



ØKONOMISTYRELSEN

Vejledning om intern finansiell kontrol

Maj 2020

2020

Indhold

1. Indledning	3
1.1 Baggrund og formål	4
1.2 Afgrænsning	5
1.3 Målgruppe	5
1.4 Læsevejledning	5
2. Gældende regelsæt for intern finansiel kontrol	7
2.1 Krav til intern finansiel kontrol	8
2.2 Særligt om sammenhængen mellem krav og vejledning	12
3. Fremgangsmåde for tilrettelæggelse af intern finansiel kontrol	14
3.1 Opbygning af et internt finansielt kontrolsystem	15
A. Etablering af kontrolsystem for interne finansielle kontroller	16
B. Levedygtigt og dynamisk kontrolsystem over tid	23
4. Implementering – forslag til redskaber	31
4.1 Redskaber til etablering af kontrolsystem	31
A. Redskaber til etablering af kontrolsystem	31
B. Redskaber til levedygtigt og dynamisk kontrolsystem over tid	38
5. Appendiks – skabeloner med redskaber	

Kapitel 1. Indledning

1. Indledning

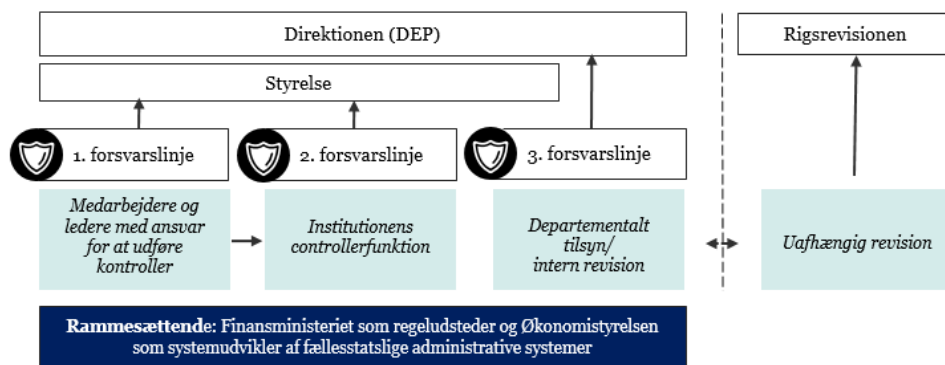
Forsvarlig forvaltning af offentlige midler forudsætter gode interne finansielle kontroller.

Denne vejledning beskriver, hvordan ministerier, virksomheder og institutioner kan tilrettelægge arbejdet med interne finansielle kontroller inden for gældende regler.

1.1 Baggrund og formål

Det er afgørende, at borgere og virksomheder kan stole på, at offentlige midler forvaltes forsvarligt. Det forudsætter bl.a. et kontinuert ledelsesmæssigt fokus på, om der er iværksat tilstrækkelige kontroller eller andre foranstaltninger til at imødegå de risici, der knytter sig til ressourcernes anvendelse.

Denne vejledning beskriver, hvordan ministerier, virksomheder og institutioner mv. kan tilrettelægge arbejdet med interne finansielle kontroller inden for gældende regler. Med bevidsthed om forskellige roller og ansvar for intern finansiell kontrol i den enkelte organisation og ift. eksterne parter. Nedenstående skitserer de tre forsvarslinjer i det overordnede kontrolsystem, som skal reducere muligheden for, at der kan ske økonomisk svindel eller misbrug. Endvidere fremgår Rigsrevisionens rolle som ekstern, uafhængig revision. Forsvarslinjerne beskrives nærmere i afsnit B2 i kapitel 3.



Vejledningen opsummerer de gældende regler, roller og ansvar samt giver inspiration, råd og vejledning. Sidstnævnte er ikke normsættende.

1.2 Afgrænsning

Nærværende vejledning fokuserer alene på det finansielle område, herunder finansielle risici. Det betyder, at begreberne 'intern kontrol' og 'internt kontrolsystem' i denne sammenhæng alene vedrører finansielle kontroller og finansielle kontrolsystemer ift. finansielle processer, såsom fx ind- og udbetalinger, regnskabsregistreringer o.lign. Vejledningen omhandler i særlig grad de finansielle processer, der skal sikre regnskabet's rigtighed.

Processer og strukturer for overvågning og tilpasning af kontrolsystemet ud over finansielle risici behandles ikke. Endvidere er generelle it-kontroller, rettet mod virksomhedens it-infrastruktur og it-drift, ikke omfattet af denne vejledning, selvom de også er grundlæggende i et godt kontrolmiljø, hvor forretningsgangene understøttes af it-systemer. Se Økonomistyrelsens hjemmeside for et overblik over alle relevante vejledninger ift. kontrol og risikostyring.

1.3 Målgruppe

Vejledningen henvender sig til ledelsen i alle departementer samt ledelsen i alle statslige institutioner, som er overordnet ansvarlige for tilrettelæggelse af arbejdet med intern kontrol. Vejledningen henvender sig derudover specifikt til økonomichefer og medarbejdere i alle statslige institutioner eller virksomheder, der har ansvar for eller deltager i arbejdet med intern kontrol.

1.4 Læsevejledning

Vejledningen er struktureret om følgende tre emner:

- **Gældende regelsæt** for intern finansiell kontrol inkl. ansvar for efterlevelsen heraf.
- **Fremgangsmåde** for opbygning af et kontrolsystem ift. intern finansiell kontrol.
- **Implementering** – forslag til konkrete redskaber til brug under opbygning og vedligeholdelse af kontrolsystemet med tilhørende eksempler.

Afslutningsvist indgår et appendiks, som indeholder skabeloner til de redskaber, der præsenteres i kapitlet om implementering.

I vejledningen anvendes en række centrale begreber. De væsentligste nøglebegreber er gengivet nedenfor og bliver udfoldet yderligere i kapitel 3 og 4.

Faktaboks – Væsentlige nøglebegreber for tilrettelæggelse af arbejdet med interne finansielle kontroller

De tre forsvarslinjer

- De *tre forsvarslinjer* beskriver roller og ansvar for intern finansiell kontrol i den enkelte organisation (1. forsvarslinje: Medarbejdere og ledere, 2. forsvarslinje: Institutionens kontrolfunktion og 3. forsvarslinje: Departementets kontrol- og tilsynsfunktion). Se nærmere beskrivelse i afsnit B2, kapitel 3.

Finansiell proces

- En *finansiell proces* dækker over alle transaktioner ift. regnskabet (dvs. alle led i processen), herunder ud- eller indbetalingsstrømme. Det kan eksempelvis være udbetaling af puljetilskud, udbetaling af løn, køb af varer og tjenester, overførselsindtægter fra kommuner, returkommission mv. Se nærmere beskrivelse i kapitel 3 og redskaber i kapitel 4.

Intern finansiell kontrol

- En *intern finansiell kontrol* er en aktivitet, der bidrager til at sikre en finansiell transaktions gyldighed og rigtighed og herigennem øger sikkerheden for regnskabets rigtighed. Interne finansielle kontroller kan være system- eller personbårne, og de kan være forebyggende eller opdagende og korrigerende. Se nærmere beskrivelse i kapitel 3 og redskaber i kapitel 4.

Finansielt internt kontrolsystem

- Et *finansielt internt kontrolsystem* er en systematik og struktur, der sikrer, at der ift. de finansielle processer i organisationen er tilstrækkelige og relevante interne kontroller til at begrænse risikoen for tilsigtede og utilsigtede fejl. Se nærmere beskrivelse i kapitel 3 og redskaber i kapitel 4.

Funktionsadskillelse

- Centralt i et internt finansielt kontrolsystem er princippet om *funktionsadskillelse*, som betyder, at der på tværs af en finansiell proces er interne kontroller, der sikrer en personmæssig adskillelse (to eller flere) mellem adgangen til at disponere, godkende, bogføre og betale, såvel direkte som indirekte. Se nærmere beskrivelse i afsnit 2.1.1, i kapitel 2.

Iboende risici

- Den iboende risiko er den risiko, der eksisterer som følge af aktiviteterne, transaktionernes eller forvaltningsstrukturernes art og kompleksitet, og som er så væsentlige, at der kan opstå afvigelser i regnskabets rigtighed. Se nærmere beskrivelse i kapitel 3.

Designeffektivitet

- Designeffektivitet udtrykker en kontrols tilstrækkelighed (hvorvidt den enkelte interne kontrol efter dens design og udformning reelt vil kunne reducere den specifikke risikoeksponering) og relevans (hvorvidt den interne kontrols placering i procesforløbet understøtter dens effektivitet i forhold til den konkrete risiko). Se nærmere i kapitel 3 og redskab i kapitel 4.

Funktionel effektivitet

- Funktionel effektivitet udtrykker, baseret på efterprøvning af de kontroller, der er fundet tilstrækkelige, relevante og vigtige, hvorvidt etablerede finansielle interne kontroller faktisk udføres og fungerer. Se nærmere i kapitel 3 og redskab i kapitel 4.

Kapitel 2.

Gældende regelsæt for intern finansiel kontrol

2. Gældende regelsæt for intern finansiel kontrol

Regnskabsbekendtgørelsen er et af de primære regelsæt, der fastsætter og tydeliggør en række regler til ministerier, virksomheder og regnskabsførende institutioner i forhold til deres tilrettelæggelse af den interne kontrol- og risikostyring. Bl.a. fastlægger bekendtgørelsen, at institutionens ledelse er ansvarlig for, at der er etableret tilstrækkelige forretningsgange og interne kontroller.

2.1 Krav til intern finansiel kontrol

Regnskabsbekendtgørelse nr. 116 af 19. februar 2018 om statens regnskabsvæsen mv. (regnskabsbekendtgørelsen) udgør et centralt regelgrundlag for en robust og sikker regnskabsmæssig forvaltning i staten. Ifølge §1 i bekendtgørelsen skal denne **bidrage til at sikre en sikker og effektiv økonomiforvaltning på alle niveauer i staten**, herunder selvejeområdet. Økonomiforvaltningen skal desuden i størst muligt omfang foregå digitalt med brug af færrest mulige ressourcer og størst mulig automatisering.

2.1.1 Opgaver ift. kontrol

Af regnskabsbekendtgørelsen fremgår en række konkrete regler, der skal iagttages i tilrettelæggelsen af et internt kontrolsystem.

1) Sikre funktionsadskillelse

Der skal (ifølge regnskabsbekendtgørelsens § 24) sikres personmæssig adskillelse mellem den regnskabsmæssige registrering og betaling. Hvis det ikke er muligt, skal det beskrives i regnskabsinstruksen, hvordan betalingerne så kontrolleres. Læs mere herom i nedenstående faktaboks.

2) Kontrol af grundlaget for ind- og udbetalinger

Der skal endvidere udarbejdes og gennemføres de nødvendige kontroller af grundlaget for ind- og udbetalingerne samt den faktiske effektivering heraf, jf. regnskabsbekendtgørelsens § 28, stk. 2. Kontrollerne tilrettelægges under hensyntagen til betalingernes størrelse og frekvens. Læs mere om hvordan i kapitel 3.

3) Etablering af tilsyn med forretningsgange og interne kontroller

Der skal (ifølge regnskabsbekendtgørelsens § 37, stk. 2) etableres forretningsgange og interne kontroller under hensyntagen til væsentlighed og risiko, som sikrer en korrekt regnskabsaflæggelse. I den forbindelse skal det sikres, at der er etableret et tilsyn med at de påkrævede forretningsgange og interne kontroller er etableret. Forretningsgange og interne kontroller beskrives i institutionens regnskabsinstruks. Læs mere herom under afsnit B2 i kapitel 3.

