" og "Overvejelser vedrørende forståelse af generelle it-kontroller".

## 2. Informationsteknologi

It-systemer genererer en væsentlig del af det revisionsbevis, revisor anvender i sin revision. Derfor bliver det stadigt mere nødvendigt for revisor at opnå forståelse for virksomhedens it-miljø med særligt fokus på de aspekter af it-miljøet, der er relevante for den finansielle rapportering, herunder hvordan informationernes integritet opretholdes. Den modernisering af standarden, som er affødt af behovet for ændringer og udvidelser i forhold til virksomhedens anvendelse af it, træder forholdsvis tydeligt frem. Den ajourførte standard har således været igennem en omfattende clarificering og udvidelse af kravene i forhold til den tidligere version af ISA 315. Nu kræves det, at revisor opnår forståelse af virksomhedens anvendelse af it i forretningsmodellen og i det interne kontrolsystem. Opnåelse af en sådan forståelse danner grundlag for revisors identifikation af risici for væsentlig fejlinformation, der opstår som følge af risici ved virksomhedens anvendelse af it, samt identifikation af relevante generelle it-kontroller, som

virksomheden har fastlagt for at adressere disse risici for væsentlig fejlinformation.

I de tilhørende vejledningsafsnit til ISA 315 (ajourført) er der foretaget væsentlige udvidelser med henblik på at understøtte de udvidede og forbedrede krav i standarden. IAASB har på glimrende vis i forbindelse med udarbejdelsen af den ajourførte standard baseret vejledningsafsnittene vedrørende it på "den principbaserede tilgang" (ingen "facitliste" over, hvad der skal gøres eller ikke gøres). Dette er formentlig en erkendelse af, at hele området for informationsteknologi ændres med stor hastighed, og at der ved en anden tilgang kunne være en risiko for, at standarden hurtigt ville kunne opfattes som uddateret.

### 3. Styrket vejledning på it-området

It er det medie, gennem hvilket en væsentlig del af revisionsbevis indhentes/opnås, og det bliver af netop denne årsag mere og mere essentielt for revisor at forstå virksomhedens it-system, herunder hvordan informationernes integritet opretholdes. Dette er også tilfældet i de situationer, hvor revisionsbeviset udarbejdes af eller er tilgængeligt fra kilder, der ligger uden for den reviderede virksomhed. Med baggrund heri er det oplagt, at ISA 315 (ajourført)[2] indeholder væsentlige udvidelser i forhold til revisors overvejelser vedrørende it, når revisor opnår forståelse for virksomhedens interne kontrolsystem, herunder:

- Eksempler på revisors forståelse af forhold i relation til it-miljøet, herunder it-applikationer, it-infrastruktur og it-processer
- Eksempler på revisors forståelse af forhold i relation til it-miljøet, der sandsynligvis vil være relevante i forhold til at fastlægge it-applikationer og andre aspekter af it-miljøet, der er relevante for revisionen
- Eksempler på revisors overvejelser i situationer, hvor virksomhedens it-system består af kommercielt software, og virksomheden ikke har adgang til kildekoden kontra situationer, hvor virksomheden anvender egenudviklede/-tilrettede og komplekse/integrerede it-systemer.

IAASB har foretaget ændringer/justeringer i en række definitioner relateret til it med det formål at skabe mere klarhed over begreberne.

De væsentligste udvidelser af kravene i ISA 315 (ajourført) vedrørende virksomhedens anvendelse af it findes i kravene i COSO-komponenten "informationssystemet og kommunikation" og vedrørende identifikationen af kontrolaktiviteter. Når revisor skal opnå forståelse for den del af informationssystemet, der er relevant for den finansielle rapportering, kræves det, at revisor forstår det tilhørende it-miljø med henblik på at opnå et tilstrækkeligt niveau af forståelse/viden om indhold og kompleksitet af miljøet og de dertilhørende processer. Gennem revisors opnåede forståelse for såvel it-miljøet som identifikationen af kontrolaktiviteter, anvender revisor en række kriterier til at fastlægge, hvilke it-applikationer og andre aspekter af it-miljøet der er relevante for revisionen. Disse kriterier bruger revisor til at identificere it-applikationer, der er karakteriseret ved, at virksomhedens brug heraf medfører forøget risiko for fejl, og som kan påvirke design, implementering eller funktionalitet (den operationelle effektivitet) af automatiske kontroller eller andre kontroller af betydning for integriteten af informationen.

For så vidt angår it-applikationer og andre aspekter af it-miljøet, som vurderes at være relevante for revisionen, identificerer revisor risici, der opstår som følge af virksomhedens anvendelse af it, og identificerer generelle it-kontroller, der imødegår/adresserer disse risici (generelle it-kontroller, der er relevante for revisionen). Vejledningsafsnittene til disse krav er blevet udvidet således, at der nu mere uddybende gives forklaring på de sandsynlige risici og kontroller, som revisor bør overveje, ligesom det implicit må lægges til grund, at de sandsynlige risici og interne kontroller, som revisor bør overveje, vil variere, baseret på omstændighederne ved opgaven og den planlagte revisionsstrategi og -tilgang. Et nyt bilag 6 giver vejledning om revisors forståelse af generelle it-kontroller.

Det må antages, at den justerede fremgangsmåde og struktur vil medvirke til at hjælpe revisor i beslutningsprocessen, når revisor skal afgøre, i hvilket omfang generelle it-kontroller er relevante for revisionen. Det er ikke nødvendigt for revisor at identificere risici, der opstår via virksomhedens anvendelse af it eller generelle it-kontroller, medmindre det er vurderet, at der er it-applikationer, der er relevante for revisionen.

