ØKONOMISTYRELSEN

Kontrolvejledning

10.06.2020
ØSY/TRI/CLG

Rettighedskontrol: Administration af brugeradgange i IndFak og RejsUd

Denne vejledning beskriver en række manuelle kontroller af brugere med privilegerede rettigheder, som skal foretages af institutionen selv.

Baggrund

Det er institutionernes ansvar at foretage rettighedskontroller i egen institution, herunder kontrol af egne privilegerede brugere. Kontrollerne skal gennemføres med udgangspunkt i institutionens valg af organisering og samlede risikobillede. Afhængigt af institutionens organisering vil denne vejledning derfor skulle anvendes af systemadministratorer og/eller controllere ude i institutionerne.

Bemærk at denne vejledning ikke fratager institutionerne deres forpligtelse til at foretage egen risikovurdering, herunder identificere hvilke løbende kontroller der samlet set er nødvendige for at leve op til denne forpligtelse.

Omfang

Systemerne IndFak og RejsUd indeholder brugerroller med særlige privilegier og med udvidet adgang. For at undgå svig og misbrug i systemer, skal tildelingen af disse roller løbende kontrolleres internt, ligesom resultatet af kontrollen efterfølgende skal godkendes ved den ansvarlige personaleleder.

Der skal som *minimum* kontrolleres for følgende ved den enkelte institution:

1. Om brugere oprettet med privilegerede rettigheder, har et godkendt funktionsafhængigt behov.
2. Om der er sket en tildeling af prokura til en lokal administrator, der ikke kan begrundes.
3. Om en lokal administrator har tildelt prokura til en anden bruger, der ikke kan begrundes.
4. Om en lokal administrator har oprettet andre lokale administratorer, der ikke kan begrundes.
5. Om lokal administrator har foretaget en ændring af e-mail eller password for en bruger, der ikke kan begrundes.
6. Om lokal administrator har udskiftet et rejsekreditornummer for et udlæg, således at udbetaling tilgår anden kreditor ind forventet.

Det er institutionens ansvar at identificere øvrige kontroller, som er nødvendige for at leve op til forpligtelsen til at foretage egen risikovurdering.

I forbindelse med systemforvaltningen af IndFak og RejsUd, påhviler det endvidere systemejer, dvs. Økonomistyrelsen, at sikre, at der foretages en rettighedskontrol for administration af brugeradgange i IndFak og RejsUd for privilegerede brugere ansat i enten Økonomistyrelsen (systemforvalter), Statens Administration (level 1 systemsupport) og hos Miracle, Tricom, og Ibistic (leverandør med underleverandører).

Brugere med privilegerede rettigheder
Brugere med privilegerede rettigheder er for IndFak og RejsUd defineret som brugere med rollerne:

Rolle	Forklaring
IndFak Lokal systemadministrator	Ved *IndFak Lokal systemadministrator* forstås administration af brugermodulet og opsætning og konfiguration. Rollen Lokal systemadministrator tildeles på lokalt niveau, typisk på et koncernniveau som fx et ministerområde og nedarves i de underliggende organisationer. Lokal systemadministrator giver adgang til at udsøge data på detaljeret niveau. Lokal systemadministrator kan ene og alene oprette/inaktivere brugere samt tildele/fjerne roller samt konfigurere systemopsætning. Lokal systemadministratorrollen giver ikke adgang til nogen form for behandling af bilag og kan derfor ikke indgå i godkendelsesflowet.
RejsUd Lokal systemadministrator	*RejsUd Lokal systemadministrator* kan danne rapporter, administrere kontor og brugere, samt ændre / redigere opsætning for udlæg og rejse.
RejsUd: Godkender (kombineret med en opsat prokura)	*RejsUd: Godkender* kan med tilstrækkelig prokura godkende bilag, der i forvejen er kontrolleret og underskrevet af anden person.

Rolle	Forklaring
IndFak: Disponent (kombineret med en opsat prokura)	*IndFak: Disponenter* kan med tilstrækkelig prokura godkende bilag, der i forvejen er varemodtaget af anden person.

Rettighederne kan ses i brugerindstillinger under kontor og brugere.