4) Forsvarlig forvaltning af udgifter og indtægter

I forlængelse af punkt tre fremgår det af regnskabsbekendtgørelsens § 46, at alle regnskabsførende institutioner skal foretage en forsvarlig forvaltning af udgifter og indtægter. Forretningsgange og interne kontroller i forbindelse hermed skal fastlægges i regnskabsinstruksen under hensyntagen til væsentlighed og risiko.

a) Disponering

Forretningsgange og interne kontroller skal sikre, at disponering af indtægter og udgifter foretages i overensstemmelse med givne bevilninger og i henhold til de bestemmelser mv., der fremgår af regnskabsinstruksen.

b) Godkendelse af disponering

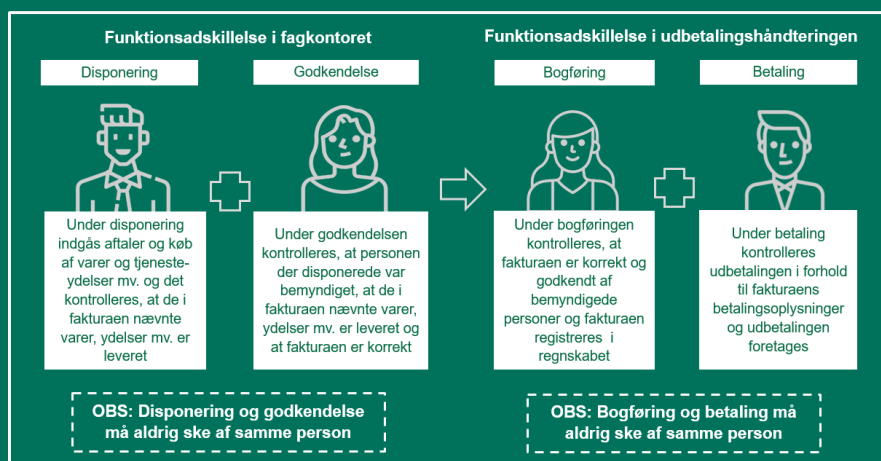
Endvidere skal forretningsgange og interne kontroller sikre, at godkendelse af indtægts- og udgiftsbilag omfatter bilagets materielle og økonomiske indhold. Det betyder, at der skal føres kontrol med, at bilaget er i overensstemmelse med indgåede aftaler og bemyndigelser, og at de i bilaget nævnte varer, ydelser mv. er leveret. Hvor der ikke foreligger en direkte modydelse (fx hvis det er et tilskud), skal der ved godkendelsen føres kontrol med, at grundlaget for indtægten eller udgiften er korrekt, og at de fastlagte arbejdsgange og procedurer er fulgt. Det skal også kontrolleres, at bilaget er korrekt, herunder at der er anvendt de rigtige priser og at beregninger stemmer.

5) Kontrol med anvendelse af betalingskort

Anvendelse af betalingskort skal fremgå af institutionens regnskabsinstruks. De nærmere retningslinjer er beskrevet i cirkulære om anvendelse af betalingskort og den tilhørende vejledning (se nærmere på Økonomitstyrelsens hjemmeside). Heri fremgår, at institutionen i regnskabsinstruksen skal beskrive principper for udstedelse og anvendelse.

Faktaboks - Funktionsadskillelse

- Centralt i et internt kontrolsystem er princippet om *funktionsadskillelse*, som betyder, at der på tværs af en finansiel proces er interne kontroller, der sikrer en personmæssig adskillelse (to eller flere) mellem adgangen til at disponere, godkende, bogføre og betale, såvel direkte som indirekte. Endvidere er det vigtigt, at der er funktionsadskillelse så fx stamdata er beskyttet mod tilsigtede og utilsigtede fejl.



- Det er centralt, at den ansvarlige ledelse forholder sig til kvaliteten af funktionsadskillelsen, dvs. hvilken kontrol der reelt udføres ift. om funktionsadskillelsen efterleves i praksis.

2.1.2 Styring

Styringen af de regnskabsmæssige opgaver, herunder tilrettelæggelsen af et tilstrækkeligt internt kontrolmiljø, skal varetages, så opgavernes placering på de forskellige organisatoriske niveauer er klar og entydig. Af regnskabsbekendtgørelsen er disse opgaver fastlagt og opdelt i henholdsvis en ministerie-, virksomheds-, og regnskabsinstruks. Ministerier, virksomheder og regnskabsførende institutioner skal i deres respektive instrukser indarbejde hovedelementerne i deres tilrettelæggelse af den interne kontrol- og risikostyring i forbindelse med regnskabsaflæggelsen.

Hovedelementerne i *ministeriets* overordnede regnskabsforvaltning, herunder tilrettelæggelse af den interne kontrol- og risikostyring, samt tilsyn med udførende enheder i forbindelse med regnskabsaflæggelsen skal (ifølge regnskabsbekendtgørelsens § 14, stk. 1 nr. 2) beskrives i **ministerieinstruksen**. Departementets ledelse skal godkende ministerieinstruksen, som sendes til virksomhederne på ministerområdet.

De underliggende *virksomheder* skal (ifølge regnskabsbekendtgørelsens § 17, stk. 1 nr. 4) udarbejde og ajourføre en **virksomhedsinstruks**, der indeholder den enkelte virksomheds tilrettelæggelse af den interne kontrol- og risikostyring, herunder hvordan der føres tilsyn med eventuelt underliggende regnskabsførende enheder. Virksomhedsinstrukserne skal godkendes af departementets ledelse og sendes til underliggende enheder.

I det omfang der under virksomhederne findes regnskabsførende *institutioner*, skal (ifølge regnskabsbekendtgørelsens § 21, stk. 1 nr. 3) disse institutioner udarbejde og ajourføre en **regnskabsinstruks**. Regnskabsinstruksen skal indeholde en beskrivelse af forretningsgangene for forvaltningen af indtægter og udgifter samt tilrettelæggelsen af den interne kontrol- og risikostyring i forbindelse med regnskabsaflæggelsen. Regnskabsinstruksen skal godkendes af institutionens ledelse og sendes til virksomheden til orientering.

2.1.3 Ledelsens ansvar

Ledelsen i departementerne har ansvaret for, at der på hele ministerområdet, dvs. inkl. underliggende institutioner, er **etableret forretningsgange og interne kontroller**, herunder funktionsadskillelse, som i videst muligt omfang sikrer, at dispositioner er i overensstemmelse med meddelte bevillinger, love og andre forskrifter samt med indgåede aftaler og sædvanlig praksis.

Ledelsen i departementerne skal (ifølge regnskabsbekendtgørelsens § 37, stk. 3) desuden minimum årligt sikre, at der er **etableret et tilsyn med virksomhederne og regnskabsførende institutioner under hensyntagen til væsentlighed og risiko**, som sikrer, at der er etableret forretningsgange og interne kontroller i forhold til underliggende virksomheder og regnskabsførende institutioner samt overholdelsen heraf.

Ved tilrettelæggelsen af regnskabsvæsenet skal ledelsen i departementerne endvidere sikre, at virksomhederne og de regnskabsførende institutioner har en sådan størrelse, at de kan gennemføre en forsvarlig tilrettelæggelse af regnskabsvæsenet.

Ledelsen på ministerielt, virksomheds- og regnskabsførende niveau har ansvaret for, at **forretningsgangene og de interne kontroller fastlægges under hensyntagen til væsentlighed og risiko**, som sikrer en korrekt regnskabsaflæggelse. For at kunne vurdere de fastlagte kontroller, kan ledelsen efterspørge information om grundlaget og dermed få viden, der kan anvendes til at vurdere behovet for supplerende tiltag, der kan styrke de finansielle kontroller. Ledelsen **skal ved ændringer og som minimum årligt følge op på**, at de påkrævede forretningsgange og interne kontroller er etableret.

Endeligt er det ledelsens ansvar på ministerielt, virksomheds- og regnskabsførende niveau at udarbejde en **regnskabsaflæggelse** i overensstemmelse med de statslige regnskabsregler.

Ledelsen i virksomhederne skal (ifølge regnskabsbekendtgørelsens § 39, stk. 4) **årligt i påtegningen af årsrapporten erklære**, at den er rigtig, dvs. at årsrapporten ikke indeholder væsentlige fejlinformationer eller udeladelser, herunder at måloppstillingen og målrapporteringen i årsrapporten er fyldestgørende samt at der er etableret forretningsgange og interne kontroller, der sikrer en økonomisk hensigtsmæssig forvaltning af de midler og ved driften af de institutioner, der er omfattet af årsrapporten.

Ledelsen i departementerne påtegner ligeledes årsrapporterne og erklærer dermed, at departementet har varetaget sin tilsynsforpligtelse i forhold til virksomhedens finansielle regnskab og regnskabsmæssige forklaringer. For de øvrige dele af årsrapporten tilkendegiver departementet, at oplysningerne ifølge departementets vurdering giver et dækkende billede af virksomhedens drift.

Yderligere skal **ledelsen i departementerne** i forbindelse med aflæggelsen af statsregnskabet godkende ministerområdets årlige regnskab (regnskabsbekendtgørelsens § 36, stk. 3 og 4). Godkendelsen af deres årlige regnskab sker via en regnskabserklæring, hvori det erklæres:

- om der er ændringer i regnskabsprincipperne, der har betydning for vurderingen af regnskabet for det pågældende finansår,
- om regnskabet indeholder alle de bogføringskredse og delregnskaber, som ministerområdet er ansvarlig for,
- om forbruget af bevillinger er opgjort korrekt,
- om aktiver og passiver er opgjort korrekt, og
- om der inden for ministerområdet er etableret forretningsgange og interne kontroller, som i videst muligt omfang sikrer, at de dispositioner, som er omfattet af regnskabsaflæggelsen, er i overensstemmelse med meddelte bevillinger, love og andre forskrifter samt med indgåede aftaler og sædvanlig praksis.

Departementernes godkendelse af ministerområdets årlige regnskab og påtegning af årsrapporterne skal ske på højest mulige ledelsesniveau i overensstemmelse med interne bemyndigelser.

2.2 Særligt om sammenhængen mellem krav og vejledning

Økonomistyrelsen fastsætter **ikke specifikke krav til, hvordan** ministerier, virksomheder og regnskabsførende institutioner tilrettelægger deres interne kontrol i forbindelse med regnskabsaflæggelsen, fordi **tilrettelæggelsen vil være et individuelt forhold**.

Tilrettelæggelsen skal ske under hensyntagen til de systemer (Navision Stat, SKS, IndFak, RejsUd, Statens Budgetsystem, SLS, HR-løn), som Økonomistyrelsen stiller til rådighed, og som institutionerne er forpligtet til at anvende, ligesom der skal tages hensyn til andre relevante fødesystemer fx tilskudsadministrerende systemer. For hvert system, som Økonomistyrelsen stiller til rådighed, er der udarbejdet servicebeskrivelser, som beskriver opgave- og ansvarsfordelingen mellem Økonomistyrelsen og institutionerne, herunder hvilke kontroller Økonomistyrelsen sikrer gennemført. [Servicebeskrivelserne](#) findes på Økonomistyrelsens hjemmeside.

Institutioner, der i henhold til regnskabsbekendtgørelsens § 11, stk. 4, har fået tilladelse til at anvende andre systemer end de, som Økonomistyrelsen stiller til rådighed, skal sikre, at der gennemføres tilsvarende kontroller i forhold til disse systemer.

Kapitel 3.

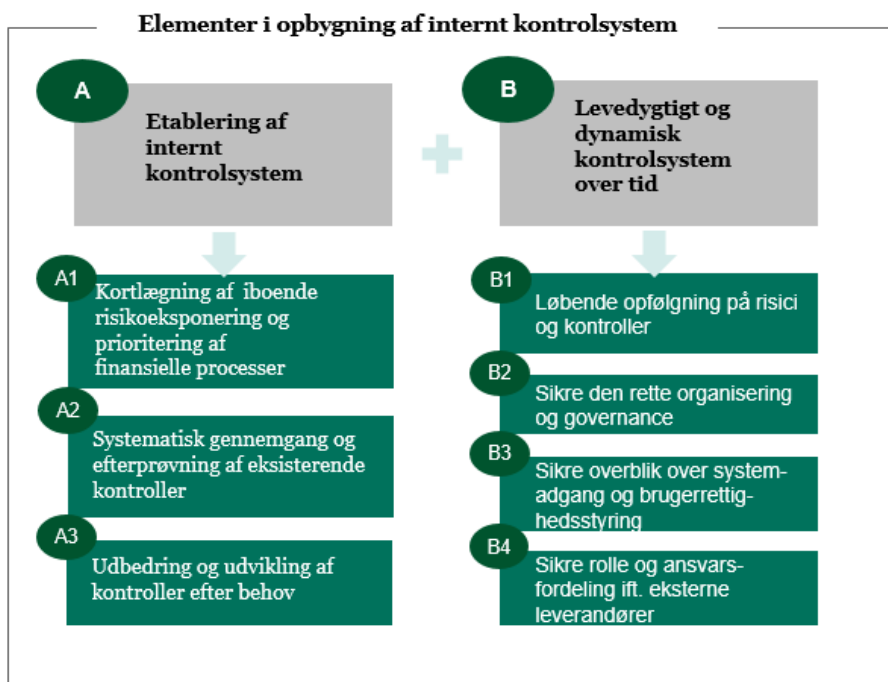
Fremgangsmåde for tilrettelæggelse af intern finansiel kontrol

3. Tilrettelæggelse af intern finansiel kontrol

Hvad er et internt kontrolsystem? Dette kapitel gennemgår, hvad intern finansiel kontrol indeholder, herunder fremgangsmåden ift. hvorledes et finansielt kontrolsystem kan etableres.

