ØKONOMISTYRELSEN

Vejledning om kontrol af rettigheder tildelt på tværs af systemer

April 2021

2021

Indhold

Kapitel 1.
Indledning

1. Indledning

En forsvarlig forvaltning af offentlige midler forudsætter, at den enkelte institution har interne kontroller, der er medvirkende til at forhindre økonomisk svindel. Kontroller omhandlende adgangsstyring og rettighedsadministration, på tværs af systemer, er centrale i indsatsen mod svindel.

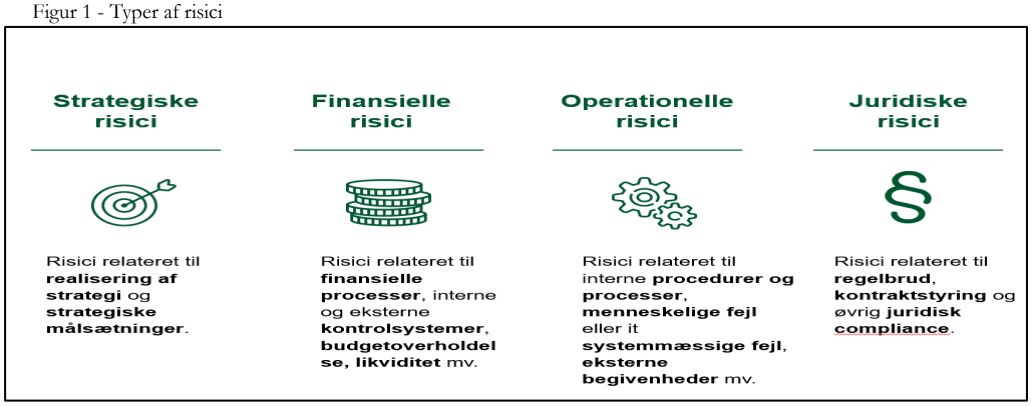
1.1 Baggrund og formål

Den enkelte institution har pligt til at sikre, at der føres kontrol med, hvem der kan tilgå udvalgte data og i hvilket omfang. Dette for at forhindre uautoriseret adgang til, eller ændring af, institutionens digitale information, hvilket funktionaliteten omkring adgangsstyring og rettighedsadministration understøtter.

Med disse systemnære og tværgående kontroller opnår institutionen dokumentation for et passende sikkerhedsniveau, og en beskyttelse af den enkelte bruger, der har et reelt arbejdsbetinget behov.

Denne vejledning beskriver, hvordan institutionen kan opnå et bedre overblik over brugernes tildelte rettigheder, i RejsUd, IndFak, Navision Stat, NemKonto-systemet og Danske Banks onlineløsning District, i forhold til den samlede udbetalingsproces fra disponering til udbetaling. Herved bliver det også muligt at tilpasse de interne kontroller til de finansielle risici. Afledt af dette forventes det, at funktionsadskillelsen i højere grad overholdes for sammenhængende processer, og at der kan sikres afledt højere sikkerhed for korrekte udbetalinger. Fokus for denne vejledning er spændet mellem de finansielle risici og de operationelle risici, se Figur 1.

Figur 1 - Typer af risici



1.2 Afgrænsning

Denne vejledning er skrevet med fokus på den samlede udbetalingsproces fra disponering til udbetaling for systemerne RejsUd, IndFak, Navision Stat, NemKonto-systemet og Danske Banks online løsning District.

Lønudbetalingsområdet og de tilhørende it-systemer; SLS, HR-Løn, Statens HR mv. er ikke omfattet af denne vejledning, og der tages også udgangspunkt i følgende nedenstående afgrænsning:

1.2.1 Lokale fagsystemer

Vejledning omhandler ikke rådgivning om tilsvarende kontrol af lokale fagsystemer.

1.2.2 Tilskudssystem

Det kommende fælles statslige tilskudssystem er ikke inkluderet i denne vejledning, idet systemet på frigivelsestidspunktet for vejledningen endnu ikke er implementeret.

1.2.3 Bagudrettede kontrol

Kontrollerne der anbefales i denne vejledning giver et her og nu øjebliksbilledet, og er *ikke* beregnet til bagudrettet kontrol.

1.2.4 Standardopsætning

Kontrolpunkterne tager udgangspunkt i den til enhver tid gældende standardopsætning af rolle/rettighedsindhold fx den officielle rettighedsfil til Navision Stat. Eventuelle lokale funktionelle tilretninger skal institutionen således selv indarbejde i vejledningen, hvor det er relevant, samt foretage kompenserende kontroller af disse lokale funktionelle tilretninger samt opsætninger.

1.2.5 Fokus på funktionsadskillelse

Vejledningen fokuserer på kontrol af de roller og rettigheder, der giver adgang til udførende part i en funktionsadskilt proces i udbetalings-flowet. Der er således *ikke* omfattet kontrol af adgang til fx stamdata, men udelukkende de kontroller der indgår i udbetalings-flowet, og hvor funktionsadskillelsen ikke er systemmæssigt påtvunget.

1.3 Målgruppe

Denne vejledning henvender sig til følgende målgrupper:

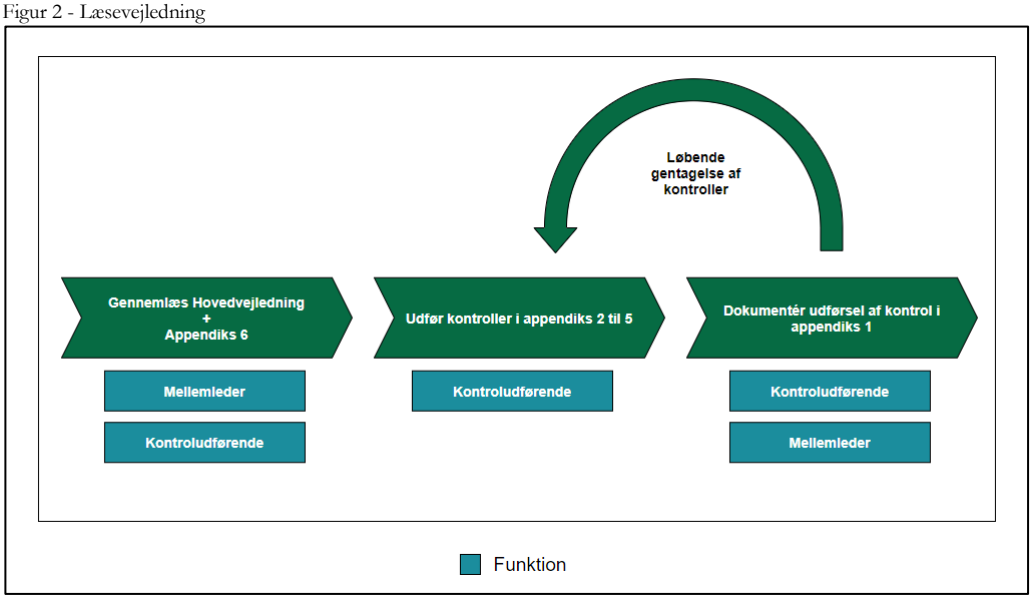
- Topledelsen, der er ansvarlig for at kontrolhierarkiet bliver implementeret, i den enkelte institution
- Mellemlederne, fx økonomiansvarlige, som skal godkende resultatet af de udførte kontroller
- Kontroludførende, fx controllerne, som skal udføre selve kontrollerne

Vejledningen er skrevet med fokus på de statslige og øvrige institutioner.

1.4 Læsevejledning

Materialet består af en hovedvejledning, hvori det beskrives, hvordan den system-understøttet funktionsadskillelse er implementeret i systemerne, der understøtter den samlede udbetalingsproces fra disponering til udbetaling. Yderligere er det identificeret, hvilke privilegerede rettigheder, der findes i de enkelte systemer, som man skal være ekstra opmærksom på, når man tildeler rettigheder til brugere.

Figur 2 - Læsevejledning



I Appendiks 1: **Skabelon til kontrolrapport**, er der udarbejdet en skabelon på en kontrolrapport, som det anbefales at institutionen udfylder, efter hver kontrol, som dokumentation på den udførte kontrol.

Appendiks 1 henvender sig til de kontroludførende samt mellemlederne fx økonomiansvarlige.

I Appendiks 2: **Kontrol af udbetalingsprocessen** beskrives, hvilke kontroller der manuelt skal udføres af institutionen, i forhold til de systemer der indgår i den samlede udbetalingsproces, fra disponering til udbetaling, under hensynstagen til krav om funktionsadskillelse.

Appendiks 2 henvender sig til de kontroludførende.

I Appendiks 3 til 5: **Kontrol af privilegerede rettigheder** (system) beskrives, hvilke kontroller der manuelt skal udføres af institutionen, i forhold til de enkelte systemers privilegerede rettigheder.

Appendiks 3 til 5 henvender sig til de kontroludførende.

I Appendiks 6: **Overblik over kontroller**, findes en detaljeret forklaring til Figur 11, samt en større udgave af figuren.

Appendiks 6 henvender sig til mellemlederne fx økonomiansvarlige og de kontroludførende.

Der vil i denne vejledning og i de tilhørende appendikser være indsat skærmbilleder fra de forskellige systemer. I tilfælde af personoplysninger er data enten blevet anonymiseret, sløret eller opdigtet.

1.5 Koncept for vedligeholdelse af dokumentet

Ved væsentlige ændringer i Økonomistyrelsens egen systemportefølje, eller sammensætning af roller og rettigheder, på de områder, der omfatter udbetalinger, vil denne vejledning blive opdateret. Økonomistyrelsen fralægger sig derfor ethvert ansvar for tidligere og forældede udgaver af denne vejledning.

1.6 Opgavevaretagelse der er ressortoverført til Statens Administration

Statens Administration har ved kongelig resolution overtaget for størstedelen af de statslige institutioner håndteringen af opgaveporteføljen, der omhandler udbetalingshåndteringen. Dette betyder, at Statens Administration, på vegne af institutionerne, kan have adgang til RejsUd, IndFak, Navision Stat, NemKonto-systemet og Danske Banks onlineløsning District.

Ressortoverførslen af løn- og regnskabsopgaverne fra den enkelte institution til Statens Administration indebærer, at det departementale tilsyn med opgavevaretagelsen er overgået til Finansministeriet, hvilket fritager det afgivende ministerium for at udføre tilsynet.

1.7 Ansvar for udførsel af kontrol

Den enkelte institution vil altid have det fulde ansvar for at udføre kontroller i forhold til egne institutionsbrugere, som er oprettet i det enkelte system, og på tværs af systemerne, samt deres adfærd.

I de tilfælde, hvor en anden myndighed varetager hele eller en delmængde af opgaven, på vegne af institutionen, skal myndigheden selv udføre kontrol af sine brugere.

For kunder der serviceres af Statens Administration, er det Statens Administrations ansvar at udføre kontrol på deres del af opgavesplittet. Den enkelte institution

vil ikke modtage dokumentation for Statens Administrations egen kontroludførelse, men kontoret for revision og tilsyn i Finansministeriet fører tilsyn med Statens Administration på dette område.

Statens Administration udarbejder en risikovurdering for deres del af opgavesplittet, men den enkelte institution er altid selv ansvarlig for egen del af opgavesplittet – uanset proces.

Statens Administration kan understøtte institutionerne med deres kontroludførelse, dette kræver dog en separat aftale med Statens Administration.

Denne vejledning fratager ikke institutionernes deres forpligtelse til at foretage egen risikovurdering af deres anvendelse af betalingsafledende systemer, og tilhørende forretningsmæssige processer herunder identificere, hvilke løbende kontroller der samlet set er nødvendige for at leve op til denne forpligtelse, før denne vejledning tages i brug.

1.7.1 Kontroludførelsesinterval

I forhold til kontrollen af, hvilke brugere som har fået tildelt en privilegeret rettighed, så anbefales det at denne foretages mindst én gang i kvartalet. I forhold til kontrol af, hvad den privilegerede rettighed er blevet brugt til, så anbefales, det at denne kontrol udføres hvert halvår. Frekvensen af kontrollerne skal dog altid vurderes op imod den risikovurdering, som den enkelte institutionen løbende skal foretage, hvilket kan betyde en hyppigere frekvens.