I mindre virksomheder og mindre komplicerede virksomheder består it-miljøet ofte alene af standardsoftware, hvor virksomheden ikke har adgang til den underliggende kildekode, og der kan således ikke foretages programændringer. Her kan revisor lægge til grund, at ingen af virksomhedens it-applikationer er relevante for revisionen, herunder at revisor planlægger at substansteste alle systemgenererede rapporter og anden information, som er produceret af virksomhedens informationssystem, som anvendes som revisionsbevis (fx debitorlisten eller lagerlisten). I modsætning hertil vil der ved større og mere komplekse virksomheder eller situationer, hvor revisor planlægger at teste funktionaliteten (den operationelle effektivitet) af automatiserede kontrol-

It er det medie, gennem hvilket en væsentlig del af revisionsbevis indhentes/opnås, og det bliver af netop denne årsag mere og mere essentielt for revisor at forstå virksomhedens it-system, herunder hvordan informationernes integritet opretholdes. Dette er også tilfældet i de situationer, hvor revisionsbeviset udarbejdes af eller er tilgængeligt fra kilder, der ligger uden for den reviderede virksomhed.

ler, kunne lægges til grund, at der er flere it-applikationer, der er relevante for revisionen. Denne omstændighed vil så betyde, at der rettes fokus på generelle it-kontroller med relevans for revisionen.

I mange revisioner, hvor brugervirksomheden anvender standardsystemer, vil revisor indhente en ISAE 3402[3] type 2-erklæring. I disse revisioner indgår systemgenererede rapporter i form af eksempelvis en aldersopdelt debitorliste til vurdering af værdiansættelsen af debitorerne. ISAE 3402-erklæringen vil ofte ikke være tilstrækkelig til, at revisor kan anvende disse rapporter som bevis uden at teste dem. Revisor skal derfor sikre sig validiteten af sådanne rapporter. Det kan gøres ved at efterprøve, om aldersopdelingen af en stikprøve af tilgodehavender er korrekt baseret på en sammentælling af alle salgsfakturaer og eventuelle kreditnotaer samt indbetalinger og eventuelle udbetalinger på balancetidspunktet.

### 4. Information udarbejdet af virksomheden

Revisor baserer i vidt omfang sine revisionshandlinger på forskellige former for indhentet revisionsbevis. ISA 500[4] (afsnit 9) fastslår, at når revisor benytter revisionsbevis udarbejdet af virksomheden, skal revisor vurdere, om informationen er tilstrækkeligt pålidelig til revisors formål, og revisor skal efter omstændighederne opnå revisionsbevis for nøjagtigheden og fuldstændigheden af informationen.

De klassiske eksempler på sådan information er systemgenererede rapporter i form af eksempelvis en aldersopdelt debitorliste eller en lagerværdiopgørelse. Når revisor skal teste nøjagtigheden og fuldstændigheden af sådanne rapporter, kan dette enten gøres ved at teste de kontroller, der sikrer nøjagtigheden og fuldstændigheden af rapporterne, eller ved at foretage substansbaserede handlinger af rapporterne. Det vil bl.a. være tilfældet i forbindelse med revisionen rettet imod nøjagtigheden af en aldersopdelt debitorliste, der anvendes som grundlag for at vurdere, om der er et nedskrivningsbehov i forhold til virksomhedens tilgodehavender.

I forhold til ISA 315 (ajourført) er det vigtigt at skelne mellem risikovurderingshandlinger og test af kontrollers operationelle effektivitet. Risikovurderingshandlinger er revisionshandlinger, der er designet og udført med henblik på at identificere og vurdere risiciene for væsentlig fejlinformation på regnskabs- og revisionsmålsniveau, uanset om de skyldes besvigelser eller fejl. Test af kontrollers operationelle effektivitet foretages i lighed med substansrevisionshandlinger for at hjælpe revisor med at konkludere, om der er væsentlige fejl i transaktioner, balanceposter eller oplysninger og tilhørende relevante revisionsmål. Kravene til det revisionsbevis, der skal indhentes for at sikre informationens nøjagtighed og fuldstændighed, er derfor mere omfattede i relation til test af kontrollers operationelle

effektivitet, end det er tilfældet for risikovurderingshandlingerne.

ISA 315 (ajourført) giver i såvel vejledningsafsnittene som i bilagsdelen glimrende eksempler på og vejledning i forhold til netop planlægning af test af kontrollers operationelle effektivitet, herunder specifikt i forhold til fuldstændigheden og nøjagtigheden af den information, som virksomheden har frembragt (kontroller vedrørende udarbejdelse af systemgenererede rapporter), når revisor i sin revision har til hensigt at tage højde for disse kontrollers operationelle effektivitet ved design og udførelse af yderligere revisionshandlinger.

Opmærksomheden skal særligt henledes på de gode eksempler, der ledsager vejledningsafsnittene til standarden, herunder eksempler på bl.a. revisors strategi for test af information udarbejdet af virksomheden, som er udarbejdet via eller involverer information fra virksomhedens it-applikationer. Ud over at teste eksempelvis en aldersopdelt debitorlistes fuldstændighed og nøjagtighed understreges det i vejledningen, at revisor også kan planlægge at teste funktionaliteten af de generelle it-kontroller, der retter sig mod risici vedrørende upassende eller uautoriserede programændringer til eller dataændringer i debitorlisten.

Revisor skal identificere de tilknyttede risici, der knytter sig til brugen af it samt virksomhedens generelle it-kontroller, der adresserer disse risici. Dette gælder for såvel it-applikationer som for andre aspekter i virksomhedens it-miljø, som har relevans for regnskabsaflæggelsen.