3.1 Opbygning af et internt finansielt kontrolsystem

Nedenfor beskrives, hvordan et kontrolsystem kan udvikles og vedligeholdes. Dette består af følgende elementer:



Først skal virksomheden **etablere et internt kontrolsystem** for de **finansielle processer**, som sikrer, at risikoen for utilsigtede og tilsigtede (fx svig og korrupsion) fejl er acceptabel. Som led heri kortlægges og vurderes alle iboende risici og eksisterende kontroller i de finansielle processer. Trin A1 til A3 beskrives nærmere i det følgende.

Dernæst skal virksomheden **etablere kontinuerlig overvågning og tilpasning af det interne kontrolsystem** til sikring af, at kontrolsystemet bliver levedygtigt og løbende tilpasses en ændret risikoeksponering. Vigtige elementer beskrives i trin B1 til B4 i det følgende.

Faktaboks – Definition af finansielle kontroller og kontrolsystem

Intern finansiell kontrol

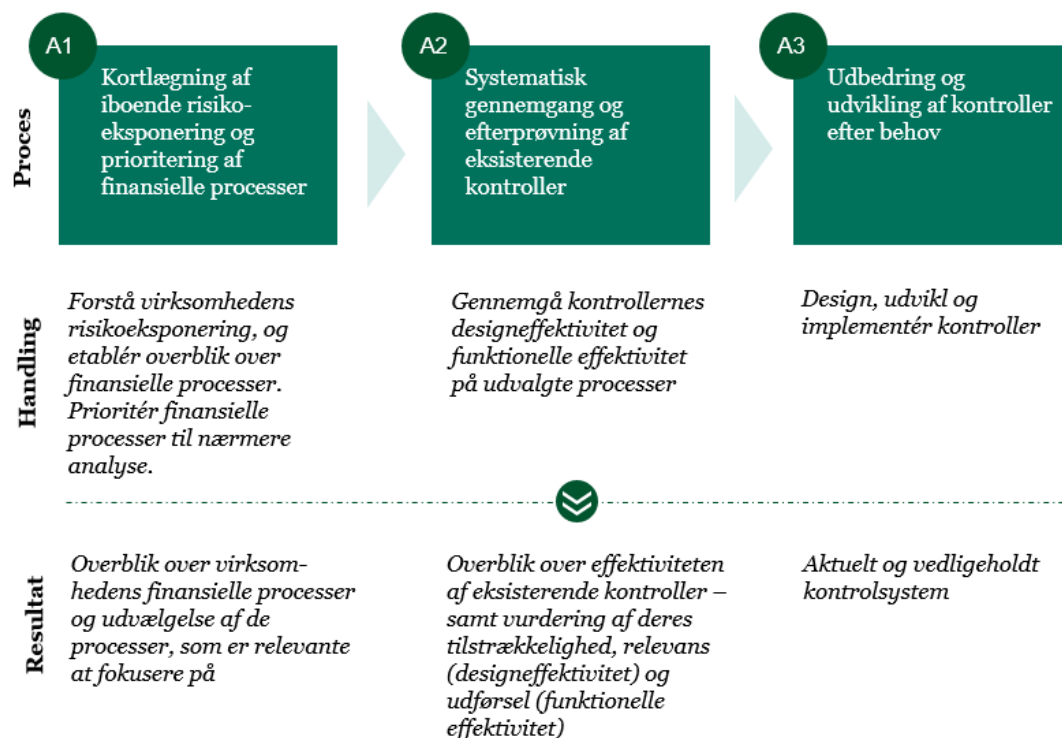
- En *finansiell intern kontrol* er en aktivitet, der bidrager til at sikre en finansiell transaktions gyldighed og rigtighed og herigennem øger sikkerheden for regnskabets rigtighed. Interne finansielle kontroller kan være system- eller personbårne, og de kan være forebyggende eller opdagende og korrigerende.

Internt finansielt kontrolsystem

- Et *internt finansielt kontrolsystem* er en systematik og struktur, der sikrer, at der i organisationens finansielle processer er tilstrækkelige og relevante interne kontroller til at begrænse risikoen for tilsigtede og utilsigtede fejl.

A. Etablering af kontrolsystem for interne finansielle kontroller

Med baggrund i regnskabsbekendtgørelsen skal statens institutioner etablere et internt finansielt kontrolsystem. Tilrettelæggelse kan følge følgende tretrinmodel:



Trin A1 omfatter en **kortlægning** af alle de risici, virksomheden samlet set er eksponeret for (**iboende risici**), herunder identifikation og risikokarakteristik af virksomhedens finansielle processer. Denne kortlægning af de iboende risici er afgørende for efterfølgende at kunne prioritere, hvilke kontrolforanstaltninger, der mest effektivt vil kunne imødegå de identificerede risici, herunder designet og omfanget af kontrollerne. Hertil understøtter dette indledende overblik en stillingstagnation til, hvilket risikoniveau der kan accepteres for den enkelte finansielle proces.

Trin A2 vedrører en **systematisk gennemgang og efterprøvning** af de interne kontroller. Efterprøvningen er en test af, om den interne kontrol effektivt imødegår de konkrete iboende risici, som kontrollerne er designet til at imødegå.

Trin A3 vedrører en **udbedring og udvikling af kontrollerne** for de finansielle processer, hvor dette vurderes relevant – således at risikoniveauet pr. proces bringes til og fastholdes på det ønskede niveau.

Nedenfor uddybes de enkelte trin, og det gennemgås, hvordan disse samlet set bidrager til en opbygning af et finansielt internt kontrolsystem, der minimerer risikoen for tilsigtede og utilsigtede fejl.

A1 *Kortlægning af iboende risikoeksponering og prioritering af finansielle processer*

I det følgende uddybes de to primære aktiviteter: 1) etablering af et overblik over, hvilke iboende risici virksomheden samlet set er eksponeret over for, og 2) identifikation og prioritering af finansielle processer.

Få overblik over risikoeksponering gennem kortlægning

Der etableres et **overblik over**, hvilke risici virksomheden samlet set er eksponeret for - disse betegnes **de iboende risici**. Dette første skridt gennemføres uden hensyn til effekten af allerede etablerede interne kontroller. Dette er for at sikre et virksomhedsspecifikt og strategisk afsæt for det videre arbejde. Se konkrete eksempler i kapitel 4 samt find et skema til denne øvelse i figur 1 i appendiks.

Med afsæt heri foretager virksomheden en samlet **vurdering af**, hvorvidt virksomheden har et højt eller lavt iboende **risikoniveau**. Et højt iboende risikoniveau er således udtryk for en høj risiko for, at der kan ske tilsigtede og utilsigtede fejl i de finansielle processer (uden hensyntagen til virksomhedens systemmæssige og manuelle interne kontroller). Elementer, der kan indgå i denne vurdering, er eksempelvis:

Faktaboks – Definition af iboende risiko

Den *iboende risiko* er forhold, der er afledt af virksomhedens formål og rammer, og som truer opfyldelsen af virksomhedens mål – *uden* hensyntagen til virksomhedens systemmæssige og manuelle interne kontroller. Det er således den risiko, der eksisterer som følge af aktiviteterne, transaktionernes eller forvaltningsstrukturens art og kompleksitet, og som er så væsentlige, at der kan opstå afvigelser i regnskabsrigtighed.

- Virksomhedens generelle regelgrundlag, kompleksiteten heri samt volatiliteten. Eksempelvis kan et komplekst regelsæt på et tilskudsområde skabe øget risiko for fejl i beregning og anvisning af tilskud.
- Virksomhedens karakter, eksempelvis hvorvidt virksomheden administrerer store finansielle transaktioner, fx tilskud og puljer eller varetager driftsopgaver af ikke-finansiell karakter.
- Karakteren af virksomhedens finansielle processer, herunder hvorvidt der i processerne er involveret mange eller få interne og eksterne interessenter. Processer med mange interne aktører – eksempelvis en tilskudsproces, der involverer et Budgetkontor, Fagkontor, Tilskudskontor, og et Regnskabskontor mv. – kan have et øget risikoniveau, da der kan være risiko for fejl som følge af manglende koordinering og viden om, hvilke opgaver de enkelte aktører udfører.
- Karakteren af de enkelte typer transaktioner, herunder fx om der er tale om eksterne bilag eller internt genererede beregninger mv.
- Systemunderstøttelsen og udstrækningen heraf. Eksempelvis kan en kompleks systemunderstøttelse skabe øget risiko for fejl som følge af mange overgange mellem systemer samt mange brugeradgange og brugerrettigheder.
- Kvantitative forhold som bevillingens størrelse og andre volumenrelaterede parametre.

Andre parametre kan være relevante at inddrage, herunder også virksomhedens historik, kritiske revisionsbemærkninger og lignende.

Denne indledende vurdering er en væsentlig forudsætning for at forstå, hvilke kontroller der er relevante og effektivt vil kunne imødegå de identificerede væsentlige iboende risici.

Etabler overblik over finansielle processer, og prioritér disse

Derefter identificerer og kortlægger virksomheden sine finansielle processer og den monetære værdi, som processerne håndterer.

Af hensyn til det interne kontrolsystems fuldstændighed **kortlægges alle** virksomhedens **finansielle processer**. Processerne kortlægges fra start til slut, således at der opnås overblik fra fastlæggelse af fx et indkøb til selve udbetalingen. Kortlægningen bør også omfatte de processer, der i et vist omfang håndteres i centraladministrative systemer eller i statslige servicecentre, fx løn. Processer vedrørende såvel indtægter som udgifter kortlægges. Kortlægningen udgør et vigtigt grundlag for at vurdere snitflader og funktionsadskillelsen.

Faktaboks – Definition af finansielle processer

En *finansiell proces* dækker over alle transaktioner ift. regnskabet, herunder ud- eller indbetalingsstrømme. Det kan eksempelvis være udbetaling af puljetilskud, udbetaling af løn, køb af varer og tjenester, overførselsindtægter fra kommuner, returkommission mv.

Kortlægningen dokumenteres, så processens forløb fra start til slut synliggøres. Dette kan gøres ved at tegne processen op i fx et procesdiagram. Det inkluderer synliggørelse af de organisatoriske ansvarsskift, som processen indeholder, fx i forbindelse med håndtering af dele af processen i Statens Administration (SAM) eller ved intern overgang fra fx Tilskudsadministration til Regnskab. Det er vigtigt optegningen indeholder **alle transaktionelle skift**, og at risici vurderes for alle disse skift. Se eksempler i kapitel 4 samt find et skema til denne øvelse i figur 2 i appendiks.

Kortlægningen kan med fordel inkludere synliggørelse af, hvilke dele af processen der er understøttet af it-systemer, og hvilke dele der er personbårne. I den forbindelse er det væsentligt at kortlægge, hvordan og af hvem processen kan initieres, da det har særlig betydning for den videre analyse af funktionsadskillelse i processen.

Som led i denne kortlægning foretages en vurdering af, hvilke finansielle iboende risici de enkelte processer er eksponeret for. Vurderingen skal omfatte alle dele af processen. De udvalgte processer kan hver især have forskellige iboende risici.