1.8 Anvendelse af andre systemer

Institutioner der i henhold til regnskabsbekendtgørelsen § 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, som denne vejledning behandler, i forhold til disse systemer.

1.8.1 Afvigelse fra Brugeradministrationsmodulet (BAM) i Navision Stat

Økonomistyrelsen stille brugeradministrationsværktøjet BAM, til rådighed for brugeradministration i Navision Stat, i det tilfælde, hvor kunden er hostet hos enten Statens It (SIT) eller KMD. Såfremt kunden ikke hostes hos enten SIT eller KMD, skal man benytte den brugeradministrationsfunktionalitet, der leveres med Navision Stat. Uanset valg af driftsmodel[1] og eventuelle lokale tilretninger, er det altid kundens ansvar, at egne brugere er tildelt passende og netop tilstrækkelige brugerrettigheder.

[1] Driftsmodeller:

1.9 Begreber

Vejledningen anvender følgende begreber:

Faktaboks – Væsentlige nøglebegreber 1/2

2-i-forening

- Når en betalingsordre eller en betaling oprettes af en bruger med *2-i-forening* fuldmagt kræves en godkendelse (2. godkendelse) af en bruger med samme fuldmagtstype.

Betalingsafledende system

- Et *betalingsafledende system*, er et system der afleder udbetalinger, enten direkte eller ved understøttelse af en eller flere delprocesser, herunder håndtering af stamdata, der sikre, at der effektueres en udbetaling fra et andet system længere fremme i den samlede udbetalingsproces. Både IndFak og RejsUd er defineret som betalingsafledende system.

Finansiel proces

- En *finansiel proces* dækker over alle transaktioner ift. regnskabet (dvs. alle led i processen), herunder ud- og indbetalingsstrømme. Det kan eksempelvis være udbetaling af puljetilskud, udbetaling af løn, køb af varer- og tjenester, overførselsindtægter fra kommuner mv.

Funktion

- I relation til de viste figurer i kapitlet Systemunderstøttet funktionsadskillelse er definitionen af *funktion*, det at varetage en arbejdsfunktion, fx bogholder, indkøber, rejsende m.v. og er illustreret med den blå farve.

Funktionsadskillelse

- Centralt i et internt finansielt kontrolsystem er princippet om *funktionsadskillelse*, som betyder, at der på tværs af en finansiel proces er interne kontroller, der sikre en personmæssig adskillelse (to eller flere) mellem adgangen til at disponere, godkende, anvise og betale, såvel direkte som indirekte. *(2-i-forening og 4-øjne princip er funktionsadskillelse).*

Privilegerede rettigheder

- *Privilegerende rettigheder* beskrives typisk forskelligt fra system til system, men i nærværende beskrivelse, gælder det at privilegeret adgang er givet ved en adgang, der giver brugeren default læse-, skrive-, redigere- og sletteadgang til samtlige eller særligt kritiske data i systemet samt adgang til at udføre alle eller særligt kritiske funktioner i systemet, samt mulighed for at give sig selv, eller andre privilegerede rettigheder til systemet.

Regnskabsmæssig registrering

- I et udbetalingssystem vil den *regnskabsmæssige registrering* udgøres af det datasæt, der ligger til grund for udbetalingen.

Faktaboks – Væsentlige nøglebegreber 2/2

Rettigheder
- *Rettigheder* giver adgang til specifikke områder i et system, fx udbetalingskladden.

Rettighedssæt
- Et *rettighedssæt* svarer til roller, og er en samling af rettigheder. I figurerne i kapitlet Systemunderstøttet funktionsadskillelse er rettighedssæt illustreret med orange farve.

Rolle
- En *rolle* svarer til et rettighedssæt, og er en samling af rettigheder. I figurerne i kapitlet Systemunderstøttet funktionsadskillelse er en rolle illustreret med den orange farve.

SKB
- Statsinstitutioner er forpligtede til at anvende *Statens Koncern Betalinger* (SKB-systemet), jf. § 11 stk. 2 i regnskabsbekendtgørelsen. SKB er et centralt betalingsformidlingskoncept, der understøttes af et privat pengeinstitut til håndtering af statens ind- og udbetalinger, og systemet kan kommunikere elektronisk med alle statsinstitutioner, uanset hvilket økonomisystem institutionerne anvender.

Udbetalingsdata
- Når betalingen effektueres i udbetalingssystemet, overgår processen til SKB (Statens Koncern Betalinger) som varetager den egentlige finansielle banktransaktion. Informationer om modtager, modtagers betalingsoplysninger, beløb, valuta, betalingsdato m.m. der oversendes til banken benævnes alle *udbetalingsdata*. Udbetalingsdata dannes ofte ud fra den regnskabsmæssige registrering, men ikke nødvendigvis altid sammenfaldende.

Udbetalingsproces
- *Udbetalingsprocessen* skal her forstås som de handlinger der udføres i et udbetalingssystem, i forbindelse med at starte en betalingstransaktion mellem udbetalingsbanken og modtagerbanken.

Udbetalingssystem
- Et *udbetalingssystem* er det system, der har integrationen til banken eller NemKonto, og som effektuerer betalingen. Navision Stat er et udbetalingssystem.

Økonomisystem
- Et *økonomisystem* er et selvstændig system, der både fungerer som kreditorsystem, udbetalingssystem og typisk ligeledes understøtter alle andre klassiske økonomiprocesser. Navision Stat er et økonomisystem.

Kapitel 2. Systemunderstøttet funktionsadskillelse

2. Systemunderstøttet funktionsadskillelse

Et væsentlig element i et velfungerende internt kontrolsystem er de understøttende it-systemer, der anvendes i opgaveudførelsen, og som bl.a. medvirker til at sikre systemunderstøttet funktionsadskillelse i de sammenhængende processer, for at sikre en højere sikkerhed for korrekt udbetaling.

Faktaboks – Definition af funktionsadskillelse jf. regnskabsbekendtgørelsen § 46 og 28

§ 46 Disponering og godkendelse

- **De 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.**
- ***Stk. 2.* Forvaltningen af udgifter og indtægter omfatter disponering og godkendelse af udgifts-/indtægtsbilag. Endvidere omfatter forvaltningen af indtægter regningsudskrivning/opkrævning for så vidt angår skatter og afgifter mv. og debitorforvaltning.**
- ***Stk. 3.* Disponering omfatter indgåelse af aftaler, køb af varer og tjenesteydelser mv., der medfører eller kan medføre udgifter eller indtægter for den regnskabsførende institution. Disponeringen skal godkendes af en hertil bemyndiget person i overensstemmelse med de givne bevillinger og under hensyntagen til Finansministeriets retningslinjer.**

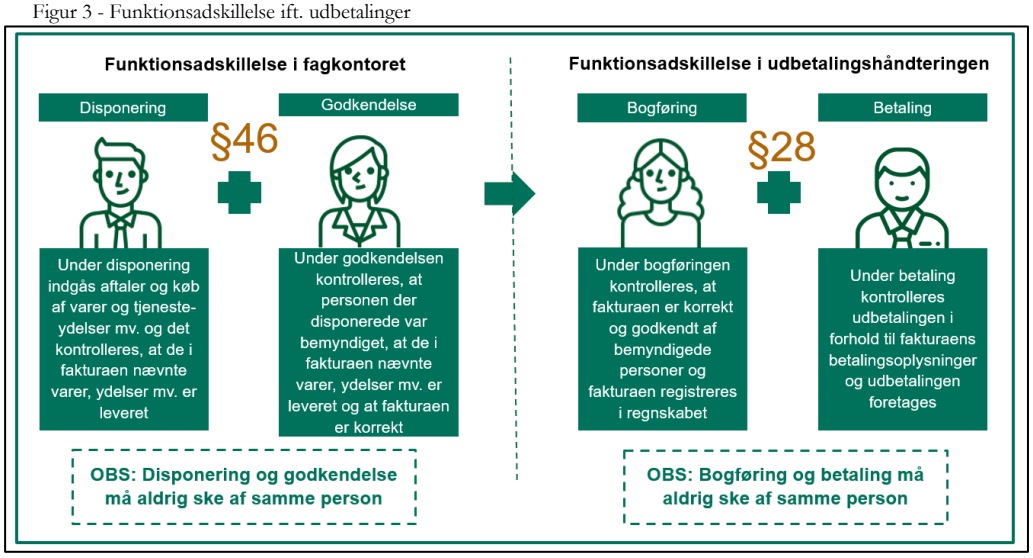
§ 28 Regnskabsmæssig registrering og betaling

- **Udbetalingsforretninger skal tilrettelægges således, at der etableres en personmæssig adskillelse mellem den regnskabsmæssige registrering og betalingen.**

Funktionsadskillelse skal sikre en personmæssig adskillelse (to eller flere) mellem adgangen til at disponere, godkende, anvise og betale, såvel direkte som indirekte, og dermed mindske risikoen for at der, forsætligt eller uforsætligt, foretages udbetalinger i uoverensstemmelse med aftalegrundlaget for betalingen.

Funktionsadskillelsen skal sikre, at det ikke er teknisk muligt for én person i et udbetalingssystem, både at foretage den regnskabsmæssige registrering, og dermed danne datagrundlaget for en udbetaling og efterfølgende sende samme betaling.

Figur 3 - Funktionsadskillelse ift. udbetalinger

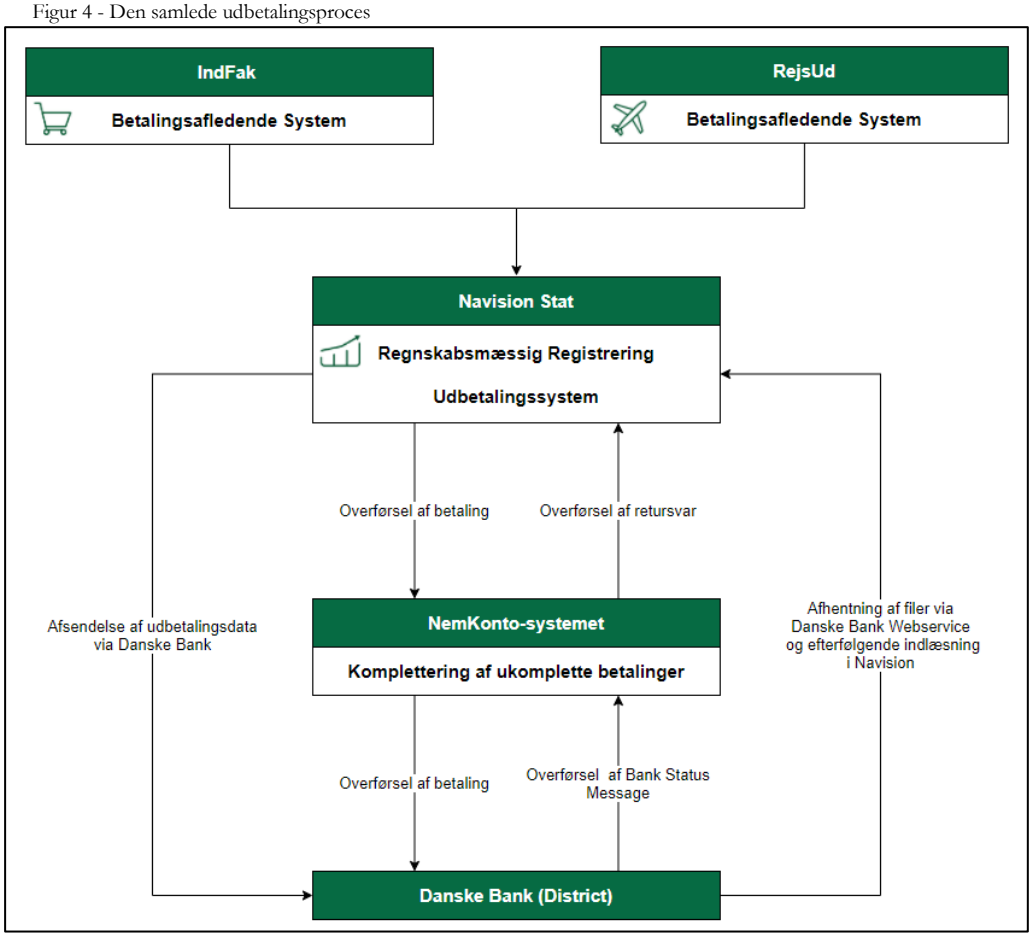


På de efterfølgende sider beskrives, hvordan den systemunderstøttet funktionsadskillelse er implementeret, i systemerne der indgår, i den samlede udbetalingsproces fra disponering til udbetaling, i forhold til konkrete arbejdsopgaver/funktioner.