## 5. It-relaterede risici og generelle it-kontroller til håndtering af disse

I ISA 315 (ajourført) afsnit 26, fremgår det, at virksomhedens it-anvendelse medfører risici, som revisor skal være opmærksom på. Således er der mulighed for, at der forekommer mangler i designet af informationsbehandlingskontroller, eller at disse kontroller ikke er operationelt effektive. Der kan også være tale om risici knyttet til integriteten af information i virksomhedens informationssystem som følge af mangler i designet af kontroller eller manglende operationel effektivitet af kontroller i virksomhedens it-processer. Det er således vigtigt, at revisor identificerer og dokumenterer disse it-relaterede risici og virksomhedens generelle it-kontroller, der håndterer disse risici. Under revisors risikovurderingshandlinger skal revisor opnå en forståelse af, hvordan anvendelsen af it er integreret i forretningsmodellen. Endvidere skal revisor opnå en forståelse af virksomhedens informationssystem og kommunikation, der er relevant for regnskabsaflæggelsen. Dette gøres fundamentalt set ved at forstå, hvordan virksomhedens aktiviteter er knyttet til informationsbehandling. Her tænkes først og fremmest på data og information, de ressourcer, der anvendes for disse aktiviteter, samt politikkerne, som for betydelige grupper af transaktioner, balanceposter og oplysninger beskriver, hvordan information strømmer gennem virksomhedens informationssystem.

Endvidere skal der opnås forståelse af it-miljøet med relevans for regnskabsaflæggelsen. Revisor skal vurdere, hvorvidt virksomhedens informationssystem og kommunikation i tilstrækkelig grad understøtter regnskabsaflæggelsen i overensstemmelse med den relevante regnskabsmæssige begrebsramme.

Revisor skal identificere de tilknyttede risici, der knytter sig til brugen af it, samt virksomhedens generelle it-kontroller, der adresserer disse risici. Dette gælder for såvel it-applikationer som for andre aspekter i virksomhedens it-miljø, som har relevans for regnskabsaflæggelsen.

Risici forbundet med informationers integritet opstår via muligheden for ineffektiv implementering af virksomhedens informationspolitikker i form af politikker, der definerer strømmen af information, registreringer og rapporteringsprocesser i virksomhedens informationssystem. Informationsbehandlingskontroller er procedurer, der understøtter en effektiv implementering af virksomhedens informationspolitikker. Informationsbehandlingskontroller kan være automatiske (dvs. indbygget i it-applikationer) eller manuelle (fx input- eller outputkontroller), og kan være afhængige af andre kontroller, herunder andre informationsbehandlingskontroller eller generelle it-kontroller.

Via forespørgsler til medarbejdere i it-afdelingen kan revisor indhente information om systemændringer, systemfejl, kontrolsvigt eller andre it-relaterede risici.

Revisor kan observere, om der er etableret funktionsadskillelse, eller at passwords indtastes. Som led i revisors risikovurderingshandlinger kan revisor foretage observation og inspektion af virksomhedens it-lokaliteter.

Revisor skal fastsætte strukturen og kompleksiteten i virksomhedens it-miljø. Virksomheden kan have ældre it-systemer i forskellige forretningsområder, som ikke er tilstrækkeligt eller hensigtsmæssigt integreret og således resulterer i et komplekst it-miljø.

It-relaterede risici kan føre til fejlagtig tillid til systemer eller programmer, som behandler data unøjagtigt og/eller behandler unøjagtige data.

Ofte vil it-applikationer for den mindre komplekse virksomhed være portaler og/eller være beliggende hos en serviceleverandør. Denne tredjepart vil være ansvarlig for de fleste generelle it-kontroller i it-infrastrukturen og it-applikationerne. Det bliver også mere udbredt, at virksomheder anvender eksterne eller interne serviceudbydere til aspekter af it-miljøet. Det kan være, virksomheden har outsourcet hele eller dele af it-miljøet til en tredjepart, eller anvender et shared service center til central styring af it-processer i en koncern. I disse tilfælde er det vigtigt, at revisor forholder sig til de kontroller, som serviceleverandøren udfører på vegne af virksomheden. En relevant handling fra revisor kan være at indhente en ISAE 3402-erklæring fra serviceleverandøren. I en ISAE 3402-erklæring vil de komplementerende kontroller i brugervirksomheden, som revisor skal identificere og vurdere samt eventuelt teste under sin revision, fremgå.

Eksempler herpå kan være:

- Uautoriseret adgang til data
- Mange brugere har adgang til en fælles database
- It-medarbejderes adgangsrettigheder/ superbrugere
- Manglende funktionsadskillelse
- Uautoriserede ændringer af data i stamfiler, systemer eller programmer
- Manglende nødvendige ændringer af systemer eller programmer
- Upassende manuel indgriben
- Tab af data eller manglende mulighed for at få adgang til data.

I afsnit 26 i ISA 315 (ajourført) kræves det endvidere, at revisor identificerer og vurderer generelle it-kontroller for it-applikationer og andre aspekter af it-miljøet, som revisor har fastlagt som værende udsat for risici, der knytter sig til brugen af it. Baggrunden herfor er, at generelle it-kontroller understøtter den fortsatte effektive funktion af informationsbehandlingskontroller. En generel it-kontrol alene er typisk ikke tilstrækkelig til at adressere en risiko for væsentlig fejlinformation på revisionsmålsniveau, da den så at sige rammer bredt og dermed ikke specifikt adresserer en fejl på revisionsmålsniveau. Generelle it-kontroller er kontroller, der er knyttet til virksomhedens it-processer, som understøtter en fortsat passende drift af virksomhedens it-miljø. Generelle it-kontroller skal sikre, at virksomhedens informationsbehandlingskontroller fortsat fungerer effektivt og understøtter integriteten af information i virksomhedens informationssystem. Integritet skal sikre informationens fuldstændighed, nøjagtighed og gyldighed. Generelle it-kontroller er politikker og processer, som understøtter mange applikationer, der gør, at informationsbehandlingskontroller fungerer effektivt. Generelle it-kontroller, som bibeholder informationers integritet og sikkerheden af informationer, omfatter normalt kontroller med reference til:

- Adgangssikkerhed
- Ændringshåndtering
- Drift af it-anvendelsen.