Eksempelvis kan administration af EU-finansierede tilskud være særligt eksponeret for risikoen for fejl i beregning af tilskud i tilfælde af ændringer i et komplekst regelgrundlag og ved fejludbetalinger. Indkøbsprocessen kan være eksponeret mod risikoen for ugyldige dispositioner, hvis mange kan foretage indkøb.

Ligeledes kan mange interne interessenter øge risikoniveauet, fordi ændringer i opgavevaretagelsen hos én interessent risikerer ikke at medføre nødvendige opgave- og procesjusteringer hos øvrige interessenter. Tilsvarende kan mange eksterne interessenter øge risikoniveauet. Det kan fx være tilfældet ved mindre tilskud til mange eksterne aktører, hvor den ansvarlige styrelse har en relativ lille administration grundet processens lave samlede økonomiske ramme. I sådanne processer kan institutionen være sårbar overfor utilsigtede og tilsigtede (fx svig) fejl i processerne.

Endelig foretages der en **prioritering af, hvilke iboende risici i de finansielle processer, der skal udvælges og vurderes nærmere**. Vurderingen foretages ud fra sandsynligheden for og konsekvensen hvis de iboende risici indtræffer. Hvis processen har en høj iboende risiko, fx som følge af et komplekst lovgrundlag, kan det være relevant at udvælge de finansielle processer til øget kontrol, som i særlig grad er underlagt denne komplekse lovgivning. Tilsvarende kan finansielle processer med en høj økonomisk volumen have en væsentlig iboende risiko som følge af dette. Det er i den forbindelse **væsentligt at vurdere, hvilke risici der kan accepteres, og hvilke der bør sættes ind over for med interne kontroller** for at eliminere eller reducere disse risici.

Der skal udvises forsigtighed med at sætte faste grænser for økonomisk væsentlighed og lade dette afspejle sig i de interne kontroller, da dette i sig selv kan medføre øget risiko for svig.

Det er et ledelsesmæssigt ansvar at beslutte den videre håndtering, herunder rækkefølge, timing og dybde af kontrol-review og efterfølgende initiativer. Andre forhold end finansiel væsentlighed kan have betydning for prioriteringen, herunder eksempelvis den eksponering virksomheden har i offentligheden.

A2 *Review og efterprøvnin g af eksisterende kontroller*

På baggrund af overblikket kan eksisterende kontroller i processerne undersøges nærmere. Dette gøres ved – for hver finansiel proces – at undersøge kontrollerne *designeffektivitet* og *funktionelle effektivitet*.

Vurdering af kontrollernes designeffektivitet

For hver prioriteret finansiel proces foretages der en analyse af, i hvilket omfang der findes interne kontroller, som reducerer risikoeksponeringen til en rimelig størrelse efter virksomhedens forhold. Konkret identificeres interne kontroller i processen, og **kontrollerne vurderes på tilstrækkelighed og relevans** (dvs. kontrollernes såkaldte *designeffektivitet*). Kontrollerne vurderes med afsæt i fx forretningsgangsbeskrivelser, hvor kontrollerne er beskrevet samt evt. samtaler med de medarbejdere der udfører kontrollerne. Såfremt kontrollerne ikke er beskrevet, bør der udarbejdes beskrivelser heraf. Se nærmere eksempler herpå i kapitel 4 samt find en skabelon til denne øvelse i figur 5 i appendiks.

Kontrollernes tilstrækkelighed vurderes ud fra, hvorvidt den enkelte interne kontrol efter dens design og udformning reelt vil kunne reducere den specifikke risikoeksponering. En proces, der håndterer meget store transaktionsmængder, vil eksempelvis næppe kunne reducere risikoeksponeringen gennem en manuel kontrol i form af gennemlæsning af bogføringsjournaler.

Kontrollernes relevans vurderes ud fra, hvorvidt den interne kontrols placering i procesforløbet understøtter dens effektivitet i forhold til den konkrete risiko. Er kontrollen eksempelvis placeret tidligere i processen end der, hvor risikoeksponeringen er størst, har kontrollen begrænset eller ingen effekt.

Faktaboks – Designeffektivitet

Designeffektivitet udtrykker en kontrols tilstrækkelighed (hvorvidt den enkelte interne kontrol efter dens design og udformning reelt vil kunne reducere den specifikke risikoeksponering) og relevans (hvorvidt den interne kontrols placering i procesforløbet understøtter dens effektivitet i forhold til den konkrete risiko).

Den interne controls fokus er vigtigt. Hvis risikoeksponeringen er knyttet til fejlagtige beregninger, skal kontrollen også være rettet specifikt mod beregningernes rigtighed. Er risikoeksponeringen knyttet til svigagtig tilegnelse af midler gennem pengeoverførsler til egne konti, skal kontrollen eksempelvis sikre, at den betalingsanvisende ikke har (systemmæssig) adgang til at ændre i betalingsrelaterede stamdata.

I forlængelse heraf vurderes det, hvorvidt der forefindes flere kontroller rettet mod det samme, idet der i givet fald vil være en effektiviseringsgevinst ved at nedlægge en af de interne kontroller. Dette scenarie er især sandsynligt, når processen gennemløber mange interne og eksterne ansvarsskift, hvor der kan være risiko for, at der udføres dobbelt-kontrol på grund af manglende viden om opgavevaretagelse hos de enkelte aktører. **Eksempelvis** gennemgås med fordel, hvilke kontroller der gennemføres i Statens Administration hhv. i den enkelte administration. Det er vigtigt, at hver enkelt institution har overblik over, hvem der foretager hvilke interne finansielle kontroller og undgår unødvendigt overlap. Det er den enkelte institutions ansvar, at de nødvendige kontroller gennemføres.

Samlet er det således vigtigt, at der foretages en vurdering af både de enkelte kontrollers tilstrækkelighed og deres relevans samt foretages en samlet vurdering på tværs af den enkelte proces. Figur 2 i appendiks kan anvendes til at optegne den enkelte proces for at kunne foretage en samlet vurdering.

Endelig er det væsentligt at vurdere, i hvilket omfang interne kontroller kan forandres fra at være personbårne til at være baseret på funktionalitet i anvendte it-systemer, herunder i de fællesstatslige it-systemer. Hertil er det væsentligt at vurdere, hvorvidt de interne kontroller kan forandres fra at være *opdagende* og *korrigerende* til at være *forebyggende* og placeret tidligt i processerne.

Vurdering af kontrollernes funktionelle effektivitet

Efter vurdering af den designmæssige effektivitet skal den **funktionelle effektivitet efterprøves** af de kontroller, der er fundet tilstrækkelige, relevante og vigtige. Formålet er at skabe vished for, at etablerede interne kontroller faktisk udføres (dvs. afprøve kontrollernes såkaldte funktionelle effektivitet). Efterprøvningen kan ske på forskellig vis, eksempelvis:

- Eftersyn, mens den interne kontrol udføres. Dette er primært en relevant tilgang i forbindelse med personbårne interne kontroller.

Faktaboks – Forebyggende vs. opdagende kontroller

Forebyggende kontroller bidrager til at forhindre fejl, mangler, mv., *inden* de sker. *Opdagende* og *korrigerende* kontroller afslører ved deres udførelse fejl eller mangler, *efter* disse er sket og retter op på fejlene.

Faktaboks - Funktionel effektivitet

Funktionel effektivitet udtrykkes, baseret på efterprøvning af de kontroller, der er fundet tilstrækkelige, relevante og vigtige, hvorvidt etablerede finansielle interne kontroller faktisk udføres og fungerer.

- Gennemgang af dokumentation for kontrollens udførelse i form af fx underskrevne afstemninger og tjeklister, godkendelser og attester mv. samt ved gennemgang af logs mv. over systembårne kontrolaktiviteter. Dokumentationen skal omfatte kontrollens indhold.

Som led i efterprøvningen af kontroller er det vigtigt at undersøge, hvordan mulige tilsigtede eller utilsigtede fejl håndteres. Herunder undersøges det, om der er klarhed over rapporterings- og eskaleringsprocesser og -ansvar i tilfælde af, at der i forbindelse med kontrollerne konstateres fejl.

Som udgangspunkt gælder det, **at en intern kontrol, hvis udførelse ikke kan dokumenteres, ikke findes**. I de tilfælde vil det være nødvendigt at sikre en dokumentation af kontrollerne eller alternativt designe, udvikle og implementere nye, supplerende interne kontroller. Det er centralt at der løbende efterspørges dokumentation for kontrollerne samt gennemføres stikprøvevis eftersyn, se mere herom i nedenstående afsnit B1.

Vurderingen af den funktionelle effektivitet kan samles med designeffektiviteten i det skema, der fremgår af figur 5 i appendiks. Se eksempel herpå i kapitel 4.

Samlet vurdering af det konkrete og ønskede risikoniveau for hver proces

Med afsæt i ovenstående vurderinger af designeffektivitet og den funktionelle effektivitet kan der for hver finansiel proces **foretages en vurdering af det konkrete risikoniveau**. Dette består af en vurdering af, hvordan risikoniveauet aktuelt nedbringes som følge af de interne kontroller, der udføres i processen. Hvis der er identificeret mangler i designeffektivitet eller i den konkrete udførelse, kan dette indebære, at der fortsat er for høj risiko for tilsigtede eller utilsigtede fejl. I så fald kan der være **behov for at implementere tiltag**, som kan bringe risikoen for fejl ned på et ønsket niveau (ledelsens stillingtagen til det *mulige risikoniveau*). På denne måde **opnås der overblik over processens tre risikoniveauer – det iboende risikoniveau, det konkrete risikoniveau og det mulige risikoniveau**.

A3 *Udbedring efter behov*

Hvis der er konstateret mangler under kortlægningen af de interne kontroller, udbedres disse, således at risikoniveauet nedbringes til det ønskede niveau. Manglerne kan fx være:

- utilstrækkeligt omfang af interne kontroller i forhold til den konkrete risikoeksponering,
- forkert design af kontrollerne, dvs. forkert fokus, genstandsfelt eller placering samt manglende beskrivelse af kontrollerne,

- utilstrækkelig funktionel effektivitet, herunder at det ikke kan dokumenteres, at kontrollerne udføres eller den foreliggende dokumentation er mangelfuld/utilstrækkelig.

Udbedringen kan vedrøre design, udvikling og implementering af nye kontroller samt re-implementering af eksisterende kontroller. Det er i den forbindelse vigtigt at sikre, at de interne kontroller for de finansielle processer er beskrevet i virksomhedens forretningsgange, instrukser eller procedurebeskrivelser mv., uanset om processerne er systemunderstøttede eller ej. Beskrivelserne bør indeholde konkrete beskrivelser af, hvilke kontroller der udføres i hver af de finansielle processer, hvilken risiko de imødegår, hvorvidt disse er system- eller personbårne, hvem der har ansvaret for at udføre dem, samt hvilke krav der gælder for dokumentation af kontrollernes udførelse.

B. Levedygtigt og dynamisk kontrolsystem over tid

Dette afsnit beskriver, hvordan virksomheden forankrer og vedligeholder det interne kontrolsystem, således at risikoen for tilsigtede og utilsigtede fejl i finansielle processer fastholdes på det ønskede niveau. Først beskrives det, hvordan der foretages løbende opfølgning på risici og kontroller, og dernæst, hvordan arbejdet med at vedligeholde kontrolsystemet organiseres. Endelig beskrives særlige opmærksomhedspunkter i forhold til systemadgange og brugerrettighedsstyring samt Statens Administrations rolle og ansvar i relation til interne finansielle kontroller.

B1 *Løbende opfølgning på risici og kontroller*

Det er afgørende for at opnå og fastholde et ønsket niveau af kontrol mod tilsigtede og utilsigtede fejl, at der **foretages løbende opfølgning** på, om kontroller i de finansielle processer gennemføres i praksis, og hvorvidt eventuelle udbedringer af mangler heri foretages (jf. afsnit A3).

Supplerende er det vigtigt, at **ændringer i risikoeksponeringen overvåges**, herunder om sådanne ændringer bør føre til ændringer i kontrollerne. Risikoeksponeringen kan således påvirkes af fx ændringer i *ydre* forhold, såsom lovgivning og regler, økonomisk volumen samt digitalisering, eller ændringer i *indre* forhold, såsom organisering, personaleudskiftning mv.