2.1 Den samlede udbetalingsproces

Den samlede udbetalingsproces ser ud som Figur 4.

Figur 4 - Den samlede udbetalingsproces



Processen starter i et betalingsafledende system, som er et system der afleder udbetalinger, enten direkte eller ved understøttelse af en eller flere delprocesser, herunder håndtering af stamdata, der sikre, at der effektueres en udbetaling fra et andet system længere fremme i den samlede udbetalingsproces. Data sendes herefter videre til et udbetalingssystem, hvor den regnskabsmæssige registrering udgøres af det datasæt, der ligger til grund for udbetalingen. Udbetalingssystemet har integration til NemKonto-systemet og pengeinstituttet, og som effektuerer betalingen.

Der systemunderstøttes tre forskellige udbetalings-flows:

1. Fra Navision Stat via NemKonto-systemet til Danske Banks onlineløsning District
2. Fra Navision Stat uden om NemKonto-systemet til Danske Banks onlineløsning District
3. Direkte i Danske Banks onlineløsning District

Ad 1. Udbetalingsfilen indeholdt både ukomplette og komplette udbetalinger, dannes og godkendes i Navision Stat, hvorefter den sendes via NemKonto-systemet, hvor de ukomplette udbetalinger kompletteres, og videresendes til Danske Banks onlineløsning District.

Ad 2. Udbetalingsfilen dannes og godkendes i Navision Stat, og derefter sendes den direkte til Danske Banks onlineløsning District.

Ad 3. Dannelse og godkendelse af udbetalinger foretages direkte i Danske Bank via onlineløsning District.

2.2 De betalingsafledende systemer RejsUd og IndFak

Overordnet kan man sige, at de betalingsafledende systemer indeholder en disponeringsdel med en efterfølgende godkendelse af den foretaget disponering.

I RejsUd indtastes rejseafregningen/udlægget, kontrolleres samt underskrives, hvis nødvendigt, hvorefter det sendes til godkendelse.

Faktaboks – Disponering og godkendelse

Disponering og godkendelse må aldrig ske af samme person.

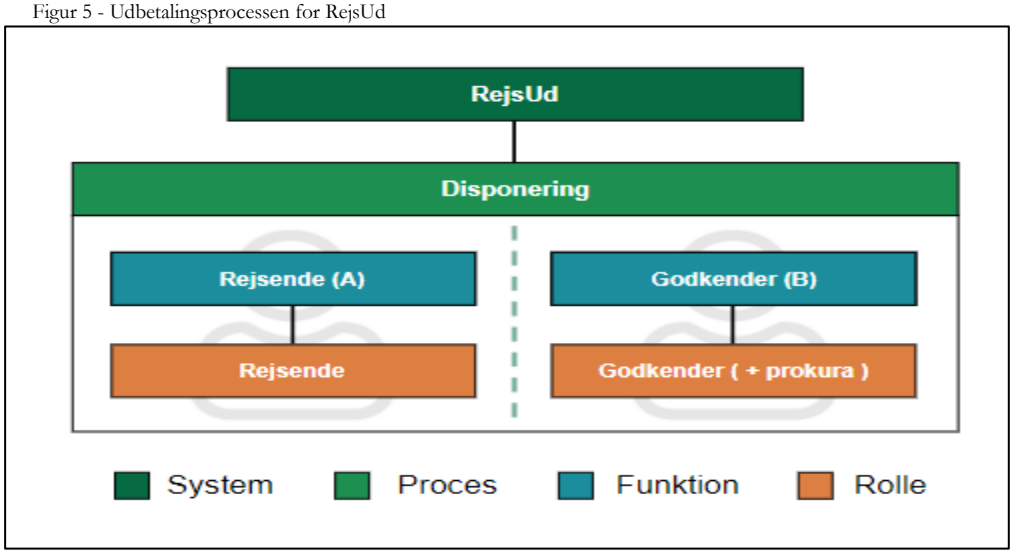
I IndFak indgås aftaler og køb af varer og tjenesteydelser mv. og det kontrolleres, at de i fakturaen nævnte varer, ydelser mv. er leveret. Under godkendelsen kontrolleres, at disponeringen var bemyndiget, at de i fakturaen nævnte varer, ydelser mv. er leveret og at fakturaen er korrekt.

2.2.1 Systemunderstøttet funktionsadskillelse i RejsUd

RejsUd understøtter rejseafregning og udlægshåndtering for rejsekreditorer (medarbejdere med rejse- og udlægsbehov), forud for aflevering til Navision Stat. Rejsekreditorerne modtager efterfølgende betalinger med udgangspunkt i de rejseafregninger og udlæg, der er registreret i RejsUd.

I RejsUd er den systemunderstøttet funktionsadskillelse implementeret ved at der er adskillelse mellem funktionen *Rejsende* (A), der ejer og har oprettet rejseafregning/udlæg og evt. underskrevet og funktionen *Godkender* (B), der har godkendt rejseafregningen/udlægget.

Figur 5 - Udbetalingsprocessen for RejsUd



Af Figur 5 ses det at den *Rejsende* (A) altid skal være forskellig fra den person som skal foretage den endelige godkendelse af en rejseafregning eller udlæg, i dette tilfælde *Godkender* (B).

Figuren viser også, hvilken rolle man skal have i RejsUd for at kunne varetage funktionerne Rejsende og Godkender.

Det er ikke muligt, for den enkelte bruger, at omgå funktionsadskillelsen fra brugergrænsefladen i RejsUd, idet det er kodemæssigt sikret.

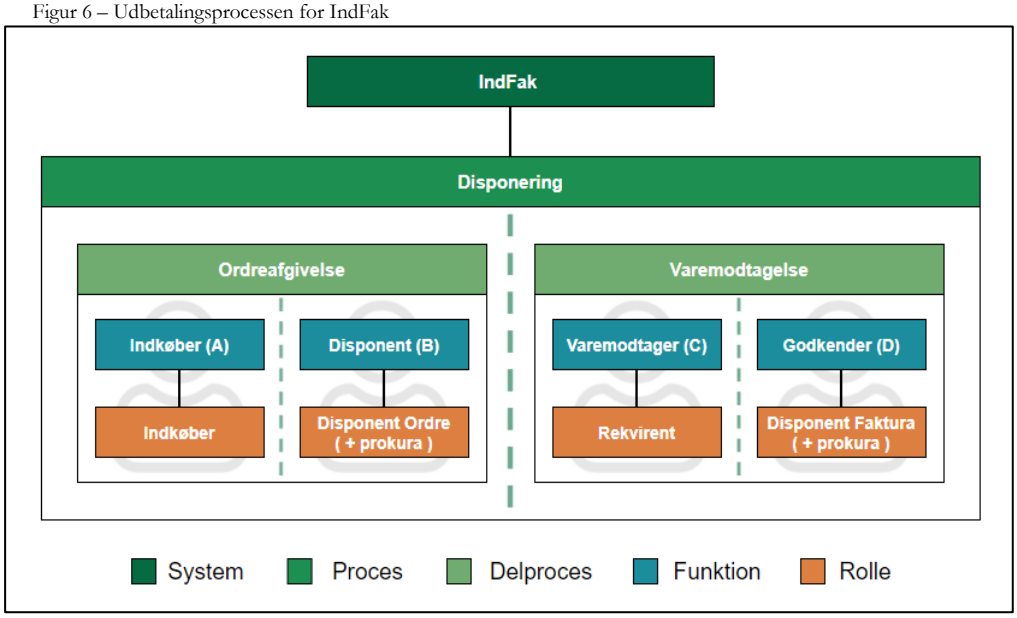
Prokuraopsætning
Der skal i RejsUd være opsat prokura for den bruger, som skal foretage godkendelsen. Er prokura ikke opsat, har man ikke lov til at godkende, selvom man har rollen **Godkender**.

2.2.2 Systemunderstøttet funktionsadskillelse i IndFak

IndFak udgør det fællesstatslige system til understøtter af indkøb og fakturahåndtering, systemet forenkler den samlede proces fra indkøb af vare til selve fakturahåndteringen. IndFak er også defineret som et betalingsafledende system, hvor disponeringen foretages.

I IndFak er den systemunderstøttet funktionsadskillelse implementeret for både ordreafgivelse og for varemodtagelse.

Figur 6 – Udbetalingsprocessen for IndFak



2.2.2.1 Implementering af funktionsadskillelse i Ordreafgivelse

I Figur 6 ses at i ordreafgivelsesdelen i IndFak er der adskillelse mellem den bruger, der har funktionen *Indkøber*, og som har oprettet ordren (A) og den bruger, som har funktionen *Disponent* , og som har godkendt disponeringen (B), hvis den efterfølgende varemodtagelse alene sker ved én person i tilfælde af opsat autogodkendelse[2].

For at håndtere funktionen *Indkøber*, skal man have rollen **Indkøber** og for at håndtere funktionen *Disponent* skal man have rollen **Disponent Ordre**.

Den bruger som opretter ordren (A) må gerne være lig den bruger der godkender disponeringen (B), hvis der *ikke* er opsat autogodkendelse.

Det er ikke muligt, for en almindelig bruger, fra brugergrænsefladen at omgå adskillelsen, idet der er implementeret 4 øjneprincip. Dog er det muligt for rollen Global systemadministrator at ændre til 2 øjneprincippet[3], hvorefter funktionen autogodkendelse ikke er muligt, og det medfører at faktura skal varemodtages og disponeres i fakturamodulet. Uanset om det er 2-øjne eller 4-øjne, vil der altid være tvungen systemunderstøttet funktionsadskillelse.

Faktaboks - Global systemadministrator

Det er kun Økonomistyrelsen og leverandøren af IndFak/RejsUd som kan få tildelt rollen Global systemadministrator, derfor skal den enkelte institution ikke foretage separat kontrol af denne rolle.

[2] Autogodkendelse: Hvis regler er opfyldt i Matchmodulet sendes faktura, direkte gennem fakturamodulet til "Klar til overførsel"/Navision Stat med informationer og kontering fra ordren. Og der er adskillelse mellem indkøber og disponent på en ordre, altså 4 øjne. Se også opsætning af matchregler.

[3] 2 øjneprincippet: 2 øjne - Samme bruger kan være indkøber og disponent på en ordre.

2.2.2.2 Implementering af funktionsadskillelse i Varemodtagelse
I varemodtagelsesdelen i IndFak er der adskillelse mellem den bruger der har funktionen *Varemodtager* (C), og har rollen **Rekvirent**, og har konteret og kontrolleret fakturaen, og den bruger, som har funktionen Godkender, og skal godkende disponeringen (D), og har rollen **Disponent faktura**.

Figur 6 viser at (C) altid skal være forskellige fra (D), dette gælder dog ikke i det tilfælde, hvor der er opsat autogodkendelse, idet her vil (C) alene kunne foretage den samlede godkendelse.

Faktaboks – Implementering af 4 øjne

Systemet vil altid kræve at der bliver valgt en anden disponent, hvis der er sammenfald. Dette er sikret kodemæssigt, og det er ikke muligt for en bruger at omgå dette fra brugergrænsefladen.

Prokuraopsætning
I IndFak skal der også være opsat prokura på brugerne med rollerne **Disponent Ordre** og **Disponent Faktura**, ellers er det ikke muligt at disponere i ordreafgivelsesdelen og endeligt godkende i varemodtagelsesdelen af IndFak.

2.3 Udbetalingssystemet Navision Stat
Funktionsadskillelsen i udbetalingssystemet er opdelt i 'Bogføring' og 'Betaling'. Under bogføringen kontrolleres, at fakturaen er korrekt[4] og godkendt af bemyndigede personer og fakturaen registreres i regnskabet.

Under betaling kontrolleres udbetalingen i forhold til fakturaens betalingsoplysninger og udbetalingen foretages.

Faktaboks – Bogføring og betaling

Bogføring og betaling må *aldrig* ske af samme person.