Informationsbehandlingskontroller er kontroller knyttet til behandlingen af information i it-applikationer eller manuelle informationsprocesser i virksomhedens informationssystem.

Virksomhedens it-miljø er de it-applikationer og understøttende it-infrastruktur samt it-processer og personale involveret i disse processer, som en virksomhed anvender til at understøtte virksomhedens drift og gennemføre forretningsstrategier.

En it-applikation er et program eller et sæt af programmer, der bruges til at igangsætte, behandle, registrere og rapportere transaktioner eller oplysninger. It-applikationer omfatter også data, warehouseløsninger og værktøjer til generering af rapporter. It-infrastruktur omfatter netværk, operativsystemer og databaser samt tilknyttet hardware og software.

Revisor skal have identificeret it-miljøet med relevans for regnskabsaflæggelsen. Et typisk it-miljø med angivelse af anvendte it-applikationer og generelle it-kontroller samt informationsbehandlingskontroller kan skitseres som i figur 1.

Som det fremgår af figuren, vil revisor anvende et Top Down approach til identifikation af it-miljøet. Under planlægning af revisionen vil revisor identificere de betydelige regnskabsposter i regnskabet med tilhørende revisionsmål. Regnskabsposterne er dannet ud fra transaktioner i perioden, der dannes i virksomhedens transaktionsstrømme i de forskellige forretningsprocesser, herunder:

- Salgsprocessen (indtægter, debitorer, likvide midler, moms)
- Indkøbsprocessen (vareforbrug, eksterne omkostninger, anskaffelse af anlægsaktiver, likvider, kreditorer, moms)
- Lønprocessen (personaleomkostninger, likvider, lønrelaterede gældsposter (A-skat, atp, feriepengehensættelse)
- Regnskabsafslutningsprocessen (alle væsentlige regnskabsposter og revisionsmål i regnskabsperioden og på balancetidspunktet).

Transaktionsstrømmene i forretningsprocesserne dannes i forskellige it-applikationer, der understøtter processerne. It-applikationer hos en typisk mindre kompleks virksomhed er eksempelvis følgende:

- Finansapplikation (fx Dynamics C5, Dynamics 365, e-conomic, Dinero)
- Virksomhedens netbank
- Lønsystem (Bluegarden, Danløn, Visma DataLøn, Salary).

It-applikationerne afvikles via og i følgende elementer i it-infrastrukturen:

- Databaser (fx MS SQL, MySQL, Oracle, Native)
- Operativsystem (Windows, Unix, Linux, macOS)
- Netværk
- Cloud Services (infratruktur, platforme eller applikationer hosted af serviceleverandører, der gør services tilgængelige for brugerne via internettet).

It-processer er virksomhedens processer for styring af adgange til it-miljøet, styring af ændringer til programmer eller til it-miljøet samt administration af it-driftsafviklingen.

Ofte vil it-applikationer for den mindre komplekse virksomhed være portaler og/eller være beliggende hos en serviceleverandør. Denne tredjepart vil være ansvarlig for de fleste generelle it-kontroller i it-infrastrukturen og it-applikationerne. Det bliver også mere udbredt, at virksomheder anvender eksterne eller interne serviceudbydere til aspekter af it-miljøet. Det kan være, virksomheden har outsourcet hele eller dele af it-miljøet til en tredjepart, eller anvender et shared service center til central styring af it-processer i en koncern.

I disse tilfælde er det vigtigt, at revisor forholder sig til de kontroller, som serviceleverandøren udfører på vegne af virksomheden. En relevant handling fra revisor kan være at indhente en ISAE 3402-erklæring fra serviceleverandøren. I en ISAE 3402-erklæring vil de komplementerende kontroller i brugervirksomheden, som revisor skal identificere og vurdere samt eventuelt teste under sin revision, fremgå.

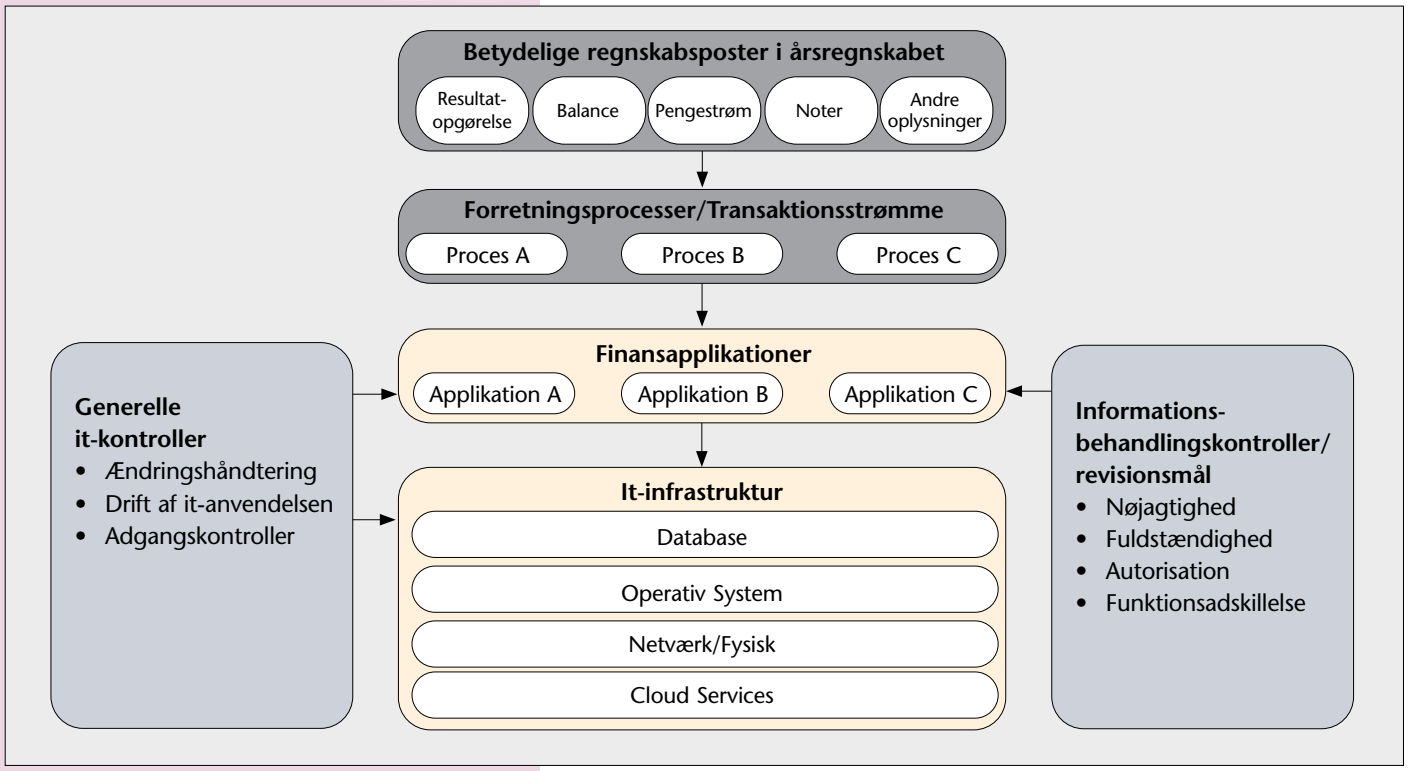
Eksempler på komplementerende kontroller, som brugervirksomheden designer og implementerer, er følgende:

- Tildeling, ændring og fjernelse af brugerrettigheder for brugervirksomhedens medarbejdere
- Etablering af passende funktionsadskillelse i applikation for brugervirksomheden
- Beredskabsplaner – hvordan skal brugervirksomheden fortsætte, hvis it-miljøet midlertidigt er ude af drift?
- Parameteropsætning for brugervirksomheden, fx krav til kodeord, spærring af samlekonti i finanssystem.

Revisor skal være opmærksom på, at en virksomheds forretningsmodel kan være afhængig af brugen af it på forskellige måder. Fx kan en virksomhed sælge sko fra en fysisk butik og i relation hertil anvende et avanceret lager- og kassesystem til at registrere salget af sko. En anden virksomhed sælger måske sko online, hvorfor alle salgstransaktioner behandles i et it-miljø, herunder initiering af transaktionerne via en hjemmeside. For disse to virksomheder er de forretningsrisici, der opstår, væsentligt forskellige som følge af en betydeligt forskellig forretningsmodel, uanset at begge virksomheder basalt set sælger sko. Dette skal revisor forholde sig til.

Virksomhedens forretningsmodel, mål, strategier og tilknyttede forretningsrisici kan resultere i en risiko for væsentlig fejlinformation i regnskabet. Dette gælder også virksomhedens anvendelse af it. Et eksempel vil være en virksomhed, der implementerer et nyt it-system. Implementeringen vil påvirke både drift og regnskabsaflæggelse.

**FIGUR 1**




Kilde: Egen tilvirkning baseret på figuren "Scoping the IT Control Project—Top Down", ISACA, IT Control Objectives for Sarbanes-Oxley: Using COBIT ® 5 in the Design and Implementation of Internal Controls Over Financial Reporting, 3rd Edition, USA, 2014

Som det fremgår af figur 1, vil revisor anvende et Top Down approach til identifikation af it-miljøet. Under planlægning af revisionen vil revisor identificere de betydelige regnskabsposter i regnskabet med tilhørende revisionsmål. Regnskabsposterne er dannet ud fra transaktioner i perioden, der dannes i virksomhedens transaktionsstrømme i de forskellige forretningsprocesser.

Derfor bør revisor opnå en forståelse for, hvordan it kan påvirke en virksomheds målopfyldelse, samt de strategiske overvejelser om den fremtidige it-anvendelse og it-miljøet, herunder om eventuel anvendelse af serviceleverandører. ISA 402[5] beskriver, hvorledes brugervirksomhedens revisor skal forholde sig, når relevante kontroller hos en serviceleverandør eller dennes underleverandører er en del af brugervirksomhedens informationssystem.

Forståelsen af virksomhedens informationspolitikker bidrager til identifikation og vurdering af risici for væsentlig fejlinformation på revisionsmålsniveau ved it-anvendelsen. Disse informationspolitikker definerer strømmene af transaktioner og andre aspekter af virksomhedens aktiviteter knyttet til informationsbehandling med relevans for regnskabsudarbejdelsen. Endvidere vurderes, om elementerne på en passende måde understøtter udarbejdelsen af virksomhedens regnskab. Denne forståelse og vurdering kan også føre til identifikationen af risici for væsentlig fejlinformation på regnskabsniveau, når resultatet af revisors handlinger er inkonsistent med forventningerne til virksomhedens interne kontrolsystem, der kan være baseret på information indhentet i forbindelse med opgaveaccept eller fortsættelse af opgaven.

Informationssystemet og de tilknyttede forretningsprocesser i mindre komplekse virksomheder er sandsynligvis mindre sofistikerede end i store virksomheder. It-miljøet i mindre komplekse virksomheder vil sandsynligvis være mindre komplekst, men informationssystemets rolle er imidlertid lige så vigtig. Mindre komplekse virksomheder med direkte ledelsesinvolvering har måske ikke behov for omfattende beskrivelser af regnskabsprocedurer, sofistikerede regnskabssystemer eller skriftlige politikker. Forståelse af de relevante aspekter af virksomhedens informationssystem kan derfor kræve mindre indsats ved revision af en mindre kompleks virksomhed og kan indebære højere grad af forespørgsler end observation eller gennemgang af dokumentation. Behovet for at opnå en forståelse er imidlertid fortsat vigtigt for at kunne danne et grundlag for designet af yderligere revisionshandlinger i overensstemmelse med ISA 330[6]. Forståelse af it-miljøet kan yderligere hjælpe revisor til at identificere eller vurdere risici for væsentlig fejlinformation.