Opfølgning på risikoeksponeringen **samt tilsynet med kontroller** i virksomheden **bør ske med en fast frekvens og rapporteres til den øverste ledelse**.

Rapporteringen kan indeholde et ajourført overblik over de finansielle processer, herunder status for implementering af kontroludbedringer samt overblik over eventuelt ændrede risici, som bør adresseres med nye eller reviderede kontroller. Figur 6 i appendiks kan anvendes hertil, se også et eksempel i kapitel 4.

B2 *Organisering og governance*

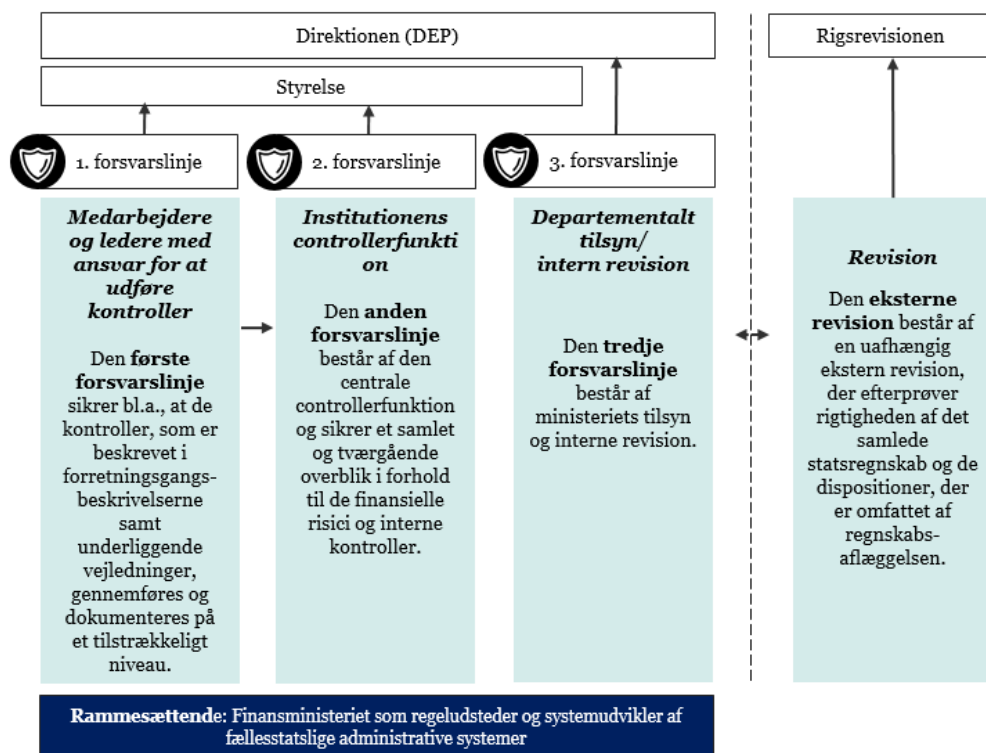
Entydige roller og ansvar er centrale i arbejdet med at udvikle og vedligeholde et kontrolsystem. Det er topledelsens ansvar at roller og ansvar internt i virksomheden er entydigt organiseret. Ledelsen i både den enkelte virksomhed og i det ansvarlige departement skal sikre dette og indgå som en aktiv del af forsvarslinjerne. Roller og ansvar kan følge principperne, der er indeholdt i modellen for de tre forsvarslinjer, som rammesættes af de fastsatte regnskabsregler.

Første forsvarslinje er de medarbejdere og ledere, som har det direkte ansvar for at udføre de kontroller, der skal sikre organisationen mod de faktiske risici.

Anden forsvarslinje er en central controllerfunktion, der har ansvaret for kontrolarbejdet i hele virksomheden samt for at bistå ledelsen med at udføre sit ansvar for organisationens risikostyring.

Tredje forsvarslinje er det departementale tilsyn og eventuel intern revision, som skal sikre en samlet overholdelse af gældende regelsæt for hele ministerområdet eller koncernen.

Endelig er der en ekstern revision, Rigsrevisionen, der sikrer en uafhængig og objektiv vurdering af regnskabets rigtighed. I det følgende udfoldes de interne forsvarslinjer (første forsvarslinje, anden forsvarslinje og tredje forsvarslinje).



Fronten (første forsvarslinje)

Første forsvarslinje rummer medarbejdere og ledere med ansvar for at udføre de kontroller, der er beskrevet i forretningsgange for de enkelte finansielle processer. Det inkluderer at sikre, at de kontroller, som er beskrevet i instrukser og forretningsgangsbeskrivelserne samt underliggende vejledninger, gennemføres og dokumenteres på et tilstrækkeligt niveau. Fx forretningsgangsbeskrivelse for varekøb, herunder hvordan varekøb godkendes af bemyndiget kollega/leder. Supplerende inkluderer det at være opmærksom på de ændringer i risici, der måtte forekomme, samt at være vidende om, hvordan fejl, som kontrollerne af-dækker, håndteres.

Afhængig af omfanget af finansielle processer og kontroller kan denne forsvarslinje være spredt ud på flere forskellige medarbejdere på tværs af organisatoriske enheder i virksomheden.

For at forsvarslinjen kan udføre sit arbejde tilstrækkelig effektivt, skal de medarbejdere, som udfører kontrollerne, have **de rette kompetencer** til at forstå risici, disses sammenhæng til finansielle processer og herigennem relevansen af de implementerede kontroller. I det tilfælde, at kompetencer ikke er tilstede, kan der igangsættes uddannelsesforløb, som sikrer, at medarbejderne uddannes i risiko- og kontrolforståelse og trænes specifikt i at udføre de kontroller, som er beskrevet i forretningsgangene. Til vurdering af medarbejderes nuværende kompetenceniveau kan der anvendes indledende test, der ledsages af periodisk opfølgende træning (e-learning-forløb).

Særlig opmærksomhed kan med fordel rettes mod personaleudskiftning af nøglemedarbejdere, der udfører kontrollerne. Dette er bl.a. for at sikre, at der er planer for, hvilke træningselementer nye medarbejdere skal gennemføre, forud for at man kan påbegynde arbejdet med at udføre interne kontroller.

Faktaboks - Eksempel på opgaver for første forsvarslinje (fronten)

- Udføre og dokumentere de kontroller, som er beskrevet i instrukser, forretningsgangsbeskrivelser samt underliggende vejledninger.
- Forstå og udvise opmærksomhed for de finansielle risici, som virksomheden er eksponeret for.
- Gennemføre træning og årlige test, der sikrer vedligeholdelse af de rette kompetencer.
- Gennemføre løbende risikovurderinger i samspil med den centrale controllerfunktion og de udpegede procesejere.
- Reagere øjeblikkeligt på hændelser, der kan indikere tilsigtede eller utilsigtede fejl.
- Kunne påtage sig rollen som procesejere, såfremt risici og kontroller er begrænset til få organisatoriske enheder.

Den centrale controllerfunktion (anden forsvarslinje)

Finansielle processer gennemløber ofte en række af virksomhedens organisatoriske enheder, og såvel risikoeksponering som kontrolarbejde bliver således ofte

spredt i organisationen. Der kan derfor etableres en **central controllerfunktion**, som **sikrer et samlet og tværgående overblik i forhold til de finansielle risici og interne kontroller**. En central controllerfunktion er ikke nødvendigvis en selvstændig organisatorisk enhed, men den vil ofte bestå af en række centrale medarbejdere i institutionens økonomifunktion, som er adskilt fra første forsvarslinje og med reference til økonomichefen har ansvaret for at løse de påkrævede opgaver.

Den centrale controllerfunktion kan have ansvaret for at sikre, at der for hver finansiel proces er en konkret person, der fungerer som procesejer, kender det samlede flow og de risici, som organisationen er eksponeret for i denne proces, samt de kontroller, der skal udføres/gennemføres. I det omfang at processerne er tværgående og gennemløber flere organisatoriske enheder i virksomheden, kan den centrale risikofunktion med fordel selv påtage sig procesejerskabet.

Den centrale controllerfunktion **skal følge de ændringer** i virksomhedens **risikoeksponering**, der udspiller sig internt og i virksomhedens omverden, og som kan få indflydelse på designet og omfanget af de interne finansielle kontroller. Det indebærer tillige løbende indsamling af viden om robustheden i det eksisterende interne kontrol setup – eksempelvis ved at facilitere, at frontmedarbejderne (første forsvarslinje) i en risikolog kan beskrive opmærksomhedspunkter i forbindelse med udførelsen af kontrollerne.

Controllerfunktionen kan med fordel have en **klar governance-struktur for opfølgning**. Det kan eksempelvis være skriftlig orientering af direktionen med faste mellemrum om ændringer i risikoeksponeringen og de afledte kontrolforanstaltninger, jf. B1.

Afslutningsvis kan controllerfunktionen på vegne af direktionen gennemføre aktivt ledelsestilsyn, der sikrer, at de i forretningsgangene beskrevne kontroller rent faktisk gennemføres. Dette kan med fordel sikres ved at gennemføre en stikprøvekontrol af den dokumentation, der ligger til grund for kontrollerens udførelse. Det er vigtigt, at ledelsestilsynet ikke implementeres som en ”dobbeltkontrol”. Tilsynet har alene til formål at sikre, at de beskrevne procedurer faktisk udføres. Ledelsestilsynet kan med fordel udføres i samarbejde med kontorchefer i de faglige kontorer (første forsvarslinje).

Faktaboks - Eksempel på opgaver for anden forsvarslinje (controllerfunktion)

- Sikre udarbejdelse af roller og ansvar i organisationen i arbejdet med det interne kontrolsystem.
- Udarbejde og følge op på årshjul for opfølgning på risikoelementer og kontroller.
- Etablere processer for løbende rapportering i organisationen.
- Udpege procesejere for de finansielle processer i organisationen.
- Monitorere nye risici og behov for kontroller ved ændringer i organisationens ydre forhold eller indre liv.
- Gennemføre årlige reviews af eksisterende forretningsgange.

Det departementale tilsyn (tredje forsvarslinje)

Det departementale tilsyn og intern revision udgør den tredje forsvarslinje i et stærkt internt kontrolsystem. Heri ligger, at **departementet**, som led i det generelle **tilsyn med virksomhedens opgavevaretagelse**, også skal have et specifikt **fokus på kvaliteten af virksomhedens interne kontrolsystem**. Udgangspunktet er, at virksomhederne selv tilrettelægger og har ejerskab til de risici og kontroller, der specifikt er gældende for den pågældende enhed. Departementets rolle består herefter primært i med passende intervaller at **opsamle de løbende informationer** fra de underliggende virksomheders **risikorapportering**, herunder fx kritiske revisionsbemærkninger, samt **forholde sig aktivt til, om der sker den nødvendige opfølgning**. Departementet har ansvaret for at reagere på svagheder i kontroller, dvs. skal reagere aktivt på alle advarsler om og tegn på svage kontroller og fejl.

B3 *Særligt om systemadgange og brugerrettighedsstyring*

Et væsentligt element i et velfungerende internt kontrolsystem er de understøttende it-systemer, der anvendes i opgaveudførelsen, og som bl.a. medvirker til at sikre systemteknisk funktionsadskillelse i de finansielle processer. God anvendelse af it-systemer, herunder sikring af funktionsadskillelse, forudsætter stringent styring af brugerrettigheder. Det gælder tildeling, ændring og afvikling inden for det enkelte system og på tværs af systemer. Derudover er det centralt at beskytte stamdata, hvilket bør indgå i et kontrolsystem.

Styring af brugerrettigheder kan struktureres i systembårne roller i henhold til de finansielle processer, disses underliggende subprocesser og tilhørende opgaver. **For hver finansielle proces** foretages der **løbende vurdering** af, hvorvidt de her til anvendte systembårne **roller og tilknyttede rettigheder stemmer overens med de opgaver, der varetages som led i processerne**. Dette er med henblik på at sikre, at brugerrollerne med tilhørende rettigheder i it-systemerne ikke giver adgang til at omgå centrale kontroller i processen, herunder især i relation til opretholdelse af fornøden funktionsadskillelse. Supplerende monitoreres det, hvem i virksomheden der har hvilke roller i de enkelte systemer og på tværs af systemer, og det dokumenteres, at tildelte roller understøtter behovet for funktionsadskillelse (herunder at krydskombinationer af roller tildelt samme bruger ikke kompromitterer funktionsadskillelse).