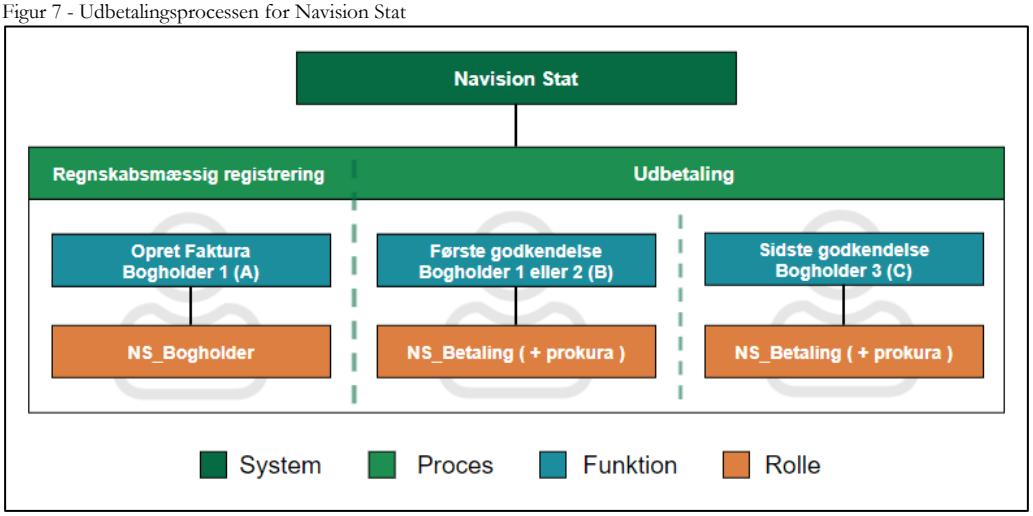
2.3.1 Systemunderstøttet funktionsadskillelse i Navision Stat
Navision Stat understøtter de handlinger der skal udføres i et udbetalingssystem, hvor udbetalingsprocessen typisk vil består af bogføring (regnskabsmæssige registrering) af udbetalingsdata, udsøgning af poster til udbetaling, trin af godkendelser af udbetalingen, afsendelse af udbetalingsdata, standsning af udbetalingsdata og lignende.

I Navision Stat er der implementeret systemunderstøttet funktionsadskillelse mellem den bogholder (A), der har bogført fakturaen og den bruger, der har foretaget

[4] Kontrollen af fakturaens korrekthed udføres ved kunden selv, hvis der anvendes et økonomiservicecenter som fx Statens Administration.

den endelige godkendelse, af den tilsvarende udbetaling (C). Funktionsadskillelsen er uafhængig af brugerens rolle, og vil derfor altid være gældende.

Figur 7 - Udbetalingsprocessen for Navision Stat



Yderligere er der adskillelse mellem den bruger, der foretager den endelige godkendelse af udbetalingen som *anden/sidste godkender* (C) og den bruger, der har udsøgt fakturaen til betalingen, som *første godkender* (B), da afsendelsen sker direkte fra Navision Stat til NemKonto-systemet eller Danske Bank.

Af ovenstående Figur 7 ses det at, den bruger der *bogfører kladden/fakturaen* (A) skal være forskellige fra, den bruger der foretager *anden/sidste godkendelsen* (C), at den bruger der foretager den *første godkendelse* (B) skal være forskellige fra, den bruger der foretager *anden/sidste godkendelsen* (C). Den bruger der *bogfører kladden/fakturaen* (A), og den bruger der foretager den *første godkendelse* (B), gerne må være sammenfaldende.

Adskillelsen er sikret kodemæssigt, således at kontrollen ikke beror på opsætninger, såsom rettigheder eller gruppemedlemskaber. Det er således ikke muligt at omgå adskillelsen fra brugergrænsefladen.

Prokuraopsætning
I Navision Stat skal man angive, hvilke specifikke brugere, der må indgå i, hvilke dele af godkendelsesprocessen af udbetalinger, hvilket sker i prokuraopsætningen. Her indmeldes brugerne i prokuragrupper, som tildeles godkendelsesgrænser i procentsatser, beløbsgrænser samt filtre for, hvilken konteringsdimensioner der må godkendes betalinger for.

Den implementerede funktionsadskillelse sikrer, at uanset prokuraopsætningen, så kan samme bruger aldrig endeligt godkende betalinger, vedkommende selv har første godkendt, eller endelig godkender selv har bogført.

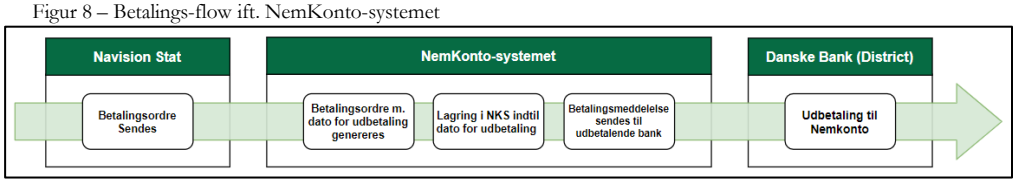
2.4 Funktionsadskillelse i NemKonto-systemet

NemKonto indgår ikke som en del af Økonomistyrelsens systemportefølje, men alle udbetalingssystemer skal understøtte en integration til NemKonto[5], som fælles offentlige udbetalingssystem. NemKonto-systemet udgør et ekstra kompletterende led i betalings-flowet fra myndigheden til pengeinstituttet.

Funktionsadskillelse jf. tidligere definition, er ikke understøttet i NemKonto-systemet, men heller ikke nødvendig, idet betalinger ikke kan rettes i NemKonto-systemet. NemKonto-systemet er en database, der kobler modtagerens CPR-nummer eller virksomhedens CVR, SE eller P-nummer med den bankkonto, som er valgt, som NemKonto[6]. Dette betyder at NemKonto-systemet komplettere ukomplette betalinger med egentlige kontooplysninger.

Da betalinger ikke kan rettes i NemKonto-systemet, er der ikke risiko for, at en sagsbehandler i en institution eller i Statens Administration kan foretage eller ændre udbetalinger. Dette gælder også for en ændring af modtagerkonto, da sådan en ændring ikke vil aktiveres med det samme, men være afhængig af et fysisk aktiveringsbrev der sendes til den adresse der er registreret på en myndigheds CVR-nummer eller på modtagerens CPR-nummer. Herefter der skal ske en aktivering udført af modtageren, virksomheden eller myndigheden selv, før aktiveringen eller ændringen træder i kraft, og aktiveringsbrevet beskriver den pågældende ændring.

Figur 8 – Betalings-flow ift. NemKonto-systemet



Når en betalingsordre sendes fra Navision Stat til NemKonto-systemet er der ikke tale om en decideret betaling indeholdende penge, men en ordre om, at der skal udbetales et givent beløb til en given NemKonto. I Figur 8 ses det, at betalingsordren indeholder en dato for udbetalingen, og bliver gemt i NemKonto-systemet, indtil at det bliver tid til at sende betalingen til udbetaling i banken.
Som tidligere beskrevet varetager Statens Administration opgavehåndteringen i NemKonto-systemet, på vegne af de statslige institutioner.

2.4.1 Statens Administration og NemKonto-systemet

I forbindelse med at Statens Administration håndterer opgaveporteføljen i forhold til udbetalingsprocessen, så har driften i Statens Administration, nærmere betegnet kreditormedarbejderne, adgang til NemKonto. Der er fra de enkelte institutioner givet fuldmagt til Statens Administration, for varetagelse af denne opgave. Driften

[5] Jf. Bekendtgørelsen om NemKonto-ordningen.
[6] Generelt om NemKonto-systemet.

i Statens Administration har kun adgang til at standse enkelte, eller bundter af, betalinger.

Statens Administration udarbejder en risikovurdering for deres del af opgavesplittet, men den enkelte institution er altid selv ansvarlig for egen del af opgavesplittet – uanset proces.

2.4.2 Sagsbehandlere i de enkelte institutioner

Ligesom det ikke er muligt for driften i Statens Administrations at manipulere ved selve betalingsmeddelelserne i NemKonto-systemet, er det heller ikke muligt for de enkelte sagsbehandlere i de enkelte institutioner. Det er kun muligt at stoppe enkeltbetalinger eller bundter af betalinger. Der er derfor ikke behov for funktionsadskillelse.

2.5 Funktionsadskillelse i Danske Banks onlineløsning District

I den samlede udbetalingsproces er der integration fra Navision Stat og NemKonto-systemet til pengeinstituttet, der varetager driften af statens koncern betalinger (SKB), i dette tilfælde Danske Bank.

2.5.1 District

Danske Banks onlineløsning District[7], er bankens internetbaserede officebanking-system, der giver adgang til at se kontoinformationer og til at oprette og godkende betalinger, dvs. uden integration med Navision Stat som afsender af en betalingsordre.

Brugerne kan være ansat hos institutionen (kontohaveren), men behøver ikke at være det. Administrative fællesskaber, som for eksempel Statens Administration, betjener (andre) institutioner (kontohavere) og vil have behov for at oprette brugere, som er ansat i det administrative fællesskab, og brugere, som er ansat hos de institutioner (kontohavere), de betjener.

En bruger skal have fuldmagt fra institutionen for at kunne foretage transaktioner i District på vegne af institutionen eller tredjemand.

2.5.2 Staten benytter 2-i-forening

For statsinstitutioner gælder kravet om personmæssig adskillelse, jf. bekendtgørelse om statens regnskabsvæsen m.v. Herefter skal der som absolut udgangspunkt være to involveret i bogførings- og betalingsprocessen.

---

[7] Om SKB/OBS i Danske Bank.

Staten benytter begrebet *2-i-forening*, når en betalingsordre eller en betaling oprettes af en bruger. Hermed kræves en godkendelse (2. godkendelse) af en bruger med sammen fuldmagtstype.

Godkendelse af to personer i forening er en effektiv måde at undgå svindel og øger sikkerheden i District. Det gør det vanskeligere for hackere at foretage betalinger i institutionens navn.

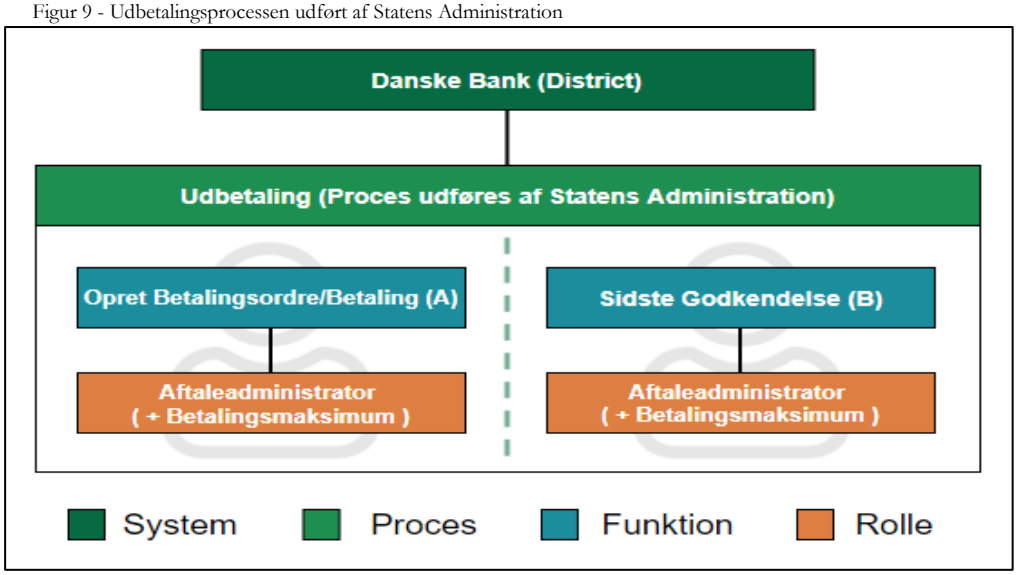
2.5.3 Prokuraopsætning

SKB understøtter automatiserede prokurakontrol, kontrol af ægtheden af brugerens identitet, samt en kontrol at om brugerne 2-i-forening er berettigede til at gennemføre en overførsel (kontrollen understøtter den personmæssige adskillelse hos institutionen (kontohaver)).