Forståelse af virksomhedens informationssystem omfatter også en forståelse af de ressourcer, der bruges i virksomhedens aktiviteter knyttet til informationsbehandling. Information om involverede medarbejdere, der kan være relevant for forståelsen af risici forbundet med informationssystemets integritet, omfatter:

- Kompetencer hos de medarbejdere, der udfører arbejdet
- Om der er tilstrækkelige ressourcer, og
- Om der er passende funktionsadskillelse.

## 6. Hvorfor skal revisor forstå det it-miljø, der er relevant for informationssystemet?

Revisors forståelse af informationssystemet omfatter it-miljøet, hvor der er transaktionsstrømme og sker behandling af information, som har relevans for regnskabsaflæggelsen. Virksomhedens brug af it-applikationer eller andre aspekter af it-miljøet giver anledning til risici, der knytter sig til brugen af it. Disse it-relaterede risici kan give anledning til væsentlige fejl i transaktionsstrømmene og dermed i regnskabet. Virksomhedens forretningsmodel samt anvendelsen af it i forretningsmodellen giver brugbar sammenhæng til arten og omfanget af it, som forventes i informationssystemet. Væsentlige fejl eller længerevarende afbrydelser i it-anvendelsen kan medføre store økonomiske tab, der i værste fald kan true virksomhedens fortsatte drift.

Ændringer i transaktionsstrømmen eller oplysninger i informationssystemet kan skyldes programændringer til it-applikationer eller direkte ændring i data i databaser, som anvendes i behandlingen eller i lagring af disse transaktioner eller informationer. I sådanne tilfælde skal årsagen til ændringer i transaktionsstrømmen eller oplysninger identificeres. Det vil ofte være nødvendigt at udføre yderligere handlinger for at sikre, at ændringerne ikke giver fejl i regnskabet.

Det er hensigtsmæssigt, at identifikation af it-applikationer og understøttende it-infrastruktur sker i forbindelse med forståelsen af, hvordan information vedrørende betydelige grupper af transaktioner, balanceposter og oplysninger strømmer ind i, gennem og ud af virksomhedens informationssystem. Dette kan meget vel ske i forbindelse med, at revisionsteamet udfører sin walk through af de forskellige forretningsprocesser, der indgår i revisionen.

Mindre virksomheder har ofte færre ansatte, hvilket kan gøre det vanskeligere at etablere en effektiv funktionsadskillelse. I en ejerledet virksomhed er ejerlederen i stand til at udøve et mere effektivt tilsyn gennem direkte involvering, end det er tilfældet i en større virksomhed, hvilket kan kompensere for de generelt mere begrænsede muligheder for funktionsadskillelse. Dog kan en enkelt persons dominans i ledelsen, som også beskrevet i ISA 240[7], være en potentiel mangel i intern kontrol, da den daglige ledelse har mulighed for at tilsidesætte kontroller. Det bør dog altid tilstræbes at etablere mest mulig funktionsadskillelse. Det oplagte eksempel er adskillelse mellem virksomhedens bogholderifunktion og adgangen til likvider.

Planlægger revisor at teste kontrollernes operationelle effektivitet, kan det være nødvendigt at teste en kombination af kontroller for at bekræfte revisors forventning om, at kontrollerne fungerer effektivt. Revisor kan planlægge at teste både direkte og indirekte kontroller, herunder generelle it-kontroller, og i så fald tage højde for kontrollernes kombinerede forventede indvirkning, når kontrolrisikoen vurderes. I det omfang den testede kontrol ikke fuldt ud adresserer den vurderede iboende risiko, fastlægger revisor betydningen for designet af de yderligere revisionshandlinger for at reducere revisionsrisikoen til et acceptabelt lavt niveau.

Når revisor planlægger at teste en automatiseret kontrols operationelle effektivitet, kan revisor også planlægge at teste den operationelle effektivitet af de relevante generelle it-kontroller, der understøtter den fortsatte funktion af den automatiserede kontrol, for at adressere risiciene, der knytter sig til it-anvendelsen, og for at danne grundlag for revisors forventning om, at den automatiserede kontrol har fungeret effektivt i hele perioden. Når revisor forventer, at tilknyttede generelle it-kontroller er ineffektive, kan denne fastlæggelse have betydning for revisors vurdering af kontrolrisikoen på revisionsmålsniveau, og det kan være nødvendigt, at revisors yderligere revisionshandlinger omfatter substanshandlinger for at adressere de relevante risici, der knytter sig til it-anvendelsen. ISA 330, vejledningsafsnit A29-A30, giver yderligere vejledning til handlinger, som revisor kan udføre under disse omstændigheder.


Det er således yderst vigtigt, at revisor forstår it og it-applikationernes indvirkning på revisionen og den enkelte virksomheds forretningsmodel. Der gælder også på dette område de almindelige spilleregler om, at revisor skal have eller have adgang til de rette kompetencer. Ved involvering af eksperter i form af it-revisorer skal kravene i ISA 620 iagttages og efterleves. It-revisorerne indgår i opgaveteamet på lige fod med de øvrige medlemmer af opgaveteamet. Det vil ofte være hensigtsmæssigt at tilknytte en revisorudpeget ekspert under planlægning af revisionen i virksomheder, hvor it har en vis grad af kompleksitet.