Eksempelvis sikres det, at medarbejdere, som beregner og anviser tilskud til en institution, ikke også med deres brugerrolle har adgang til at foretage selve udbetalingen. Generelt bør brugerrettigheder som udgangspunkt være bestemt af relevans for den enkeltes ansvar for opgaveløsning og tildeles efter mindst muligt privilegium.

Logdata kan anvendes som redskab i et effektivt kontrolsystem. Kontrolsystemet skal således også sikre, at logdata er defineret og beskyttet mod ændringer.

Den centrale controllerfunktion kan være ansvarlig for, at dette overblik etableres og vedligeholdes. Procesejere kan være ansvarlige for at indhente dokumentation for, hvilke it-systemer der anvendes til at gennemføre handlinger i subprocesser. Dette vil typisk ske i tæt samarbejde med it-funktionen, og det er en integreret del af den i afsnit A2 beskrevne kortlægning af processer.

Med en fast kadence og ved større justeringer kan controllerfunktionen med fordel facilitere en gennemgang af brugerrettighedstildelinger, herunder at de er i overensstemmelse med interne forretningsgange i fx regnskabsinstruksen.

Nedenfor er angivet ansvarsdeling for de systemer, som Økonomistyrelsen stiller til rådighed, og som institutioner er forpligtet til at anvende. Ansvarsdeling tager udgangspunkt i systemernes [servicebeskrivelser](#), som findes på Økonomistyrelsens hjemmeside. Institutioner, der anvender andre systemer skal sikre tilsvarende kontroller og beskrive, hvem der gennemfører dem.

System	Ansvar	
	Økonomistyrelsen	Institution
Navision Stat		⋮
SLS		⋮
...		⋮

B4 Særligt om administrative fællesskabers rolle og ansvar i forhold til finansielle interne kontroller

En lang række statslige institutioner anvender administrative fællesskaber (shared servicecenter) til at løse dele af sagsbehandlingen i de finansielle processer. Det kan eksempelvis være institutioners anvendelse af Statens Administration i løn- og regnskabsprocesser eller administrative fællesskaber i selvejesektoren på uddannelsesområdet mv. Fællestrækket for en række af de finansielle processer ved anvendelse af et administrativt fællesskab er, at processerne ofte initieres ved en hændelse i den enkelte institution (en ansættelse, et varekøb, en opkrævning mv.). Herefter pågår der sagsbehandling hos det administrative fællesskab, som afsluttes med et output tilbage i institutionen. Det er derfor **centralt, at det samlede interne kontrolsystem ses i et end-to-end-perspektiv på tværs af institution og administrativt fællesskab.**

Det er hver enkelte institution, der har ansvaret for at sikre tilstrækkelige kontroller i den enkelte finansielle proces. Institutionen kan derfor stille krav om, at de kontroller, som de administrative fællesskaber varetager, er tydeligt og klart beskrevet i en service level agreement (SLA), der regulerer opgavesnitfladen mellem de administrative fællesskaber og institutionen. Endvidere kan det kræves, at de konkrete arbejdsgange, hvormed de administrative fællesskaber foretager kontrollerne, er beskrevet for de relevante procestrin og er dokumenteret på en sådan måde, at de let kan tilgås og forstås af den enkelte institution. Det er eksempelvis tilfældet for Statens Administration, hvor der er detaljerede SLA'er, som institutionen kan tilgå.

Med afsæt i en tydelig og klar beskrivelse af de kontroller, som de administrative fællesskaber udfører, kan virksomheden tilrettelægge de supplerende kontroller, som samlet set sikrer et hensigtsmæssigt internt kontrolsystem. Denne proces kan gennemføres med afsæt i de redskaber og skabeloner, der er beskrevet i kapitel 4.

Faktaboks – Opgaver for administrative fællesskaber og den enkelte virksomhed

Opgaver for administrative fællesskaber

- De administrative fællesskaber beskriver de kontrolaktiviteter, der er rettet mod konkrete risici i specifikke finansielle processer. Kontrollerne dokumenteres i en service level agreement (SLA), der indgår som en del af aftalegrundlaget mellem den enkelte institution og de administrative fællesskaber.
- Den operative udførelse af kontrollerne dokumenteres i et lettilgængeligt skriftligt format, som leverandøren har ansvaret for at vedligeholde, og som til alle tider kan tilgås af den enkelte institution.

Opgaver for den enkelte virksomhed

- Virksomheden vurderer iboende risici for hver finansielle proces, hvor den eksterne leverandør er en del af sagsbehandlingen, jf. afsnit A3. Under iagttagelse af de kontroller, som de administrative fællesskaber udfører for sin del af processen, tilrettelægges de kontroller, som finder sted i virksomheden forud for indberetning til de administrative fællesskaber samt efter modtagelse af uddata.

**Kapitel 4.
Implementering af
interne kontroller
– forslag til redskaber**

4. Implementering – forslag til redskaber

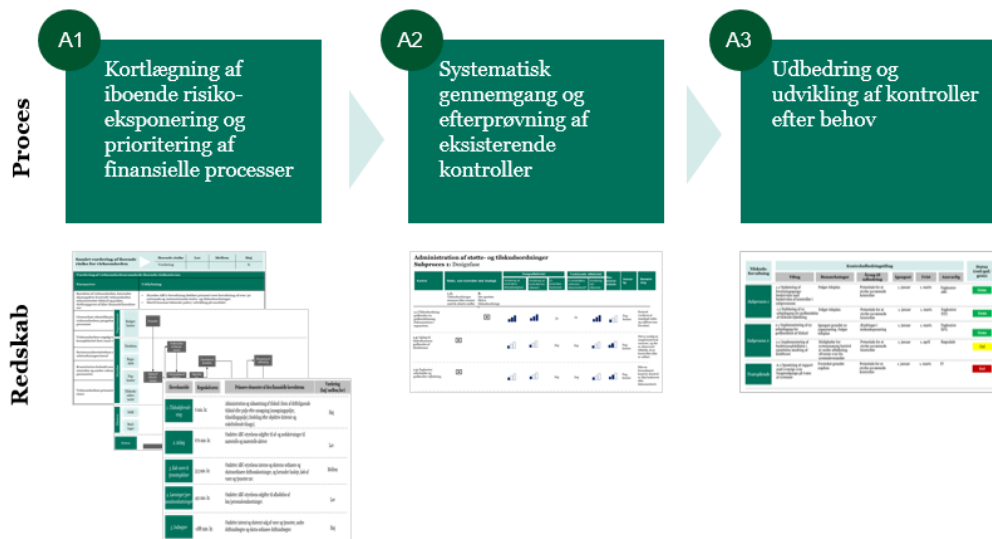
Hvordan opbygges og struktureres det interne kontrolsystem konkret? Dette kapitel gennemgår eksempler på redskaber til etablering af et kontrolsystem som følger fremgangsmåden skitseret i kapitel 3.

4.1 Redskaber til etablering af kontrolsystem

Dette afsnit beskriver de konkrete redskaber, som kan anvendes i arbejdet med tilrettelæggelse af kontrolsystemet, som beskrevet i kapitel 3. Beskrivelsen tager afsæt i konkrete eksempler, der illustrerer, hvordan redskaberne bruges. Alle redskaber er endvidere samlet i et appendiks, hvor de er klar til brug og kan indgå som bilag til instrukser, sådan at det er dokumenteret, hvordan tilrettelæggelse er udmøntet.

A. Redskaber til etablering af kontrolsystem

Der er udviklet en række centrale redskaber i form af skabeloner til hvert af de tre trin i etableringen af et kontrolsystem. Disse gennemgås nedenfor.



A1 *Nuværende risikoeksponering og prioritering af finansielle processer*

Dette trin understøttes af en række redskaber til først at skabe overblik over risikoeksponering og dernæst at etablere overblik over iboende risici i de finansielle processer samt prioritere disse.

Kortlægning af alle iboende risici

Med dette redskab dokumenteres ledelsens indledende og overordnede vurdering af virksomhedens iboende risici og risikoniveau. Redskabet er bygget op om mindst fem parametre. Som minimum bør følgende parametre indgå, når iboende risikoniveau skal fastlægges: 1) regelgrundlag, 2) opgaveportefølje, 3) karakter af finansielle processer, 4) systemunderstøttelse og 5) kvantitative forhold.

I redskabet beskrives for hvert parameter virksomhedens hovedkarakteristika. Dernæst foretages en samlet vurdering – på tværs af de fem parametre – af virksomhedens iboende finansielle risikoniveau. Se et konkret eksempel i figur 1.

I **Eksemplet** i figur 1 ses det, at direktionen samlet vurderer, at styrelsen har en høj eksponering i forhold til iboende finansielle risici. Det baseres bl.a. på stor tilskudsforvaltning med store udbetalinger, et komplekst regelgrundlag, en ældre systemportefølje og flere eksterne aktører.

Direktionens indledende vurdering af iboende risici rammesætter det videre arbejde med tilrettelæggelse af interne finansielle kontroller.

Figur 1. Eksempel på vurdering af iboende risikoniveau

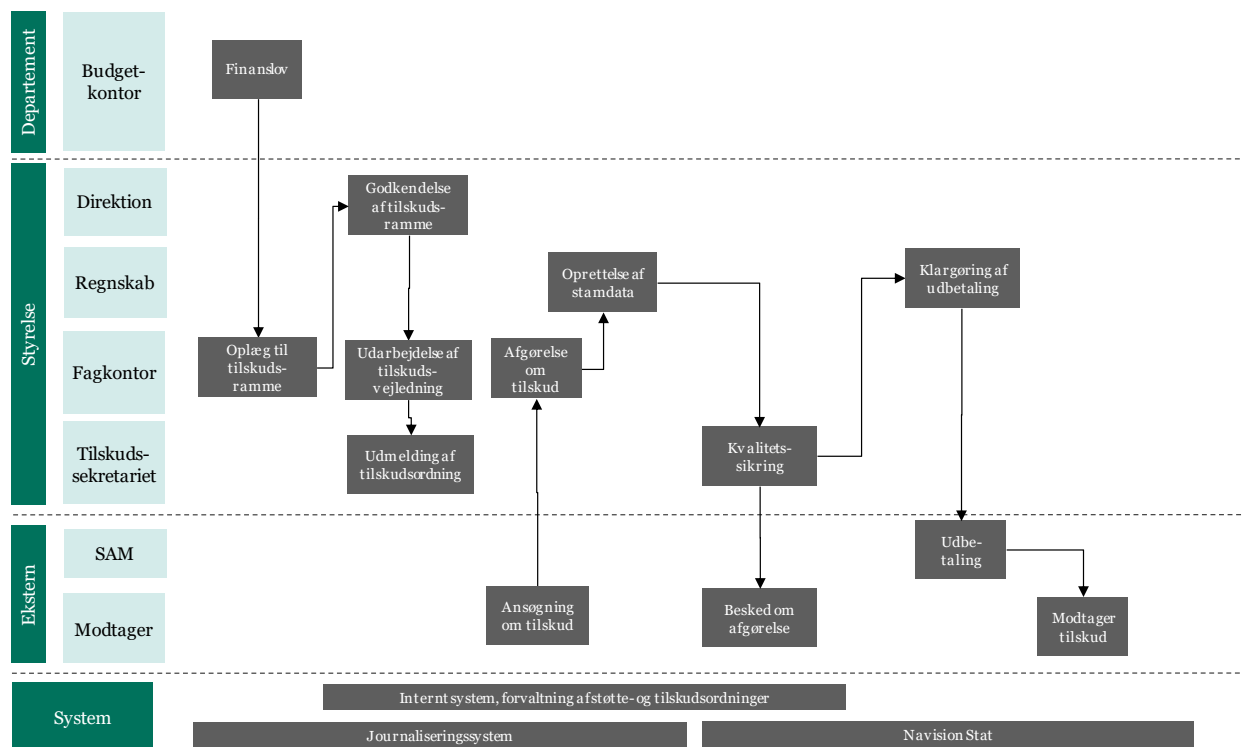
Samlet vurdering af iboende risikoniveau for virksomheden	Iboende risikoniveau	Lavt	Mellem	Højt
				X
Vurdering af virksomhedens samlede iboende risici				
Parameter	Uddybning			
Karakter af virksomheden, herunder eksempelvis hvorvidt virksomheden administrerer tilskud og puljer, driftsopgaver af ikke-finansiell karakter mv.	<ul style="list-style-type: none"> Styrelsens forvaltning dækker primært over 1) forvaltning af nationale og internationale støtte- og tilskudsordninger, 2) drift og forvaltning af område x og y samt 3) løbende policy-udvikling på området. 			
Overordnet identifikation af virksomhedens pengebærende processer	<ul style="list-style-type: none"> Udbetaling af støtte og tilskud (nationale og internationale tilskudsordninger) Udgifter til løn (styrelsen har mange timelønnede) Udgifter til køb af varer- og tjenesteydelser Af- og nedskrivninger til materielle og immaterielle aktiver. 			
Virksomhedens regelgrundlag, kompleksiteten heri samt volatiliteten	<ul style="list-style-type: none"> Styrelsens forvaltning er reguleret af både EU og national lovgivning. Lovgivningen er kompleks og er ofte underlagt ændringer. 			
Systemunderstøttelsen og udstrækningen heraf	<ul style="list-style-type: none"> Styrelsens forvaltning er understøttet af en række ældre og komplekse systemer, som er udviklet internt i styrelsen. Disse systemer forventes at skulle udskiftes i nær fremtid. Styrelsen anvender herudover de fællesstatslige systemer. 			
Kvantitative forhold som bevillingens størrelse og andre volumenrelaterede parametre.	<ul style="list-style-type: none"> Styrelsen har en samlet bevilling på knap 8 mia. kr. Styrelsen har 300 ansatte. Styrelsens forvaltning har en grænseflade til mange eksterne aktører, herunder tilskudsmodtagere. 			
Virksomhedens primære finansielle iboende risici	<ul style="list-style-type: none"> Risiko for fejl i udbetaling af støtte og tilskud grundet mange interne processer på tværs af afdelinger, kompleks systemunderstøttelse og komplekst lovgrundlag Risiko for fejl i administration af løn, herunder særligt grundet manuel administration af timelønnede Risiko for fejl i køb af varer og tjenester grundet høje prokuragrænser. 			