2.5.4 Statens Administration

I det tilfælde hvor Statens Administration har overtaget opgaven at oprette en betalingsordre eller betaling på vegne af en institution, via en tredjemandsfuldmagt til District, er der funktionsadskillelse via '2-i-forening [A-fuldmagt[8]]', hvilket følger af kravene i regnskabsbekendtgørelsens regler om funktionsadskillelse. Af Figur 9 ses det at den bruger der opretter en betalingsordre/betaling (A) altid skal være forskellige fra den bruger, der foretager sidste godkendelsen (B).

Figur 9 - Udbetalingsprocessen udført af Statens Administration



[8] Når en ordre eller betaling oprettes af en bruger med A-fuldmagt, er den automatisk godkendt af denne (1. godkendelse). Ordren eller betalingen kræver endnu en godkendelse (2. godkendelse) af en bruger med enten Alene-, A-, B- eller C-fuldmagt. Brugere med A-fuldmagt er sideordnede, og godkendelsesrækkefølgen er derfor underordnet.

2.5.5 Små institutioner

Enkelte meget små institutioner, både statslige og øvrige, kan have vanskeligt ved at overholde en funktionsadskillelse, fordi de ganske enkelte er for få ansatte. De skal så, hvis de bruger Alene-fuldmagt[9], have kompenserende kontroller[10] og beskrive både baggrunden for bemyndigelserne og kontrollerne i regnskabsinstruksen[11]. Ved anvendelse af Alene-fuldmagt skal institutionen altid overveje tidsbestemt tildeling af rettigheder – så de tildelte rettigheder understøtter konkrete og aktuelle behov i opgavevaretagelsen, og endvidere medvirker til at minimere risikoen for fejl og misbrug.

2.5.6 Direkte betaling

Der kan være enkelte institutioner, hvor det er nødvendigt at have mulighed for at oprette betalinger direkte i banken, til trods for at Statens Administration håndtere størstedelen af deres udbetalinger, og der er indgået en tredjemandsfuldmagt. Det kan være *sammedagsbetalinger*, som gennemføres senere samme dag eller en *straksbetaling*, som gennemføres øjeblikkeligt.

Institutioner der opretter betalinger direkte i banken, skal selv foretage kontrol i District, i forhold til disse betalinger, idet Statens Administration kun udfører kontrol i forhold til deres del af opgavesplittet.

---

[9] Alene fuldmagt: Når en ordre eller betaling oprettes eller ændres af en bruger med denne fuldmagt, betragtes den automatisk som godkendt af brugeren. Det kræver ikke 2- godkendelse. Brugere med denne fuldmagt kan også godkende ordre eller betalinger, der er lagt ind af brugere med alle andre fuldmagtstyper.

[10] En sådan kompenserende kontrol kan evt. drøftes i regi af eget departement, der evt. vil kunne bistå med opgaven. Som kunde hos Statens Administration kan der indgås en aftale omkring udmøntning af kompenserede kontroller eller alternativt sparring herom.

[11] Se mere på retinformation.dk og vejledning om finansiel intern kontrol på oes.dk

Kapitel 3. Privilegerede rettigheder

3. Privilegerede rettigheder

Privilegerede rettigheder beskrives typisk forskelligt fra system til system, hvilket også er tilfældet for de systemer, som understøtter den samlede proces fra disponering til udbetaling.

Ved tildeling af privilegerede rettigheder, til den enkelte bruger, følger en forpligtelse som institutionen skal være opmærksom på, idet der ved denne type rettighed er en forøget mulighed for at begå svig og misbrug i systemet.

Faktaboks – Definition af Privilegerede rettigheder

I nærværende beskrivelse gælder det at privilegerede *rettigheder* er givet ved en adgang, der giver brugeren default læse-, skrive-, redigere- og sletteadgang til samtlige eller særligt kritiske data i systemet samt adgang til at udføre alle eller særligt kritiske funktioner i systemet, samt mulighed for at give sig selv, eller andre, privilegerede rettigheder til systemet.

3.1 Tildeling af privilegerede rettigheder

Muligheden for at begå svig og misbrug i de enkelte systemer forøges, når en bruger tildeles en såkaldt privilegerede rettighed. Det betyder, at man skal være yderst varsom med tildelingen af denne type rettighed.

Når man som institution får tildelt, eller ønsker at få tildelt, privilegerede rettigheder, så *skal* man være opmærksom på følgende:

1. Tildeling og anvendelse af privilegerede adgangsrettigheder bør begrænses og styres[12]
2. Den enkelte bruger skal have et godkendt arbejdsbetinget behov jf. institutionens opgaveportefølje, for at få tildelt rettigheden
3. Der skal foretages kontroller, som kan afsløre evt. misbrug i forhold til rettigheden baseret på logdata
4. Brugere med privilegerende rettigheder må ikke, som ene person kunne gennemføre en udbetaling
5. Brugere med privilegerende rettigheder må ikke alene definere de kontroller, som de selv skal kontrolleres ud fra

[12] ISO 27002, afsnit 9.2.3 Styring af privilegerede adgangsrettigheder

3.1.1 Privilegerede rettigheder i IndFak og RejsUd

I IndFak og RejsUd systemet er brugere med privilegerende rettigheder defineret som brugere med de nedenstående oplistede roller.

Tabel 1 - Privilegerede rettigheder i IndFak og RejsUd

Privilegerede rettigheder		
Rolle	**System**	**Beskrivelse**
Global system-administrator	IndFak/RejsUd	Brugere med denne rolle kan oprette nye brugere, slette eller de-aktivere eksisterende brugere samt tildele roller til alle brugere i systemet.
Lokal system-administrator + **Disponent** (kombineret med en opsat prokura)	IndFak	Brugere med denne rolle kan oprette nye brugere, slette eller de-aktivere eksisterende brugere samt tildele roller, til sig selv og til andre brugere der er oprettet på samme koncernniveau eller underliggende. Disponenter kan med tilstrækkelig prokura godkende bilag, der i forvejen er varemodtaget af anden person[13].
Lokal system-administrator + **Godkender** (kombineret med en opsat prokura)	RejsUd	Brugere med denne rolle kan oprette nye brugere, slette eller de-aktivere eksisterende brugere samt tildele roller, til sig selv og til andre brugere der er oprettet på samme koncernniveau eller underliggende. Godkender kan med tilstrækkelig prokura godkende bilag, der i forvejen er kontrolleret og underskrevet af en anden person.

Faktaboks - Global systemadministrator

Det er kun Økonomistyrelsen og leverandøren af IndFak/RejsUd som kan få tildelt rollen Global systemadministrator, derfor skal den enkelte institution ikke foretage separat kontrol af denne rolle.

3.1.1.1 Kontroller i forhold til privilegerede rettigheder for IndFak/RejsUd

Selve tildelingen af rollen **Lokal systemadministrator** til en bruger er i sig selv ikke alvorlig, idet en lokal systemadministrator ikke kan danne transaktioner i IndFak eller RejsUd, uden yderligere roller og prokura. Man *skal* dog kontrollere for, at der ikke har fundet en egen tildeling af ekstra roller og prokura sted.

[13] I de mindre institutioner bestående af et mindre antal medarbejdere kan én bruger med både Rekvirent og Disponent rollerne varemodtage og godkende samme bilag i en og samme handling. Det kræver, at organisation er opsat med "2-øjne profil", hvilket skal være velbegrundet og kan kun opsættes af Miracle på anmodning fra institutionen via Supporten.

Se Appendiks 3: Kontrol af privilegerede rettigheder i IndFak og RejsUd for udførsel af de manuelle kontroller, listet herunder:

1. Er der oprettet brugere med privilegerede rettigheder, der ikke har et godkendt **arbejdsbetinget behov**?

Der skal dannes et øjebliksbillede af, hvorvidt brugere med privilegerede rettigheder har et godkendt arbejds- og/eller funktionsbetinget behov, for netop disse rettigheder for både IndFak og RejsUd.

2. Er der sket en **tildeling af prokura til en bruger der har rollen Lokal systemadministrator**, der ikke kan begrundes?

En bruger med rollen **Lokal systemadministrator** kan ikke danne transaktioner i IndFak og RejsUd, uden yderligere roller og prokura, og har som udgangspunkt heller ikke brug for dette. Men en bruger med rollen **Lokal systemadministrator** kan godt tildele roller og prokura til en anden bruger med rollen **Lokal systemadministrator**. Det er derfor kritisk at undersøge, om dette er sket, eller om en bruger med tildelt prokura skifter rolle til **Lokal systemadministrator** uden tilstrækkelig dokumentation herfor.

3. Har en bruger med rollen **Lokal systemadministrator tildelt prokura til en anden bruger**, der ikke kan begrundes?

En bruger med lokal systemadministratoradgang kan tildele roller og prokura til en vilkårlig anden bruger, uden der findes et arbejdsbetinget behov herfor. Det er derfor kritisk at undersøge om der er sket en tildeling med tiltrækkelig dokumentation for et arbejdsbetinget behov.

4. Har en bruger med rollen **Lokal systemadministrator oprettet andre brugere med rollen Lokal systemadministrator**, der ikke kan begrundes?

En bruger med rollen **Lokal systemadministrator** kan oprette en anden bruger med rollen **Lokal systemadministrator**, eller tildele en eksisterende bruger rollen **Lokal systemadministrator**. Det bør derfor undersøges, om der er tilstrækkelig dokumentation herfor.

5. Har en bruger med rollen **Lokal systemadministrator foretaget en ændring af e-mail eller password på en anden bruger**, der ikke kan begrundes?

En bruger med rollen **Lokal systemadministrator** har adgang til at rette notifikations e-mail og nulstille password for andre brugere, hvorved det bliver muligt at logge på som en anden bruger, angive nyt password, og sørge for, at brugernes normale e-mail notifikationer fremsendes til anden bruger end den brugerkonto,

der logges på med. Derved bliver det muligt at overtage prokura fra en given bruger på løsningen, uden at brugeren opdager det.

Som dokumentation på at den enkelte manuelle kontrol er udført, anbefales det at institutionen udfylder en tilhørende kontrolrapport. Se Appendiks 1: Skabelon til kontrolrapport, for eksempel på, hvordan denne kontrolrapport kan se ud.

3.1.2 Privilegerede rettigheder i Navision Stat

I Navision Stat findes der to privilegerede rettighedssæt, som vises i nedenstående tabel. Med rettighedssættet SUPER, er det muligt for en bruger at udføre næsten samtlige handlinger i Navision Stat.

Tabel 2 - Privilegerede rettigheder i Navision Stat

Privilegerede rettigheder		
Rettighedssæt	**System**	**Beskrivelse**
SUPER	Navision Stat	Rettighedssættet giver rettigheder til alle data og alle funktioner i Navision Stat, kun begrænset af restriktioner i forretningslogik og licens. Dette er et særligt rettighedssæt som ikke kan ændres eller slettes. Det kræver SUPER for at kunne oprette brugere.
SUPER(DATA)	Navision Stat	Rettighedssættet giver rettigheder til at læse, indsætte, redigere samt slette i alle data i Navision Stat, uden at give adgang til afvikle funktionalitet.

Faktaboks - Statslige institutioner serviceret af Statens Administration

De privilegerede rettigheder i Navision Stat er forbeholdt driftsleverandørerne, da de benyttes til udvikling og support af Navision Stat.

Dette betyder, at man lokalt i institutionen og i Statens Administration ikke må få tildelt disse to rettighedssæt.

Faktaboks - Øvrige institutioner

De privilegerende rettigheder i Navision Stat er forbeholdt driftsleverandørerne, da de benyttes til udvikling og support af Navision Stat.

Dog er det tilladt for øvrige institutioner at få tildelt rettighedssættet, men de kan ikke tildele det selv, hvis de er hostet hos KMD eller SIT, og benytter brugeradministrationsmodulet BAM.

Hvad enten en institution hoster selv, benytter BAM eller ej, så har institutionen mulighed for at få oprettet privilegerede rettigheder. Derfor har institutionen altid selv ansvaret for at udføre kontrol af de privilegerede rettigheder.

3.1.2.1 Kontroller i forhold til privilegerede rettigheder i Navision Stat
I forhold til de privilegerede rettigheder i Navision Stat, *skal* der foretages nedenstående kontroller.

Se Appendiks 4: Kontrol af privilegerede rettigheder i Navision Stat, for hvordan de manuelle kontroller, listet herunder, skal udføres.