Kontrol 1: Om brugere oprettet med privilegerede rettigheder, har et godkendt funktionsafhængigt behov

Der skal dannes et øjebliksbillede af, hvorvidt brugere med privilegerede rettigheder har et godkendt funktionsafhængigt behov for netop disse rettigheder for både IndFak og RejsUd.

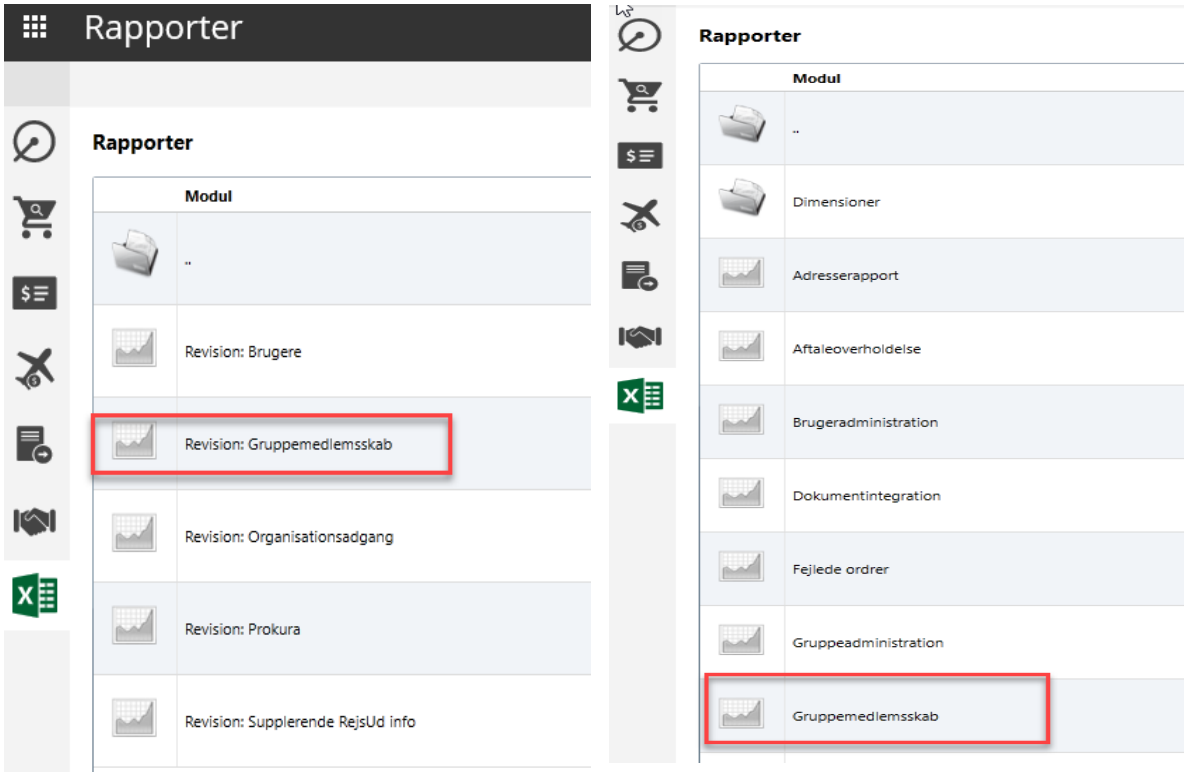
Roller der skal kontrolleres:

- Rolle IndFak: Lokal systemadministrator
- Rolle IndFak: Disponent
- Rolle RejsUd: Lokal systemadministrator
- Rolle: RejsUd: Godkender

Følgende rapporter anvendes:

- IndFak Administrationsdel – Rapporter – Revision – Gruppemedlemsskab, periode -> Excel format (viser de roller der er tildelt/slettet for den valgte periode).
- IndFak Administrationsdel – Rapporter – Support – Gruppemedlemsskab, "Med underorganisationer" -> Excel format (viser øjebliksbillede af roller)

Rapporten skal trækkes på niveau: Højeste lokale organisationsniveau.