### 7. Dokumentation af revisors forståelse af it-anvendelsen ved virksomhedens regnskabsaflæggelse

Revisor skal i overensstemmelse med ISA 230[8] udarbejde tilstrækkeligt fyldestgørende revisionsdokumentation og i forhold til it-området særligt være opmærksom på at sikre dokumentation for nøgleelementerne i revisors forståelse for:

- Indledende vurdering af omfanget af virksomhedens it-anvendelse:
  - Systemoversigt med vurdering af systemets indflydelse på regnskabsaflæggelsen og regnskabsaflæggelsesprocessen samt virksomhedens drift
  - I hvilken grad anvendelsen af it er integreret i virksomhedens forretningsmodel
  - Den del af it-miljøet, der er relevant for regnskabsaflæggelsen og regnskabsaflæggelsesprocessen
  - It-applikationer og andre dele af it-miljøet, der er relevante for transaktionsstrømme og informationsbehandling
  - Outsourcede it-ydelser (Serviceleverandør – ISA 402 og ISAE 3402-erklæring
- Forhold af betydning for risikovurderingen:
  - Risiko for væsentlige økonomiske tab ved reduktion eller bortfald af it
  - Trusler vedrørende virksomhedens fortsatte drift ved bortfald af it
  - Hvordan it-applikationer og andre aspekter i virksomhedens it-miljø er påvirket af risici, der knytter sig til brugen af it
  - Ødelæggelse/sletning af elektronisk regnskabsmateriale, der kan medføre, at virksomhedens regnskab ikke kan aflægges og/eller revideres
  - Risiko for tilsigtede eller utilsigtede fejl eller mangler i regnskaber som følge af fejlagtig (mis)brug af it
  - Typiske fejl som følge af svagheder ved it-anvendelsen
- Generelle it-kontroller, der er relevante for revisionen.

Opsummeret kan det således konkluderes, at revisor skal sørge for at dokumentere sin forståelse for virksomhedens it-ressourcer, anvendelse af it og generelle it-kontroller.

ISA 315 (ajourført) giver eksempler på indholdet af nøgleelementerne i vejledningsdelen, og det fremgår bl.a. af standarden, at it-applikationer og andre aspekter af it-miljøet med relevans for revisionen set fra revisors synspunkt betyder overvejelser om, hvorvidt applikationerne omfatter:

- Automatiserede kontroller, som den daglige ledelse baserer sig på, og som har relevans for revisionen
- Kontroller, der adresserer risici, hvor substanshandlinger alene ikke giver tilstrækkeligt og egnet revisionsbevis
- Systemgenererede rapporter, som anvendes i revisionen uden at foretage substanstest af input og output
- Opretholdelse af integriteten af informationer, der lagres og behandles i informationssystemet for betydelige grupper af transaktioner, balanceposter og oplysninger.

Det understreges i afsnit 38 i ISA 315 (ajourført), at revisors risikovurderingshandlinger skal dokumenteres. Det kan ske via en egentlig detailplan indeholdende risikovurderingshandlingerne eller et mere overordnet memo, som forklarer de centrale dele af revisors risikovurdering.

Standarden understreger også på dette punkt, at kravene til revisors dokumentation kan skaleres i forhold til virksomhedens størrelse og kompleksitet. Det essentielle i forhold til den gode og fyldestgørende dokumentation vil være at sikre dokumentation for forståelsen af, hvorledes it-anvendelsen i virksomheden potentielt kan medføre forøget risiko for væsentlige fejl i regnskabet. Det er næppe nødvendigt at understrege, at standardens øgede fokus på revisors professionelle skepsis også skal skærpe revisors opmærksomhed herpå ved udførelse af risikovurderingshandlinger relateret til virksomhedens it-anvendelse.

## 8. Anvendelse af revisorudpeget ekspert (it-revisor)

ISA 315 (ajourført) forudsætter, at virksomheder er afhængige af it-anvendelsen. I standarden anerkendes og understreges det dog, at der er forskel på kompleksiteten af virksomhedernes forretningsmodel og interne kontrolsystem. Endvidere er anvendelsen af og kompleksiteten i virksomhedernes it forskellig. De ændringer, der er foretaget i ISA 315 (ajourført) vedrørende it-relaterede forhold i virksomhederne, og de afledte effekter heraf i revisors tilgang til opnåelse af forståelse for it-anvendelsen og de generelle it-kontroller vil formentlig betyde, at der oftere end hidtil vil skulle overvejes inddragelse af revisorudpegede eksperter med særlige kompetencer inden for it-revision. Det skyldes blandt andet vigtigheden af tilstrækkelig forståelse for følgende forhold:

- Konsekvenser for revisionsbevis dannet af regnskabssystemer og andre it-understøttede systemer
- Effektivitet i revision, herunder tilstrækkeligt og egnet revisionsbevis for komplekse og store datamængder / transaktioner
- Adgang til systemer og data
- Ændringshåndtering
- Drift af it-anvendelsen
- Konsekvenser/kompenserende kontroller ved svagheder i generelle kontroller.

Det er således yderst vigtigt, at revisor forstår it og it-applikationernes indvirkning på revisionen og den enkelte virksomheds forretningsmodel.

Der gælder også på dette område de almindelige spilleregler om, at revisor skal have eller have adgang til de rette kompetencer. Ved involvering af eksperter i form af it-revisorer skal kravene i ISA 620[9] iagttages og efterleves. It-revisorerne indgår i opgaveteamet på lige fod med de øvrige medlemmer af opgaveteamet. Det vil ofte være hensigtsmæssigt at tilknytte en revisorudpeget ekspert under planlægning af revisionen i virksomheder, hvor it har en vis grad af kompleksitet. It-revisor vil kun vejlede teamet i forhold til de planlægningsaktiviteter og handlinger, der er nødvendige. Planlægning og udførelse af risikovurderingshandlinger koordineres med it-revisorerne, og typisk vil en væsentlig del af it-revisorernes arbejde kunne udføres på et tidligt tidspunkt i processen. I det hele taget opnås den bedste effektivitet i revisionen ved at involvere it-revisorerne så tidligt som muligt, ligesom it-revisorernes deltagelse i revisionsteamets arbejde i årets løb vil være en gevinst for både revisionsteamet og virksomheden. It-revisorerne kan bl.a. assistere med at vurdere it-baseret revisionsbevis, herunder beviser, der er dannet fra it-applikationer.