1. Er der oprettet brugere med privilegerede rettigheder, der ikke har et godkendt **arbejdsbetinget behov**?

Det skal undersøges om der findes privilegerede brugere, som ikke længere har et arbejdsbetinget behov, og om disse har foretaget handlinger med rettighedssættet.

2. Er der sket en **tildeling af prokura til en bruger med privilegerede rettigheder**, der ikke kan begrundes?

En bruger med privilegerede rettighed kan tildele roller og prokura til en anden bruger med privilegeret rettighed. Derfor er det kritisk at undersøge, om dette er sket, uden tilstrækkelig dokumentation herfor.

3. Har en **bruger med privilegerede rettigheder tildelt prokura til en anden bruger**, der ikke kan begrundes?

En bruger med privilegerede rettigheder i Navision Stat kan tildele roller og prokura til en vilkårlig anden bruger, uden der findes et arbejdsbetinget behov herfor. Det er derfor kritisk at undersøge, om der er sket en tildeling med tilstrækkelig dokumentation for et arbejdsbetinget behov.

4. Har en **bruger med privilegerede rettigheder oprettet andre brugere med privilegerede rettigheder**, der ikke kan begrundes?

En bruger med privilegerede rettighedsadgang kan oprette andre brugere med superadgang. Det bør derfor undersøges, om der er tilstrækkelig dokumentation herfor.

Som dokumentation på at den enkelte manuelle kontrol er udført, anbefales det at institutionen udfylder en tilhørende kontrolrapport. Se Appendiks 1: Skabelon til kontrolrapport, for eksempel på, hvordan denne kontrolrapport kan se ud.

3.1.3 Privilegerede rettigheder i NemKonto-systemet
Ud fra definitionen af privilegerede rettigheder, så indeholder NemKonto-systemet ikke privilegerede rettigheder.

Institutionen skal være opmærksom på, at de rolleprofiler der tildeles, altid skal tildeles restriktivt sådan, at disse kun tildeles medarbejdere, hvor behovet er helt nødvendigt[14].

3.1.4 Privilegerede rettigheder i Danske Banks onlineløsning District

Brugere med privilegerede rettigheder er, for Danske Banks onlineløsning District, defineret som brugere med nedenstående rolle samt specifik tildelt brugerrettighed.

Tabel 3 - Privilegerede rettighed i Danske Banks onlineløsning District

Privilegerede rettigheder		
Rolle	**System**	**Beskrivelse**
Aftaleadministrator **+ (Rolle kombineret med brugerrettigheden Alene-fuldmagt)**	District	Aftaleadministratorer er dem, der administrerer District-aftalen på den enkelte institution, og skal herunder oprette brugeradministratorer, tildele brugeradgange til Districts forskellige funktioner og tildele brugerrettigheder [fx fuldmagter]. Alene-fuldmagt: oprette, ændre ordre eller betalinger, og de betragtes automatisk som godkendt af brugeren, og kræver ikke 2. godkendelse.

3.1.4.1 Kontroller i forhold til privilegerede rettigheder i Danske Banks onlineløsning District

I forhold til de privilegerede rettigheder i Danske Bank onlineløsning District, anbefales det at der foretages nedenstående kontrol.

Se Appendiks 5: Kontrol af privilegerede rettigheder Danske Banks onlineløsning District for udførsel af de kontroller, der listes herunder.

1. Er der oprettet brugere med privilegerede rettigheder, der ikke har et **godkendt arbejdsbetinget behov**?

Det skal undersøges om der findes privilegerede brugere, som ikke har et arbejdsbetinget behov.

2. Er der privilegerede **brugere som har fået tilknyttet en Alene-fuldmagt**?

Det skal undersøges, om der findes privilegerede brugere i Danske Banks onlineløsning District, som har fået tilknyttet en såkaldt Alene-fuldmagt. Har en brugere

[14] Se side 29 i NemKonto håndbogen afsnittet Hvilken rolleprofil anbefales myndigheden at tildele sagsbehandlere.

en Alene-fuldmagt, så kan vedkommende oprette eller ændre ordre eller betalinger, og de betragtes automatisk som godkendt af brugeren, og det kræver ikke 2. godkendelse. Yderligere så kan brugere med denne fuldmagt også godkende ordre eller betalinger, der er lagt ind af brugere med andre fuldmagtstyper[15].

Som dokumentation på at den enkelte manuelle kontrol er udført, anbefales det at institutionen udfylder en tilhørende kontrolrapport. Se Appendiks 1: Skabelon til kontrolrapport, for eksempel på, hvordan denne kontrolrapport kan se ud.

[15] Se også betingelser for Danske Banks onlineløsning District.

Kapitel 4.
Best Practice for op-sætning af brugere

4. Best Practice for opsætning af brugere

Det er vigtigt, at de medarbejdere, der skal have adgang til ét eller flere af de systemet, som understøtter den samlede udbetalingsproces, opsættes ud fra en 'Best Practice', således at man, allerede ved oprettelsen af brugere, forebygge muligheden for svig.

4.1 Anbefaling for opsætning af brugere

For at forebygge muligheden for misbrug og svig i de enkelte systemer, angives her de retningslinjer, som Økonomistyrelsen anbefaler, at de enkelte institutioner benytter sig af, når processen for opsætning af brugere i de enkelte systemer pågår.

4.1.1 Samme identifikation pr. system

Det anbefales, at enhver fysisk bruger, som udgangspunkt, oprettes med samme identifikation pr. system.

Er ovenstående ikke muligt, skal der findes en nøgle, der binder kontoadgangen samme ved kontrol, det vil ofte kunne lade sig gøre via en arbejdsmail. Derudover er det vigtigt at ajourføre stamdata om brugerne i de enkelte systemer, som beskrevet under 4.1.7.

4.1.2 Én adgangsgivende konto pr. system

Det anbefales, at enhver fysisk bruger kun må have én adgangsgivende konto pr. system. Det er især vigtigt at sikre dette, ved ændring af personers e-mail, eller for eksempel tildeling af ny AD[16] konto. Man skal således være opmærksom på at lukke gamle adgange, når der oprettes nye adgange.

4.1.3 Tildeling af roller/rettigheder som svarer til arbejdsfunktionen

Når en bruger skal have adgang til ét eller flere systemer, er det vigtigt at der inden tildeling af roller/rettigheder, er klarlagt, hvilket arbejdsbetinget[17] behov brugeren har.

[16] AD: Active Directory

[17] Arbejdsbetinget: Vurdering af hvorvidt de 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.

Faktaboks - Rettigheder

Rettigheder bør som udgangspunkt være bestemt af relevans for den enkeltes ansvar for opgaveløsning og tildeles efter mindst muligt privilegium.

Økonomistyrelsen har tidligere publiceret et redskab til understøttelse af dette. Se Tabel 1. Redskab til sammenligning af opgaver og systembårne roller (procesvinkel) i Appendiks til Vejledning om intern finansiel kontrol[18].

4.1.4 Tildeling af opsætningsroller

Det anbefales at brugere som får tildelt opsætningsroller/rettigheder i de enkelte systemer ikke får tildelt roller/rettigheder, som giver dem mulighed for at kunne gennemføre transaktioner, med direkte økonomisk konsekvenser, i samme system.

4.1.5 Sikre funktionsadskillelse

For at sikre funktionsadskillelse, må brugere ikke opsættes på en sådan måde, at de for én og samme proces kan optræde som den ene halvdel af en funktionsadskilt proces, og dernæst som den anden halvdel af samme proces. Dette gælder for alle systemer, lige meget, om der er systemunderstøttet funktionsadskillelse eller ej.

4.1.6 Tildeling af rettigheder til brugere der skal udføre opgaver i forbindelse med udbetalingsprocessen

Brugere der skal varetage funktioner i forbindelse med udbetalingsprocessen som fx bogføre kladde eller kontering af fakturaer, i de enkelte systemer, bør ikke få tildelt privilegerede rettigheder, idet de ikke har et arbejdsbetinget behov for at få tildelt disse rettigheder. Vær særlig opmærksom på, at det jf. bekendtgørelsen om statens regnskabsvæsen mv. § 21 stk. 2, ikke er tilladt at varetage opgaver relateret til driftsafvikling samtidig med regnskabsmæssige funktioner.

4.1.7 Ajourføre oplysninger i systemet ved stamdata ændring

Det anbefales, at når der foretages en ændring i en brugers stamdata, for eksempel ved navneskifte, så ajourføres alle de systemer, hvori brugeren har adgang med det samme.

---

[18] Læs mere om vejledning om intern finansiel kontrol

Kapitel 5.
Kontroller der skal foretages på tværs af systemer

5. Kontroller der skal foretages på tværs af systemer

Der findes ingen systemmæssig kontrol af rettighedstildeling på tværs af systemadgangen for den samme bruger. Det betyder at institutionen selv har en forpligtelse til, at skaffe/danne sig et overblik, over de medarbejdere, der har adgang på tværs af systemer. Regnskabsinstruksen skal klart beskrive institutionens proces for overvågning af adgange på tværs af systemerne.

Yderligere skal det dokumenteres, at de tildelte roller understøtter funktionsadskillelse, herunder at krydskombinationer af roller tildelt samme brugere ikke kompromitterer funktionsadskillelse.

Den enkelte medarbejder kan isoleret set have en passende adgang i ét system, men kombinationen af denne adgang, og adgangen til et eller flere andre systemer kan gøre, at den enkelte medarbejder potentielt kan have en for samlet bred adgang.

Har en medarbejder en for bred adgang, er der en potentiel mulighed for at medarbejderen kan begå svig og misbrug på tværs af systemerne.

Figur 10 neden for viser at der findes kombinationer af adgange, der er tilladte, og kombinationer der *ikke* er tilladte.

For tilladte adgange gælder det, at der i det enkelte system er en systemmæssigt funktionsadskilt understøttelse, som sikrer, at den bruger, som foretager disponeringen, altid vil være forskellige fra den bruger, som foretager den endelige godkendelse. Eller at den bruger, som foretager den regnskabsmæssige registrering, altså bogføringen, altid vil være forskellige fra den bruger, som foretager den endelige godkendelse af betalingen.

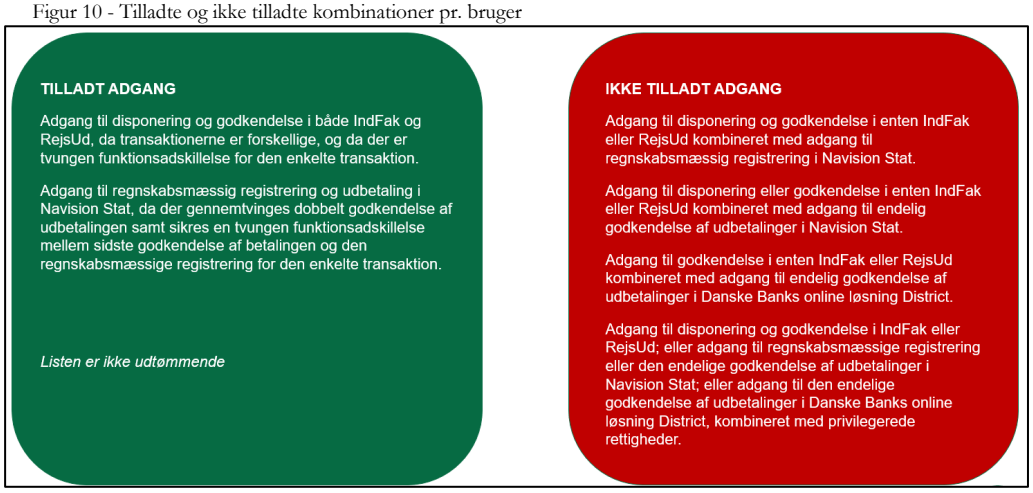
For ikke tilladte adgange gælder det generelt, at der på tværs af systemer, *ikke* findes en systemunderstøttet funktionsadskillelse.

Derfor skal man, som institution, sikre via kontroller, at den samme bruger *ikke* enten foretager en disponering eller godkendelse i et af de betalingsafledende systemer, OG efterfølgende bogfører eller foretager den endelige godkendelse i udbetalingssystemet, idet den samme bruger, i sidste ende i så fald godkender sin egen handling, og derved omgår funktionsadskillelsen.