Handling:

1. Resultatet kommenteres, herunder om der er behov for justeringer i brugere med privilegerede rettigheder.

2. Rapporten inkl. kommentarer udskrives og underskrives af kontrollant, samt ledelsesgodkendes.

Kontrol 2: Om der er sket en tildeling af prokura til en lokal administrator, der ikke kan begrundes

En lokal administrator kan ikke danne transaktioner i IndFak og RejsUd, uden yderligere roller og prokura, og har som udgangspunkt heller ikke brug for denne adgang. Men en bruger med lokal administratoradgang kan godt tildele roller og prokura til en anden lokal administrator. Derfor er det kritisk at undersøge, om dette er sket, uden tilstrækkelig dokumentation herfor.

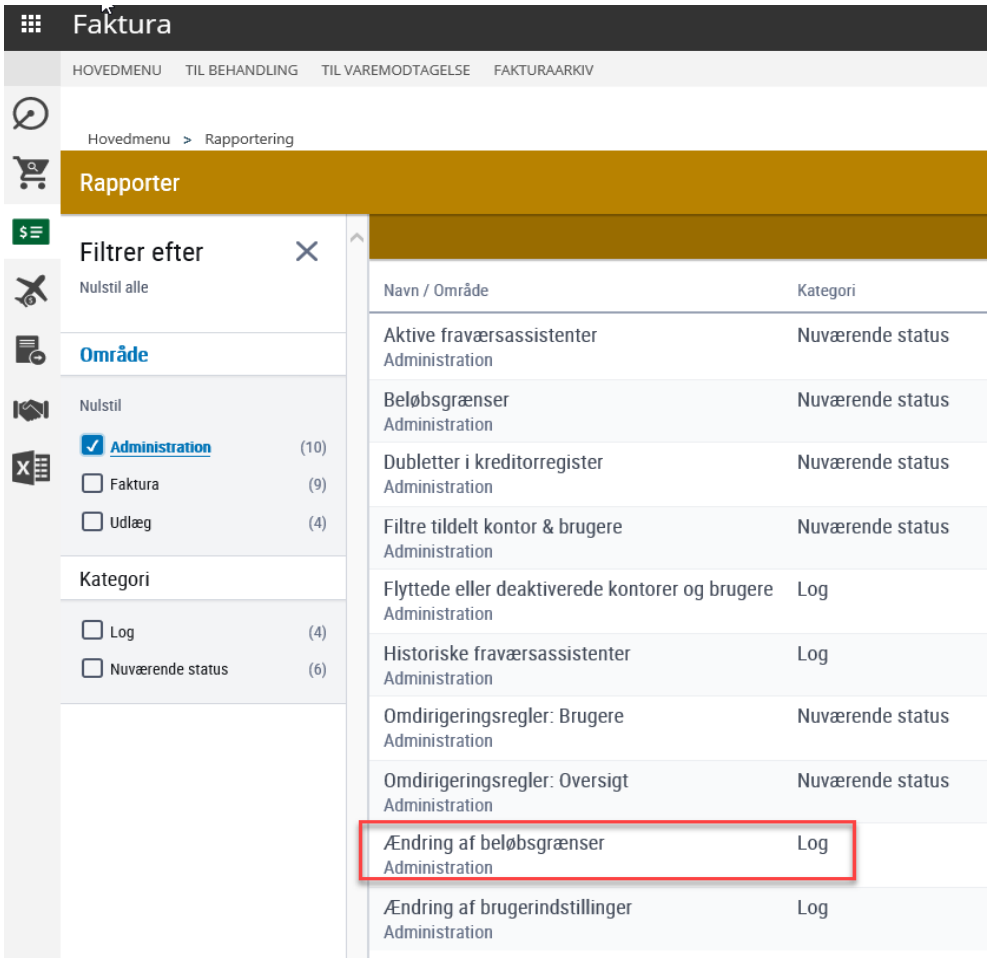
Roller der skal kontrolleres:

- Rolle IndFak: Lokal systemadministrator
- Rolle RejsUd: Lokal systemadministrator

Følgende rapport anvendes:

- Fakturadel – Rapporter – Ændring af beløbsgrænser, Start – Slut periode -> Excel format

Rapporten skal trækkes på niveau: Højeste lokale organisationsniveau.



Handling:

1. Resultatet kommenteres med oplysning om, hvem der har fået rollen/rollerne og prokura. Dokumentationen skal indeholde en ledelsesmæssig beslutning for tildelingen.
2. Rapporten inkl. kommentarer og dokumentation udskrives og underskrives af kontrollant samt ledelsesgodkendes.