Kortlægning af finansielle processer og prioritér heraf ift. risici

Herefter kan virksomhedens finansielle processer identificeres og kortlægges. Dette kan gøres ved først at gruppere alle transaktioner (ind- og udbetalinger) i de finansielle processer og for hver proces kortlægge aktiviteterne fra start til slut. Se et konkret eksempel herpå i nedenstående figur 2.

Figur 2 viser en proces for udbetaling af støtte og tilskud. **Eksemplet** illustrerer, hvordan flere aktører (departementet, styrelsen, Statens Administration (SAM) og modtagere) indgår i forløbet fra fastlæggelse af ramme på finansloven til udbetaling af tilskud til tilskudsmodtager. Supplerende illustrerer eksemplet, at såvel økonomisystem (Navision Stat) som tilskuds fagligt og journaliseringsystem anvendes i processen. I nedenstående eksempel er processen optegnet på overordnet niveau. Dette kan understøttes af bagvedliggende uddybninger af processtrinene.

Figur 2. Eksempel på kortlægning af finansielle proces fra start til slut



Herefter kan risikoniveau for hver finansiel proces identificeres, hvilket understøttes af nedenstående redskab i figur 3 til at lave en risikokarakteristik for hver enkelt proces. Karakteristikken baseres på et antal kriterier, som hver især vurderes i forhold til iboende risikoniveau.

I **eksemplet** er det den kortlagte tilskudsproces, der er vurderet til at have et højt iboende risikoniveau, idet processen rummer høj volumen, mange transaktioner, høj grad af faglig kompleksitet, høj grad af kompleksitet i understøttende it-miljø og mange eksterne aktører.

Figur 3. Eksempel på skabelon til at identificere iboende risikoniveau for hver finansiel proces

Samlet vurdering af iboende risikoniveau vedrørende administration af tilskuds- og støtteordninger		Iboende risikoniveau	Lavt	Mellem	Højt
		Vurdering			X
Umiddelbar vurdering af processens iboende risici					
Kriterie	Observationer	Vurdering			
Økonomisk volumen	<ul style="list-style-type: none"> Ramme på 6 mia. kr. årligt (2018). 				Høj
Antal modtagere/transaktioner	<ul style="list-style-type: none"> Udmøntning af cirka 20-30 tilskuds- og støtteordninger årligt Omkring 20.000 åbne sager i sagsstyringssystemet. 				Høj
Faglig kompleksitet	<ul style="list-style-type: none"> Der er en række forskellige former for tilskuds- og støtteordninger, som er reguleret af national og internationalt lovgivning. <i>Lovgivningen er kompleks</i> og er ofte underlagt ændringer. Processen går på tværs af <i>fagkontorer, tilskudssekretariat og regnskab</i> med mange medarbejdere involveret. 				Høj
Kompleksitet i understøttende it-miljø	<ul style="list-style-type: none"> Ældre internt udviklet tilskudssystem med manuelle processer og kontroller Der anvendes en <i>række forskellige systemer</i> i processen (internt system, Navision Stat, ansøgningsplatform og journaliseringsystem). 				Høj
Antal interne og eksterne aktører	<ul style="list-style-type: none"> <i>Interne aktører:</i> Processen går på tværs af tilskudssekretariat, fagkontorer og regnskab. <i>Eksterne aktører:</i> SAM, ansøgere/modtagere. 				Høj
Risiko-karakteristik af modtagere	<ul style="list-style-type: none"> Hovedsagelig virksomheder, kommuner samt foreninger, udvalg og organisationer relateret til området. 				Høj

På baggrund af kortlægningen af alle de finansielle processer og deres iboende risiko foretages en prioritering af, hvilke processer der burde underlægges nærmere kontrol-review. Redskabet i figur 4 sammenfatter resultaterne fra kortlægningen struktureret i henhold til hovedområde, økonomisk volumen, finansielle hovedstrøm og iboende risikovurdering. Dette er for, at direktionen kan prioritere, hvilke processer som skal underlægges kontrol-review. I **eksempel** nedenfor udvælges tilskudsforvaltning og indtægter til nærmere analyse.

Figur 4. Eksempel på skabelon til at prioritere processer til kontrol-review

Pengebærende proces	Regnskab 20xx	Primære elementer af den finansielle hovedstrøm	Vurdering af iboende risikoniveau
1. Tilskudsforvaltning	6 mia. kr.	Administration og udmøntning af tilskud i form af driftslignende tilskud eller pulje efter ansøgning (ansøgningspuljer, tilmeldingspulje), fordeling efter objektive kriterier og enkeltstående tilsagn	Høj
2. Anlæg	670 mio. kr.	Omfatter styrelsens udgifter til af- og nedskrivninger til materielle og immaterielle aktiver	Mellem
3. Køb af varer og tjenesteydelser	513 mio. kr.	Omfatter styrelsens interne og eksterne ordinære og ekstraordinære driftsomkostninger, herunder husleje, køb af varer og tjenester mv.	Mellem
4. Lønninger/personaleomkostninger	491 mio. kr.	Omfatter styrelsens udgifter til afholdelse af løn/personaleomkostninger	Lav
5. Indtægter	-188 mio. kr.	Omfatter internt og eksternt salg af varer og tjenester, andre driftsindtægter samt ekstraordinære driftsindtægter	Høj

A2 *Review og efterprøvnin g af eksisterende kontroller*

Dette trin understøttes af et redskab til at analysere, i hvilket omfang der i de prioriterede finansielle processer (fx processer med en "Mellem" eller "Høj" iboende risikoniveau) findes tilstrækkelige interne kontroller til at reducere risikoeksponeringen til en rimelig størrelse. Fremgangsmåden er følgende:

Først opdeles den udvalgte proces i **subprocesser**. For hver subprocess identificeres de primære finansielle risici og kontroller i processen. Disse noteres i redskabet (figur 5 i appendix).

Dernæst vurderes den enkelte kontrols **designeffektivitet**. Dette gøres ved at vurdere, hvorvidt kontrollen er tilstrækkelig til at imødegå risikoen. Samtidig undersøges kontrollernes relevans, herunder om der er risici i subprocessen, som ikke bliver mødt af kontroller. Disse vurderinger noteres ligeledes i redskabet. Herefter kan kontrollernes **funktionelle effektivitet** vurderes. Det undersøges, om der er dokumentation for kontrollernes gennemførelse, og om kontrollerne udføres i henhold til det beskrevne. Sidstnævnte kan foretages ved en stikprøvegennemgang af sager, hvor relevante medarbejdere viser, hvordan kontrollerne er

udført/udføres. Vurderingen af funktionaliteten kan ligeledes noteres i kontrolmatricen.

Eksempel er vist i nedenstående figur 5, som indeholder en vurdering af subprocessen ”designfase” for administration af tilskuds- og støtteordninger. Her ses det, at der er fire kontroller, og at disse vedrører de to identificerede risici i subprocessen. Det er dog vurderet, at to kontroller i lav grad er effektive til at adressere disse risici. Det skyldes udfordringer i kontrollernes tilstrækkelighed og relevans. Tilsvarende er de to kontroller ikke dokumenteret, ligesom stikprøvegennemgangen har vist udfordringer i den konkrete udførelse.

Figur 5. Eksempel på skabelon til vurdering af eksisterende kontrollers designeffektivitet og funktionelle effektivitet

Risiko	Kontrol	Designeffektivitet			Funktional effektivitet		Res- source- indsats	Ansvarlig	Bemær- ning
		Vurdering af kontrollens tilstrækkelighed	Vurdering af kontrollernes relevans	Er kontrollen beskrevet?	Er kontrollens udførelse dokumenteret?	Vurdering ved stikprøve			
1.A: Tilskudsordninger stemmer ikke overens med de afsatte midler. B: Der oprettes fiktive tilskudsordninger.	<input checked="" type="checkbox"/> 1.1 Tilskudsordning godkendes via godkendelsessag. Dokumenteres i sagssystem.			Ja	Ja		Fag-kontor	Kontrol vurderes at imødegå risiko og udføres som forudsat.	
<input checked="" type="checkbox"/>	1.2: Oplæg til tilskudsramme godkendes af direktionen.			Nej	Nej		Fag-kontor	Det er muligt at omgå kontrol af rammer, og der er observeret tilfælde, hvor kontrollen ikke er udført.	
<input checked="" type="checkbox"/>	1.3: Fagkontor udarbejder og godkender vejledning.			Nej	Nej		Fag-kontor	Der er ikke en formaliseret kontrol. Kontrol er ikke beskrevet eller dokumenteret.	

A3 *Udbedring ved behov*

Hvis der er konstateret mangler i de interne kontrollerne, udbedres disse. Disse udbedringer kan noteres i ovenstående kontrolmatrice ved løbende at ændre vurderingerne ud fra kontrollerne, i takt med at udbedringerne foretages. En skabelon til opfølgning på kontroludbedringer fremgår endvidere af nedenstående figur 6.