I de tilfælde, hvor udbetalingen godkendes i Danske Banks online løsning District, skal der foretages kontrol med, at det ikke er den samme bruger, som godkender i banken, som også har foretaget godkendelsen i et af de betalingsafledende systemer, idet den samme bruger, også i dette tilfælde, godkender sin egen handling, og omgår funktionsadskillelsen.

Det er heller ikke tilladt at, den bruger som skal foretage godkendelse, hvad enten det er i de betalingsafledende systemer eller i Navision Stat, har privilegeret adgang. Med en privilegeret adgang, har man mulighed for at tildele sig selv yderligere roller og rettigheder, som for eksempel prokura, og har dermed mulighed for at begå svig og misbrug. En bruger der varetager regnskabsmæssige funktioner må *ikke* tildeles privilegeret adgang, hverken internt i et system, eller på tværs af systemer, jf. § 21, stk. 2 i Bekendtgørelsen om statens regnskabsvæsen mv.

Figur 10 - Tilladte og ikke tilladte kombinationer pr. bruger



5.1 Omfang af kontrollerne

Kontrollerne, der nævnes i denne vejledning, kan benyttes både som forebyggende kontroller, for at forhindre muligheden for at begå svig og misbrug, men også som opdagende kontroller, idet de vil kunne afsløre et potentielt uhensigtsmæssig brugeropsætning på tværs af systemerne.

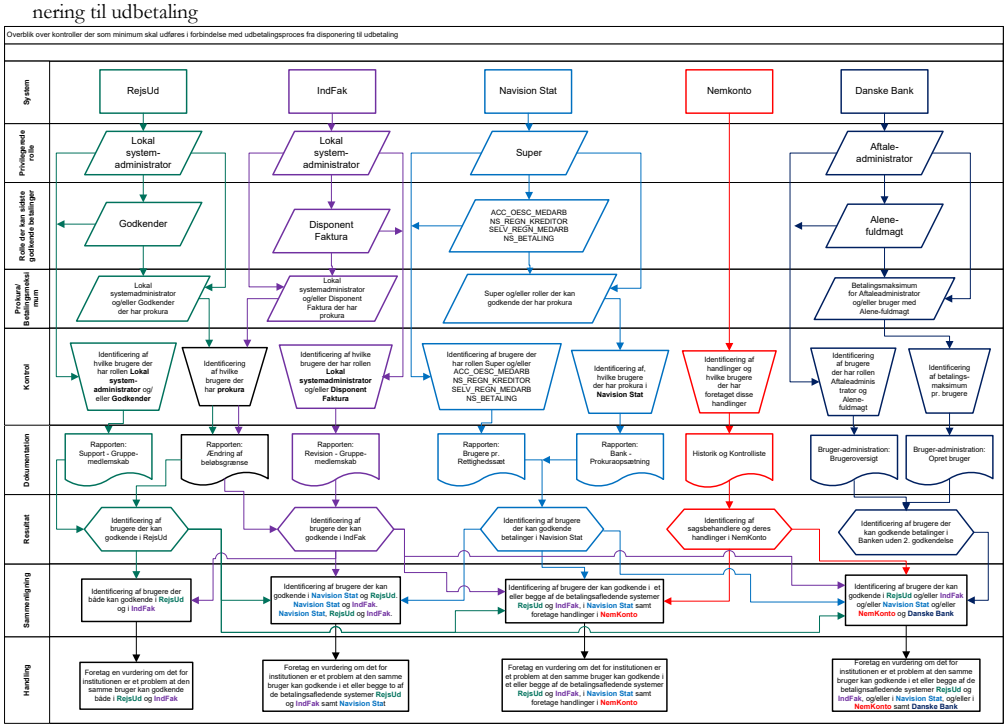
Omfanget af kontrollerne indbefatter ikke der, hvor funktionsadskillelsen er systemmæssigt påtvunget jf. kapitel 2 Systemunderstøttet funktionsadskillelse.

Kontrollerne omfatter følgende:

1. **Overblik**: Dannelse af et overblik over hvem, der kan udføre funktioner på tværs af systemer
2. **Stillingstagen**: Den ansvarlige i institutionen, skal stå inde for at det er berettiget at en bruger kan udføre handlinger i udbetalingsprocessen i flere systemer, herunder godkende og acceptere risikoen

3. **Vurdering**: Vurdering af det arbejdsbetinget behov for brugernes funktioner i systemerne. Selv om der ikke er tale om risici ved at en given medarbejder kan udføre funktioner i et eller flere systemer, skal det vurderes, om hver bruger har behov for at kunne udføre funktionen

Figur 11 - Overblik over kontroller der som minimum skal udføres i forbindelse med udbetalingsprocessen fra disponering til udbetaling



Figur 11 kan benyttes som udgangspunkt for, hvad der som minimum skal kontrolleres med og for. Figuren findes også i Appendiks 6: Overblik over kontroller, hvor figuren bliver forklaret samt kan ses i en større udgave.

5.2 Dokumentation

For at undgå en mistanke om ændring i datamaterialet, anbefales det at rapporter først trækkes i PDF format, der hvor det kan lade sig gøre, og derefter i Excel format, således at man har mulighed for at bearbejde data efterfølgende. Herved har man efterfølgende altid mulighed for at gå tilbage i PDF dokumentationen og validere at Excel dataene ikke er blevet manipuleret.

5.3 RejsUd og IndFak

5.3.1 RejsUd

I afsnit 2.2.1 Systemunderstøttet funktionsadskillelse i RejsUd, identificeres det at brugere med rollen **Godkender** og tildelt prokura har mulighed for at foretage den sidste godkendelse af en rejseafregning eller udlæg. I afsnit 3.1.1 Privilegerede

rettigheder i IndFak og RejsUd identificeres det at rollen **Lokal systemadministrator** har mulighed for at tildele sig selv roller, heriblandt **Godkender**.

Derfor skal det først identificeres om institutionen har brugere, der har rollen **Lokal systemadministrator** og/eller rollen **Godkender**.
Til dette skal rapporten *Support – Gruppemedlemskab* benyttes.

Derefter skal det identificeres om der er tildelt prokura til de brugere der har rollen **Lokal systemadministrator** og/eller rollen **Godkender**.
Til dette skal rapporten *Ændring af beløbsgrænse* benyttes.

Står den samme brugere i begge rapporter, så har man identificeret en bruger der kan foretage godkendelse i RejsUd.

Se Appendiks 2 afsnit 1.1 Kontroller der skal udføres i IndFak/RejsUd, for en beskrivelse af, hvordan man udfører de manuelle kontroller.

Resultatet af disse kontroller skal anvendes til at identificere om der er sammenfald brugermæssigt og funktionsmæssige, på tværs af de systemer, der indgår i den samlede udbetalingsproces.

5.3.2 IndFak

I afsnit 2.2.2 Systemunderstøttet funktionsadskillelse i IndFak, identificeres det at brugere med rollen **Disponent Ordre** eller **Disponent Faktura** og tildelt prokura, har mulighed for at foretage den sidste godkendelse af en ordreafgivelse eller en varemodtagelse. Som i systemet RejsUd, identificeres det også her, at den privilegerede rolle **Lokal systemadministrator** har mulighed for at tildele sig selv roller, heriblandt de to disponent roller.

Derfor skal det først identificeres om institutionen har brugere der har rollen **Lokal systemadministrator** og/eller rollen **Disponent Ordre/Disponent Faktura**.
Til dette skal rapporten *Support – Gruppemedlemskab* benyttes.

Derefter skal det identificeres om der er tilknyttet prokura til de brugere der har rollen **Lokal systemadministrator** og/eller rollen **Disponent Ordre/Disponent Faktura**.
Til dette skal rapporten *Ændring af beløbsgrænse* benyttes.

Står den samme brugere i begge rapporter, så har man identificeret en bruger der kan foretage godkendelse i IndFak.

Se Appendiks 2 afsnit 1.1 Kontroller der skal udføres i IndFak/RejsUd, for en beskrivelse af, hvordan man udfører de manuelle kontroller.

Resultatet af disse kontroller skal anvendes til at identificere om der er sammenfald brugermæssigt og funktionsmæssige, på tværs af de systemer, der indgår i den samlede udbetalingsproces.

5.4 Navision Stat

I afsnit 2.3.1 Systemunderstøttet funktionsadskillelse i Navision Stat, identificeres det at brugere med rollen **NS_BETALING** og tildelt prokura har mulighed for at foretage sidste godkendelse af en betaling. I afsnit 3.1.2 Privilegerede rettigheder i Navision Stat identificeres det at rollen **SUPER** har mulighed for at oprette nye brugere og tildele sig selv roller.

Derfor skal det identificeres om institutionen har brugere, der er opsat med prokura og har rettigheder til at foretage en sidste godkendelse af en betaling i Navision Stat.

Til identifikation af dette skal rapporterne *Brugere pr. rettighedssæt* og *Bank – prokuraopsætning* benyttes.

Står den samme brugere i begge rapporter, så har man identificeret en bruger der kan foretage godkendelse i Navision Stat.

Som beskrevet i afsnit 2.3.1 er det i forbindelse med funktionsadskillelsen systemunderstøttet sikret at den samme bruger ikke kan foretage sidste godkendelsen, hvis denne bruger også har bogført bilaget. Men den samme bruger må godt være opsat således, at det er muligt at brugeren både kan bogføre, første godkende og sidste godkende, så længe alle funktionerne ikke udføres for den samme konkrete udbetaling.

Til identifikation af dette, skal rapporten *Brugere pr. rettighedssæt* benyttes.

Se Appendiks 2 afsnit 1.2 Kontroller der skal udføres i Navision Stat, for en udførlig beskrivelse af, hvordan man udfører de manuelle kontroller.

Resultatet af disse kontroller skal anvendes til at identificere om der er sammenfald brugermæssigt og funktionsmæssige, på tværs af de systemer, der indgår i den samlede udbetalingsproces.

5.5 NemKonto-systemet

I NemKonto-systemet er det ikke muligt fra sagsbehandlergrænsefladen, at trække en rapport eller liste over de brugere/sagsbehandlere, der har adgang til sagsbehandlergrænsefladen i de forskellige institutioner. Dokumentationen i NemKonto-systemet vil derfor have karakter af en bagudrettet kontrol.

Ønsker man at vide mere om, hvilke sagsbehandlere der har gjort hvad, for et givent tidspunkt, skal man ind i sagsbehandlergrænsefladen via www.nemkonto.dk. Her kan sagsbehandlere med adgang til grænsefladen logge ind og se historikken. I historikken er det muligt at se initialerne på den sagsbehandler, der har anvist en aktiv NemKonto, til hvilket CVR/CPR-nummer og for hvilken konto.

På sagsbehandlergrænsefladen er det også muligt at hente kontrollister til og med 2017 via 'Elektronisk uddata', via søgning på kontrolliste[19].

Institutioner med adgang til NemKonto-systemet, skal derfor gennemgå historikken, og kontrollere ændringer, ved at holde disse op mod den dokumentation, der ligger til grund for ændringen eller anvisningen. For eksempel skal et kontonummer matches med det kontonummer der står i den dokumentation, som institutionen har indsendt for at sikre, at det ikke er en uvedkommendes konto, der anvendes.

Idet der, som tidligere beskrevet, sendes fysiske aktiveringsbreve mellem NemKonto og den adresse der er registreret på en myndigheds CVR-nummer, eller på modtageres CPR-nummer, er kontrolfunktionaliteten i NemKonto-systemet ikke yderligere udviklet.

Resultatet af den gennemgået historik anvendes til at identificere om der er sammenfald brugermæssigt på tværs af systemerne, der indgår i den samlede udbetalingsproces.

5.6 Danske Banks onlineløsning District

I afsnit 2.5.4 Statens Administration, identificeres det, at der hvor Statens Administration (SAM) har overtaget opgaven med at oprette betalingsordre eller betalinger på vegne af en institution, har SAM-brugerne rollen **Aftaleadministrator** samt funktionsadskillelse via 2-i-forening [A-fuldmagt]. Så den bruger, der opretter en betalingsordre/betaling vil altid være forskellig fra den bruger, der fortager den sidste godkendelse af betalingen.

I afsnit 3.1.4 Privilegerede rettigheder i Danske Banks onlineløsning District afklares det at rollen **Aftaleadministrator** kan tildele brugeradgange og brugerrettigheder, for eksempel fuldmagter, der giver adgang til at godkende betalinger.