I virksomheder, som anvender simple og standardiserede it-systemer, vil der i de fleste tilfælde fortsat ikke være behov for involvering af it-revisorer. Selv med de nye og skærpede krav til revisors fokus på it-anvendelsen i virksomheden er det vores vurdering, at generalistrevisoren har tilstrækkelige kompetencer til at kunne efterleve kravene i ISA 315 (ajourført).

## 9. Opsummering

ISA 315 (ajourført) har øget de forventninger, der kan opstilles til revisors forståelse af og handlinger rettet imod virksomhedens it-anvendelse og it-miljø ved revision. Det er en naturlig udvikling, der stemmer fint overens med den øgede digitalisering, vi alle har mærket i samfundet generelt gennem de seneste år. En stor del af revisionsbevis er dannet fra forskellige it-applikationer. Disse beviser udgør således grundlaget for revisors konklusion på den udførte revision og dermed på revisors erklæring på det reviderede regnskab.

Kravet til revisors forståelse og dokumentation af virksomhedens it-anvendelse ligger de facto i standarden. Standarden lægger op til, at virksomhederne er afhængige af it i forbindelse med regnskabsaflæggelse. Denne afhængighed af it bliver mere udtalt, hvis lovforslaget til ny bogføringslov[10] bliver vedtaget i Folketinget, i og med at stort set alle virksomheder herefter vil blive omfattet af et krav om digital bogføring og opbevaring af regnskabsmateriale.

Anvendelse af it medfører forskellige it-relaterede risici, der ultimativt kan medføre fejl i regnskabet. Virksomhederne implementerer generelle it-kontroller til at håndtere disse it-relaterede risici. Det vil primært være kontroller vedrørende adgangsforhold og ændringer til applikationer og systemer.

For de fleste revisionsopgaver vedrørende mindre virksomheder og mindre komplicerede virksomheder vil der ikke være behov for at anvende en revisorudpeget ekspert (it-revisor) i revisionsprocessen. Det kan dog være hensigtsmæssigt at inddrage en it-revisor i planlægningsfasen, herunder særligt når der skal konkluderes på vurdering af it-relaterede risici og generelle it-kontroller. Det må generelt anbefales at anvende en it-revisor, når it-kompleksiteten i virksomheden øges, og informationsbehandlingskontroller udgør en større del af revisors overbevisning.

Den gode sagsløsning i relation til kravene i ISA 315 (ajourført) må i alle tilfælde dokumentere, om revisor har identificeret og vurderet relevante risici ved virksomhedens it-anvendelse, herunder generelle it-kontroller.

Revisor skal sikre tilstrækkelig dokumentation for nøgleelementerne i sin forståelse for:

- I hvilken grad anvendelsen af it er integreret i virksomhedens forretningsmodel
- Den del af it-miljøet, der er relevant for regnskabsaflæggelsen og regnskabsaflæggelsesprocessen
- It-applikationer og andre dele af it-miljøet, der er relevante for transaktionsstrømme og informationsbehandling
- Hvordan it-applikationer og andre aspekter i virksomhedens it-miljø er påvirket af risici, der knytter sig til brugen af it
- Generelle it-kontroller, der er relevante for revisionen.

Revisor skal også i relation til risici, der er affødt af virksomhedens anvendelse af it, demonstrere sin professionelle skepsis ved planlægning og udførelse af risikovurderingshandlinger.

Samlet set må det anbefales, at revisor sikrer tilstrækkelig dokumentation af risikovurderingshandlinger relateret til it-anvendelsen og gennemgangen af generelle it-kontroller.

## Noter

1 Seneste ajourførte udgave er ISA 315 (ajourført), *Identifikation og vurdering af risici for væsentlig fejlinformation igennem forståelse af virksomheden og dens omgivelser*, December 2016

2 ISA 315 (ajourført 2019), *Identifikation og vurdering af risici for væsentlig fejlinformation*

3 ISAE 3402, *Erklæringsopgaver med sikkerhed om kontroller hos en serviceleverandør*, December 2016

4 ISA 500, *Revisionsbevis*, December 2016

5 ISA 402, *Revisionsmæssige overvejelser vedrørende en virksomhed, der anvender serviceleverandør*, September 2014

6 ISA 330, *Revisors reaktion på vurderede risici*, December 2016

7 ISA 240, *Revisors ansvar vedrørende besvigelser ved revision af regnskabet (ajourført)*, December 2016

8 ISA 230, *Revisionsdokumentation*, December 2016

9 ISA 620, *Anvendelse af en revisorudpeget eksperts arbejde*, April 2009

10 L 163, Forslag til lov om bogføring, fremsat 6. april 2022.

Kravet til revisors forståelse og dokumentation af virksomhedens it-anvendelse ligger de facto i standarden. Standarden lægger op til, at virksomhederne er afhængige af it i forbindelse med regnskabsaflæggelse. Denne afhængighed af it bliver mere udtalt, hvis lovforslaget til ny bogføringslov bliver vedtaget i Folketinget, i og med at stort set alle virksomheder herefter vil blive omfattet af et krav om digital bogføring og opbevaring af regnskabsmateriale. Anvendelse af it medfører forskellige it-relaterede risici, der ultimativt kan medføre fejl i regnskabet. Virksomhederne implementerer generelle it-kontroller til at håndtere disse it relaterede risici. Det vil primært være kontroller vedrørende adgangsforhold og ændringer til applikationer og systemer. For de fleste revisionsopgaver vedrørende mindre virksomheder og mindre komplicerede virksomheder vil der ikke være behov for at anvende en revisorudpeget ekspert (it-revisor) i revisionsprocessen.