Kontrol 3: Om en lokal administrator har tildelt prokura til en anden bruger, der ikke kan begrundes

Tildeling af prokura skal ske ved lokal administrator på samme niveau, som prokuraen skal anvendes. Men en bruger, med lokal administratoradgang, kan tildele roller og prokura til en vilkårlig anden bruger, uden der findes et arbejdsbetinget behov herfor. Derfor er det kritisk at undersøge, om dette er sket med en tildeling tilstrækkelig dokumentation for et arbejdsbetinget behov.

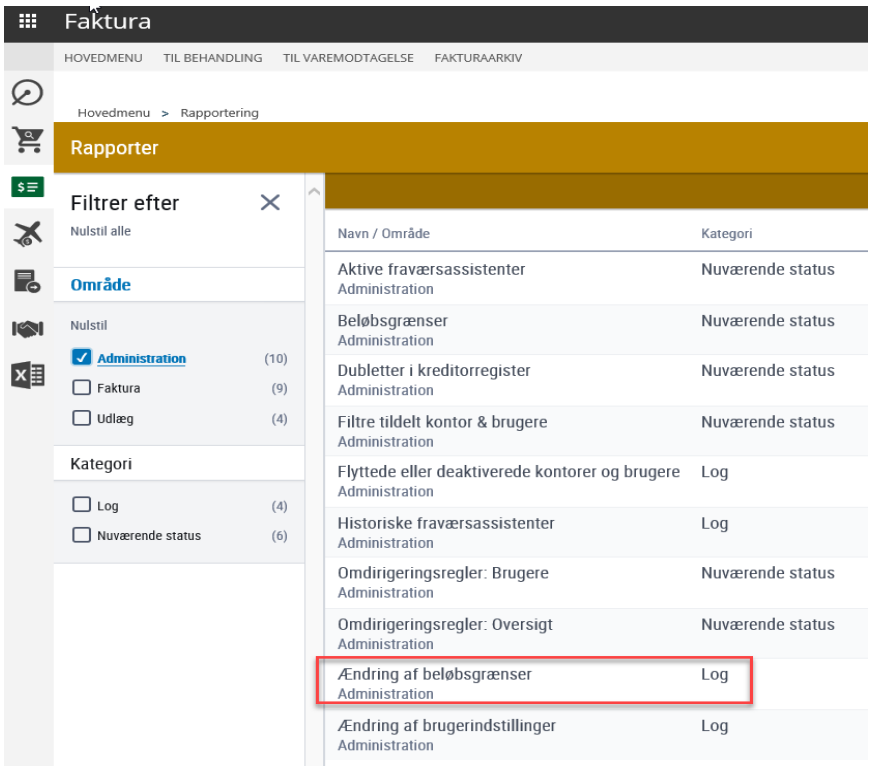
Roller der skal kontrolleres:

- Rolle IndFak: Lokal systemadministrator
- Rolle RejsUd: Lokal systemadministrator

Følgende rapport anvendes:

- Fakturadel – Rapporter - Ændring af beløbsgrænser, Start – Slut periode -> Excel format

Rapporten skal trækkes på niveau: Højeste lokale organisationsniveau.



Handling:
1. Resultatet kommenteres med oplysning om, hvem der har fået rollen/rollerne og prokura. Dokumentationen skal indeholde en ledelsesmæssig beslutning.
2. Rapporten inkl. kommentarer og dokumentation udskrives og underskrives af kontrollant, samt ledelsesgodkendes