For institutioner, der har brugere med adgang til Danske Banks onlineløsning District, skal det derfor identificeres, hvilke: brugerrettigheder, fuldmagtstype og tildelte betalingsmaksimum disse brugere har.

Til identifikation af dette skal menupunktet *Brugeroversigt* benyttes.

---

[19] Der findes ingen kontrollister efter 2017, idet der i 2017 blev foretaget en systemmæssig ændring.

Se Appendiks 2 afsnit 1.4 Kontroller der skal udføres i District, for en beskrivelse af, hvordan man udfører de manuelle kontroller.

Faktaboks - Retningslinjer

Der eksisterer ingen særskilte retningslinjer for, hvilke medarbejdere institutionen kan udpege til at være henholdsvis aftale- eller brugeradministrator eller brugere i SKB/OBS.

Tildeling af rettigheder bør dog ske i overensstemmelse med de generelle disponeringsregler og god forvaltningsskik i øvrigt.

Resultatet af disse kontroller skal anvendes til at identificere om der er sammenfald brugermæssigt og funktionsmæssige, på tværs af de systemer, der indgår i den samlede udbetalingsproces. Er der sammenfald bør institutionen foretage risikovurdering og implementere kompenserende kontroller.

5.7 Det samlede resultat

Det samlede resultat kan vises i en matrix der kan synliggøre, hvilke systemer den enkelte medarbejder samlet set har adgang til, samt om nogle medarbejdere har en uhensigtsmæssig adgang til flere systemer, som fx kan indebære, at de kan gennemføre en udbetalingsproces fra start til slut eller omgå centrale kontroller.

I Appendiks 2: Kontrol af udbetalingsprocessen findes Tabel 3. **Redskab til oversigt over medarbejderes adgange på tværs af systemer – med adgang til funktionsadskilte processer i udbetalingsprocessen**, der viser et eksempel på, hvordan denne matrix er udfyldt, på baggrund af de opnåede kontrolresultater pr. system som gennemgås i Appendiks 2. Matrixen er en tilretning til den matrix, som anvendes i Vejledning om intern finansiel kontrol[20].

5.8 Institutionens forpligtelse

Den enkelte institution har ikke kun en forpligtelse til at have et overblik over, hvilke brugere som kan udføre forskellige funktioner på tværs af de systemer som indgår i udbetalingsprocessen fra disponering til udbetaling.

Den funktionsansvarlige i institutionen skal ligeledes godkende og derved acceptere den risiko der kan være, ved at de samme brugere kan udføre handlinger i udbetalingsprocessen på tværs af flere systemer.

[20] Læs mere om Redskab til oversigt over medarbejderes adgange på tværs af systemer.

Det skal endvidere vurderes, om de identificerede brugere har et arbejdsbetinget behov, for at kunne udføre de forskellige funktioner.

Det skal afslutningsvist vurderes, om de tildelte rettigheder stemmer overens med de opgaver, der skal varetages undervejs frem til udbetaling

Vurderes det at der findes brugere i institutionen, som ikke har et arbejdsbetinget behov, så skal den ansvarlige i institutionen sørge for at rettighederne og/eller opsætningerne bliver tilpasset, eller helt fjernet, således at den enkelte bruger kun har adgang til de handlinger, som brugeren også har et arbejdsbetinget behov for. Ved løbende at have fokus på dette, bliver de fremtidige kontroller mere retvisende.

Det er endvidere institutionens ansvar at identificere øvrige nødvendige kontroller, under hensynstagen til egen risikovurdering.

I Appendiks 1: Skabelon til kontrolrapport, er udarbejdet et eksempel på, hvordan dokumentationen til udførte kontroller kan se ud, så det efterfølgende er muligt at følge op på og vurdere fortsat behov.

5.8.1 Dokumentation

For systemer der håndtere økonomiske tranaktioner, anbefales det, at der vurderes en række elementer i forhold til tildelingen af rettigheder, specielt i forhold til privilegerede rettigheder. Nedenstående punkter er udpluk fra en inspirationsliste som sikkerdigital.dk står bag.[21]

- Dokumentation af tildeling med angivelse af årsag, evt. godkendelse og dato. – så det efterfølgende er muligt at følge op og vurdere fortsat behov, fx ved opgaveskrift.
- Vurdering af begrænset eller tidsbestemt tildeling af rettigheder – så de tildelte rettigheder understøtter konkrete og aktuelle behov i opgavevaretagelsen, og endvidere medvirker til at minimere risikoen for utilsigtede fejl og misbrug.
- Ved afvigelser fra eventuelle eksplicitte retningslinjer dokumenteres godkendelse af afvigelsen – så eventuelle risici er synliggjorte. Bør ledelsesgodkendes og registreres ved informationssikkerhedskoordinator.
- Periodisk opfølgning på tildelte rettigheder, fortsatte relevans og afledt adfærd [min. hver 6. måned] – så risikoen for misbrug eller fejl minimeres, og så retningslinjer og lovgivning [jf. fx databeskyttelsesforordningen] efterleves.
- Periodisk gennemsyn og re-information af relevante instrukser – så medarbejdere, der er tildelt privilegerede rettigheder, løbende holdes opdaterede om gældende og evt. justerede retningslinjer.

---

[21] Se den fulde liste på sikkerdigital.dk

- Periodisk rapportering på området – så de ansvarlige chefer løbende holdes orienteret om sikkerhedsmæssige forhold herunder eventuelle uhensigtsmæssigheder.
- Udarbejdelse af plan for eventuelle korrigerede handlinger efter registrerede hændelser – så konstaterede uhensigtsmæssigheder kan prioriteres og håndteres struktureret og effektivt.

Kapitel 6.
RPA - Implementering

6. RPA - Implementering

Med udviklingen og lokal implementering af RPA (Robotic Process Automation) til automatisering af forretningsprocesser skal institutionen være bevidst om det ansvar og de regler der er gældende for implementering af RPA. Dette både for det enkelte system, men også på tværs af systemer.

6.1 Systemmæssigt ansvar for RPA-processer

Vælger en institutioner at få implementeret RPA-processer på ét eller på tværs af flere systemer, i Økonomistyrelsens systemportefølje, så må implementeringen ikke kompromittere den indbyggede forretningslogik i den enkelte applikation, og de sikkerhedsforanstaltninger, der er pålagt det enkelte system. Den automatiserede proces skal følge samme regler og principper som, hvis det var en bruger der udførte processen.

Institutionen har selv det systemmæssige ansvar, hvilket betyder at institutionen har ansvar for at robotterne bliver tilpasset i det omfang, det skulle blive nødvendigt i forlængelse af en opdatering af applikationen[22].

6.2 RPA – for Applikationsoptimering

Systemerne i Økonomistyrelsens systemportefølje bliver løbende ændret, med forskellig frekvens alt efter system. Dette betyder at, hvis der er implementeret tilknyttede RPA – processer lokalt i institutionen, og der opstår ændringer i et ØS system, kan det aflede nødvendig ændring i RPA-processerne.

Økonomistyrelsen frigiver, i forhold til Navision Stat, ved hver opdatering en liste over rettede objekter. Denne liste kan institutionen benytte til at identificere, om en opdatering afleder behov for re-konfiguration af institutionens RPA-processer[23].

6.3 RPA og funktionsadskillelse

Ved implementering af RPA på ét eller flere systemer, påtager institutionen sig et ansvar som systemejer for processen. For processer der afleder en bogføring eller en udbetaling fra et system, er dette særligt kritisk.

---

[22] Se servicebeskrivelser for Økonomistyrelsens systemer og løsninger
[23] Servicebeskrivelse for Navision Stat.

Funktionsadskillelsen må under ingen omstændigheder omgås, og den implementerede RPA løsning skal være opbygget af mindst to forskellige regnskabsprocesser, der afvikles med forskellige konti, således at indbygget funktionsadskillelse jf. §§ 28 og 46 i regnskabsbekendtgørelsen overholdes på brugerniveau i systemet. To robotter alene sikrer *ikke* en funktionsadskillelse.

Robotterne må ikke godkende hinandens aktivitet "blindt", hvilket fordre at der implementeres et decideret godkendelses-flow i begge regnskabsprocesser. Godkendelses flowet skal have defineret klare og restriktive regelsæt og robotten skal kunne kontrollere udbetalingen op mod det oprindelige grundlag, ligesom en almindelige bruger ville gøre.

Kan robotten ikke verificere kontrollen, fx en udbetaling, så skal kontrollen overgå til manuel behandling.

Der er krav om garanti for dataintegritet som er gældende på tværs af systemer, der indgår i betalingsprocessen. En disponering skal altid godkendes af et menneske, som første led i betalingsprocessen. Efterfølgende godkendelser og procestrin kan udføres af en RPA-implementering, så længe det kan verificeres, at data ikke har været ændret efter den første godkendelse.

6.4 RPA - for Adgangsstyring og Rettighedstildeling

Ønsker en institution, eller har en institution allerede fået udviklet og implementeret en RPA-proces til tildeling og ændring af roller og rettigheder i et system, så har institutionen følgende forpligtelse:

- Sikre integriteten af RPA funktionaliteten ved bl.a. kodereveiw, adskillelse af udviklings- og produktionsmiljøer, samt sikring af kildekoden.
- Definere risici ved RPA-processen, ved at udarbejde en risikovurdering eller en konsekvensanalyse af, hvad robotten kan påvirke. *(Her er det vigtig at tænke på, at hvis robotten gør noget galt, så kan det komme til at gå galt mange gange).*
- Sikre at der er beskrevet proces for godkendelse og tildeling af roller og rettigheder, se afsnittet Institutionens forpligtelse.
- Sikre at robotten kun tildeles samme rettigheder, efter samme retningslinjer, som en fysisk person, der skal udføre opgaven/handlingerne hos institutionen.
- Foretage løbende kontrol, fx kontrol af brugere og deres rettigheder mv.

Faktaboks - Support

Økonomistyrelsen yder ikke support på de RPA-processer som institutionen får implementeret lokalt.

Kapitel 7.
Oversigt over appendikser og ekstra materiale

7. Oversigt over appendikser og ekstra materiale

Her ses et overblik over de tilhørende appendikser, som er blevet udarbejdet til denne vejledning, samt ekstra materiale bestående af Excel-skabelon.

- 1. Appendiks – Skabelon til kontrolrapport
  Indeholder en word-skabelon, hvor man kan angive resultatet af den udførte kontrol.
  (Skal bruges af de kontroludførende og mellemlederne fx de økonomiansvarlige)
- 2. Appendiks – Kontrol af udbetalingsprocessen
  Indeholder en detaljeret beskrivelse af, hvilke kontroller der skal udføres i udbetalingsprocessen samt hvordan disse kontroller kan udføres.
  (Skal bruges af de kontroludførende)
- 3. Appendiks – Kontrol af privilegerede rettigheder i IndFak/RejsUd
  Indeholder en detaljeret beskrivelse af, hvordan man skal foretage kontrol af privilegerede rettigheder i IndFak/RejsUd.
  (Skal bruges af de kontroludførende)
- 4. Appendiks – Kontrol af privilegerede rettigheder i Navision Stat
  Indeholder en detaljeret beskrivelse af, hvordan man skal foretage kontrol af privilegerede rettigheder i Navision Stat.
  (Skal bruges af de kontroludførende)
- 5. Appendiks – Kontrol af privilegerede rettigheder i Danske Banks onlineløsning District
  Indeholder en detaljeret beskrivelse af, hvordan man skal foretage kontrol af privilegerede rettigheder i Danske Banks onlineløsning District.
  (Skal bruges af de kontroludførende)
- 6. Appendiks – Overblik over kontroller
  Indeholder en visio-tegning der skal give et overblik over de kontroller der som minimum skal udføres, i forbindelse med den samlede udbetalingsproces.
  (Skal bruges af de kontroludførende og mellemlederne fx de økonomiansvarlige)
- Excel-skabelon - Redskab til oversigt
  Indeholder en skabelon inkl. eksempel til oversigt over medarbejderes adgange på tværs af systemer – med adgang til funktionsadskilte processer i udbetalingsprocessen.
  Benyttes i forbindelse med 2. Appendiks – Kontrol af udbetalingsprocessen.
  (Skal benyttes at de kontroludførende)

ISBN nummer 87-7956-627-8

oes.dk