B. Redskaber til levedygtigt og dynamisk kontrolsystem over tid

Følgende tre redskaber bidrager til at sikre et levedygtigt og dynamisk kontrolsystem over tid samt sikre, at kontrolsystemet forankres i de organisatoriske strukturer og understøtter ledelsen i løbende at kunne tilpasse finansielle kontroller til det aktuelle risikoeksponeringsniveau. Først gennemgås redskaber til løbende

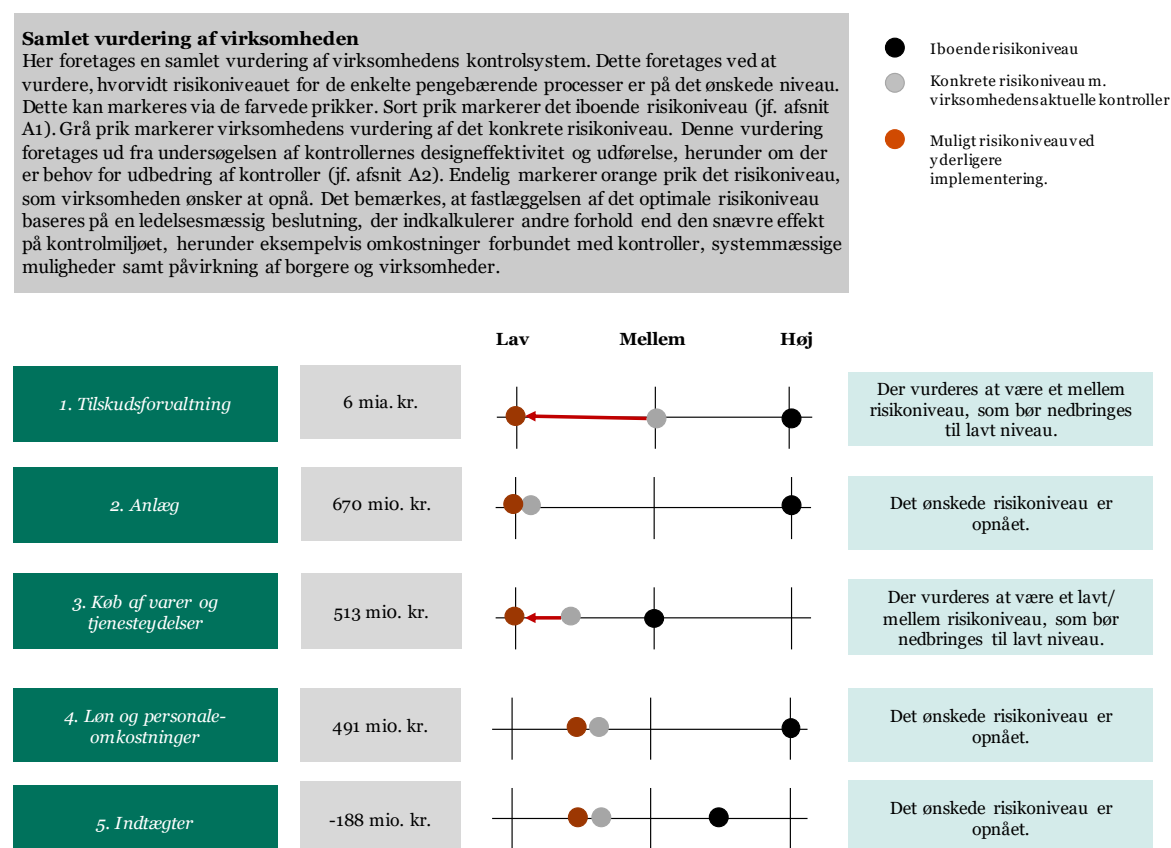
rapportering (figur 6 og 7), dernæst gennemgås redskaber til etablering af governance (figur 8), og endelig beskrives redskaber til at skabe overblik over brugerrettigheder i anvendte systemer (tabel 1-3).

B1 Løbende opfølgning på risici og kontroller

Overblikket over risici og tilsynet med kontroller i institutionen understøttes af et rapporteringsredskab, som kan forelægges institutionens øverste ledelse i henhold til aftalt frekvens. Redskabet består af en forside, der for finansielle hovedprocesser sammenfatter organisationens samlede risikoeksponering set i forhold til ønsket niveau. For hver hovedproces udfoldes eventuelle kontroludbedrings-tiltag med angivelse af årsag til igangsættelse, start- og slutdato samt ansvarlig. Rapporteringen bliver dermed ledelsens værktøj til dels at styre organisationens samlede risikoniveau og dels at sikre eksekvering af tiltag til kontroludbedringer for de enkelte finansielle hovedstrømme.

I **eksemplet** nedenfor er det vist, hvordan ledelsen bibringes overblik i forhold til det nuværende og det mulige risikoniveau for finansielle processer.

Figur 6. Eksempel på skabelon til løbende opfølgning på risici og kontroller



Arbejdet med at nedbringe risikoniveauet for hver finansiel proces kan rapporteres i nedenstående redskab (figur 7). **Eksemplet** neden for viser, at der er udfordringer, for så vidt angår implementering af to kontroludbedringstiltag.

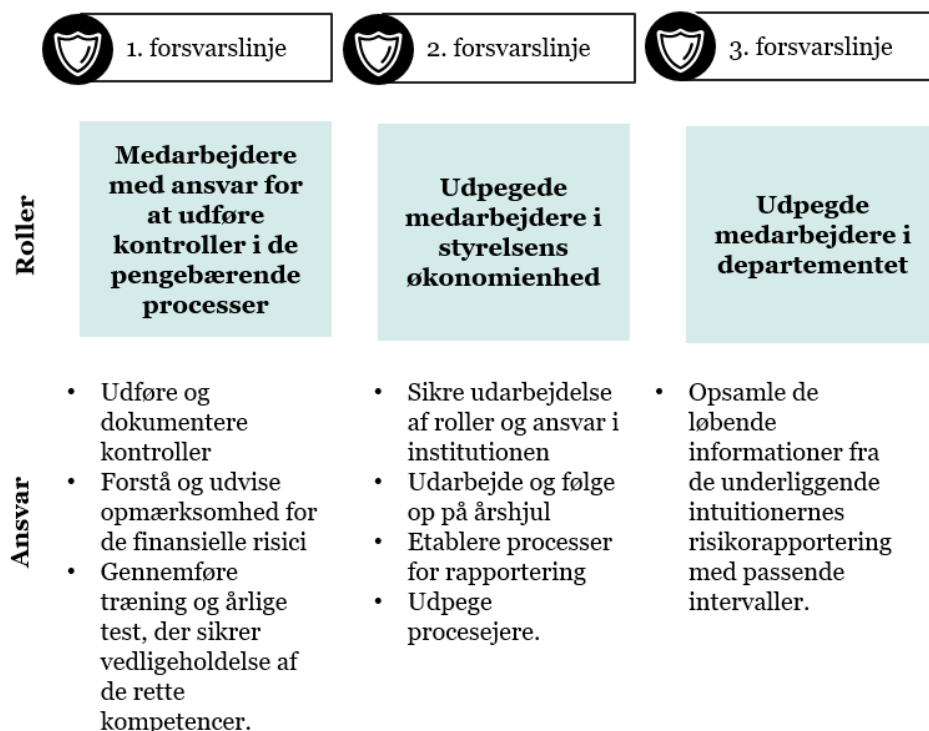
Figur 7. Eksempel på skabelon til opfølgning på kontroludbedringstiltag

Tilskudsforvaltning	Risici	Kontroludbedringstiltag						Status (rød/gul/grøn)
		Tiltag	Bemærkninger	Årsag til udbedring	Igangsat	Frist	Ansvarlig	
Subproces 1	...	1.1 Opdatering af forretningsgangsbeskrivelse m. beskrivelse af kontroller i subprocessen	Følger tidsplan	Potentiale for at styrke nuværende kontroller	1. januar	1. marts	Fagkontor ABC	Grøn
		1.2 Etablering af ny arbejdsgang for godkendelse af tilskudsvejledning	Følger tidsplan	Potentiale for at styrke nuværende kontroller	1. januar	1. marts	Fagkontor XYZ	Grøn
Subproces 2	...	2.1 Implementering af ny arbejdsgang for godkendelse af tilskud	Igangsat grundet ny organisering. Følger tidsplan	Ændringer i risikoeksponering	1. januar	1. marts	Fagkontor EFG	Grøn
		2.2 Implementering af funktionsadskillelse i oprettelse/ændring af kreditorer	Muligheder for systemmæssig kontrol er under afdækning. Afventer svar fra systemleverandør	Potentiale for at styrke nuværende kontroller	1. januar	1. april	Regnskab	Gul
Tværgående	...	A.1 Opsætning af rapport med oversigt over brugeradgange på tværs af systemer	Forsinket grundet sygdom	Potentiale for at styrke nuværende kontroller	1. januar	1. marts	IT	Rød

B2 Klar governance-struktur

Entydige roller og ansvar er centrale i arbejdet med at udvikle og vedligeholde et kontrolsystem. Nedenstående redskab (figur 8) viser et eksempel på roller og ansvar for en styrelse. Første forsvarslinje er placeret hos de medarbejdere, som udfører de faktiske kontroller i processen. Anden forsvarslinje er placeret hos udpegede medarbejdere i styrelsens controllerenhed. Tredje forsvarslinje ligger i styrelsens departement.

Figur 8. Eksempel på skabelon til opfølgning på kontroludbedringstiltag



B3 *Særligt om systemer og anvendelse af understøttende rapporter*

God anvendelse af it-systemer, herunder sikring af funktionsadskillelse, forudsætter stringent styring af brugerrettigheder. Den stringente styring af brugerrettigheder kan foretages ud fra en **procesvinkel** og en **systemvinkel**.

Procesvinklen dækker over, hvorvidt roller i systemerne stemmer overens med de opgaver, som medarbejderne skal foretage i processen – eksempelvis hvorvidt rollen ”rapportering” i et fagsystem matcher den opgave, som personerne med den tildelte rolle skal løse i fagsystemet. Dette er med henblik på at sikre, at rollen i systemet ikke giver adgang til for meget eller for lidt. **I eksemplet** nedenfor (tabel 1) er det vist, hvordan der for hver subprocess er foretaget en sammenligning af centrale opgaver og de roller i systemet, som understøtter opgaverne. Her ses det, at én rolle i fagsystemet er for bred, idet rollen giver medarbejderen adgang til både at oprette og godkende en sag, selvom medarbejderen i processen kun skal kunne oprette sagen.

Tabel 1. Redskab til sammenligning af opgaver og systembårne roller (procesvinkel)

Sub-proces	Centrale opgaver	System	Rolle i system	Er der overensstemmelse mellem opgave og rolle?	Tiltag til at sikre overensstemmelse
Sub-proces 1	Opgave 1.1: Udarbejdelse af godkendelsessag	Sagssystem	Rollen "Sagsoprettelse"	Nej (rollen giver både adgang til at oprette og godkende sag, hvilket omgår en central kontrol i processen)	Ændr rollen, så der ikke er mulighed for at godkende sagerne
Sub-proces 2	Opgave 2.1: Oprettelse og ændring af kreditorer	Økonomi-system	Rollen "Kreditor-oprettelse"	Ja	-
..					

Systemvinklen dækker over, hvorvidt de rigtige medarbejdere har adgang til systemet. Dette foretages for hvert system og på tværs af systemer.

Eksemplet nedenfor illustrerer, hvilke roller de enkelte medarbejdere har i det enkelte system, jf. tabel 2.

Tabel 2. Redskab til oversigt over medarbejderes adgang til ét system (systemvinkel)

Medarbejder	Roller i Sagssystem		
	Læseadgang	Retteadgang	Administrator
Medarbejder 1	x		
Medarbejder 2		x	X
Medarbejder 3		x	x
...			

Eksemplet nedenfor (tabel 3) er det endvidere vist, hvilke systemer medarbejderne samlet set har adgang til. På denne måde sikres en opfølgning på, om nogle medarbejdere har en u hensigtsmæssig adgang til systemer, som fx kan indebære, at de kan gennemføre en udbetalingsproces fra start til slut eller omgå centrale kontroller.

Tabel 3. Redskab til oversigt over medarbejderes adgange på tværs af systemer (systemvinkel)

Medarbejder	Adgang på tværs af systemer		
	Sagssystem	Økonomisystem	System x
Medarbejder 1	x	x	
Medarbejder 2		x	
Medarbejder 3	x	x	x
...			

I dette tilfælde vil det fx være relevant at undersøge, om medarbejder 3 har en uhensigtsmæssig kombination af adgange, idet denne person har adgang til alle tre systemer. Dette undersøges ved, jf. ovenstående tabel 2, at afdække, hvilke konkrete roller medarbejder 3 har i de tre systemer.

oes.dk