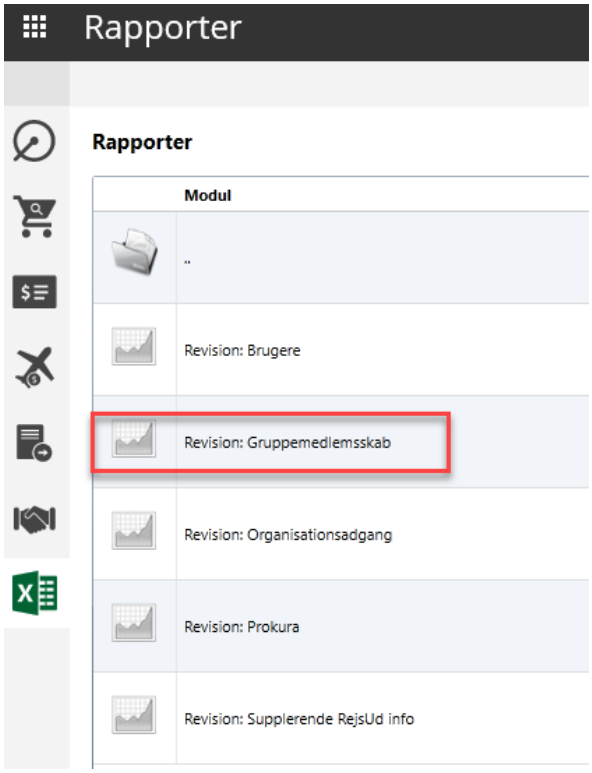
Kontrol 4: Om en lokal administrator har oprettet andre lokale administratorer, der ikke kan begrundes

En lokal administrator kan oprette en anden lokal administrator. Det bør undersøges, om der er tilstrækkelig dokumentation herfor.

Roller der skal kontrolleres:
- Rolle IndFak: Lokal systemadministrator
- Rolle RejsUd: Lokal systemadministrator

Følgende rapport anvendes:
- IndFak Administrationsdel – Rapporter – Revision – Gruppemedlemsskab, periode -> Excel format (viser de roller der er tildelt/inaktiveret for den valgte periode).

Rapporten skal trækkes på niveau: Højeste lokale organisationsniveau.



Handling:

1. Resultatet kommenteres med oplysning om, hvem der har fået rollen, og hvem der har tildelt rollen. Dokumentationen skal indeholde en ledelsesmæssig beslutning.
2. Rapporten inkl. kommentarer og dokumentation udskrives og underskrives af kontrollant samt ledelsesgodkendes.

Tips:

- Tjek om der er mange forekomster på samme tidspunkt, fx ved at kigge på kolonnen "Sidst ændret" eller "Sidst ændret af".
- Flytning af brugere er også en ændring.
- Det er meget tunge regneark. Det kan derfor være nødvendigt at kopiere og indsætte som værdier i et nyt regneark.

Kontrol 5: Om lokal administrator har foretaget en ændring af e-mail eller password for en bruger, der ikke kan begrundes

Lokal administrator har adgang til at rette notifikations-e-mail og nulstille password for andre brugere, hvorved det er muligt at logge på som en anden bruger, angive nyt password, og sørge for, at brugerens 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.

Derfor skal det kontrolleres om dette er sket, og om det i så fald kan begrundes.

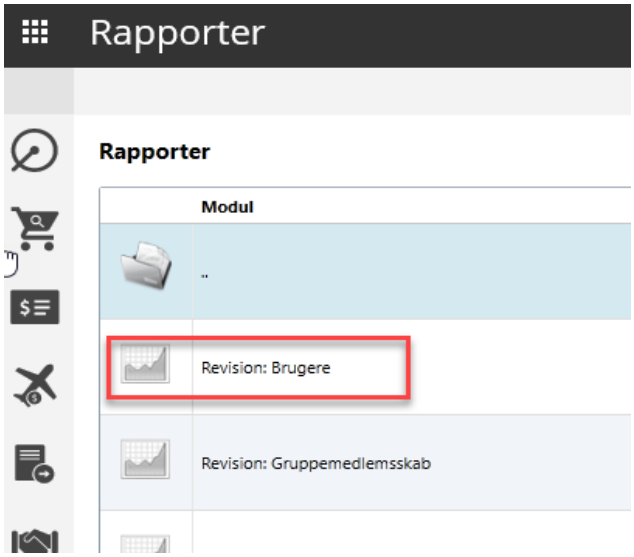
Roller der skal kontrolleres:

- Rolle IndFak: Lokal systemadministrator
- Rolle RejsUd: Lokal systemadministrator

Følgende rapport anvendes:

- IndFak Administrationsdel – Rapporter – Revision – Brugere, periode -> Excel format (viser brugerændringer foretaget på brugere i den valgte periode).

Rapporten skal trækkes på niveau: Højeste lokale organisationsniveau.



Handling:

1. Resultatet kommenteres med begrundelse for ændringen. Dokumentation: mailkorrespondance eller eventuelt sagsnummer.
2. Rapporten inkl. kommentarer og dokumentation udskrives og underskrives af kontrollant samt ledelsesgodkendes.

Tips:
Nogle ændringer kan være legale, som de ændringer der er listet nedenfor, tjek derfor om:

- Ændringen er sket til en "dummy" e-mail konto, fx trash@
- Der evt. er et fejlagtigt "blank" tegn efter den oprindelig email
- Der er tegn på, at den oprindelige e-mail blot var oprettet forkert, fx forkert angivet
- Der er tegn på, at ændringen er sket indenfor institutionens domæne
- Ændringen kan være udført i forbindelse med en ressortomlægning

Kontrol 6: Om lokal administrator har udskiftet et rejsekreditornummer for et udlæg, således at udbetaling tilgår anden kreditor ind forventet

Aktuelt sker der en mapning mellem kreditorer overført fra Navision Stat til RejsUd og rejsekreditorer oprettet som brugere i RejsUd. Derfor er det muligt som Lokal administrator at ændre denne mapning og derved omdirigere den udbetaling af et udlæg, der var tiltænkt en specifik kreditor, til en anden kreditor.

Det skal derfor tjekkes om der er foretaget ændring af mapninger ved Lokal administrator, som ikke kan begrundes.

Roller der skal kontrolleres:

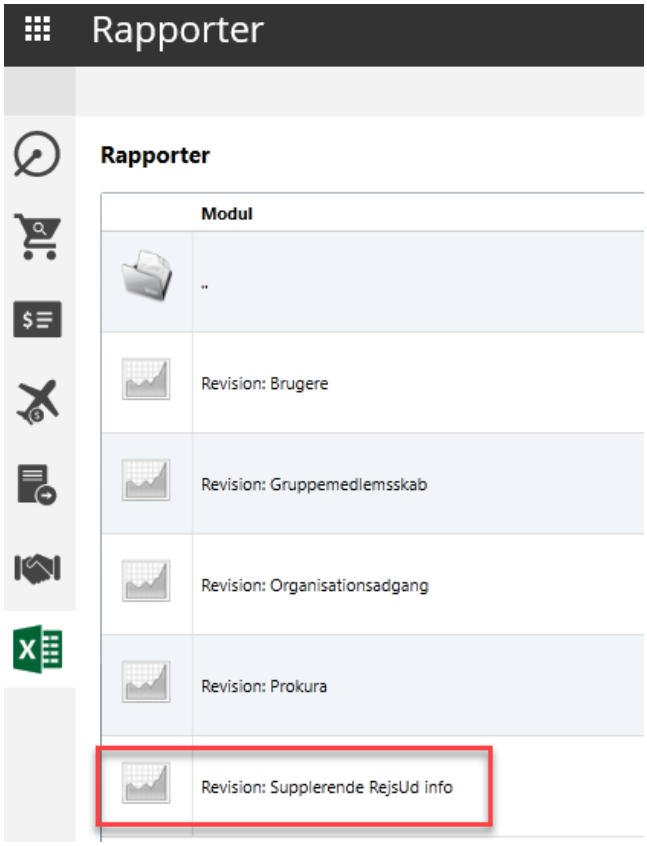
- Rolle IndFak: Lokal systemadministrator

- Rolle RejsUd: Lokal systemadministrator

Følgende rapport anvendes:

- IndFak Administrationsdel – Rapporter – Revision – Entitetsværdier/Revision: Supplerende RejsUd info, periode -> Excel format (viser ændringer i RejsUd supplerende oplysninger for den valgte periode).

Rapporten skal trækkes på niveau: Højeste lokale organisationsniveau.



Handling:

1. Resultatet kommenteres med begrundelse for ændringen. Dokumentation: e-mailkorrespondance eller eventuelt sagsnummer.
2. Rapporten inkl. kommentarer og dokumentation udskrives og underskrives af kontrollant samt ledelsesgodkendes.

Tips:

OBS: rapporten er meget tung – og skal muligvis trækkes i flere omgange over kortere perioder!

Nogle ændringer kan være legale, tjek derfor om:

- Der i opsætningsøjemed kan være sket en reel forveksling af brugere, fx fordi 2 kreditorer har tæt på samme navn