ØKONOMISTYRELSEN

Kontrolvejledning

25. juni 2024/8. november 2024
ØSY/CLG

Rettighedskontrol: Administration af brugeradgange i Statens Digitale Indkøb

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

Systemet Statens Digitale Indkøb 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 har mulighed for at tildele sig selv rollen Godkender, 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

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 Statens Digitale Indkøb, påhviler det endvidere systemejer, dvs. Økonomistyrelsen, at sikre, at der foretages en rettighedskontrol for administration af brugeradgange i Statens Digitale Indkøb for privilegerede brugere ansat i enten Økonomistyrelsen (systemforvalter), Statens Administration (level 1 systemsupport) og hos Acentio (leverandør).

Brugere med privilegerede rettigheder

Brugere med privilegerede rettigheder er for Statens Digitale Indkøb defineret som brugere med rollerne:

Rolle	Forklaring
Lokale Systemadministrator	Ved *Lokal systemadministrator* forstås administration af brugermodulet og opsætning og konfiguration. Rollen tildeles på lokalt niveau, typisk på et koncern niveau som fx et ministerområde og nedarves til de underliggende organisationer. Lokale systemadministratorer kan oprette/slette (eller inaktivere) samt tildele roller til brugere, der er oprettet på samme koncern niveau eller underliggende. Oprettelse af Lokal Systemadministrator er underlagt systemunderstøttet 4-øje princip, således at oprettelsen skal godkendes af en anden Lokal Systemadministrator. Lokal Systemadministrator giver adgang til at udsøge data på detaljeret niveau. Lokal systemadministrator rollen giver ikke adgang til nogen form for behandling af bilag og kan derfor ikke indgå i godkendelsesflowet.
Fakturagodkender	*Fakturagodkender* kan med tilstrækkelig prokura godkende bilag, der i forvejen er bekræftet af anden person.
Ordregodkender	*Ordregodkender* kan med tilstrækkelig prokura godkende ordrer, der er oprettet af Indkøber/Rekvirent. Hvis der er opsat Autogodkendelses regel og reglen er opfyldt, kan ordre/faktura autogodkendes og sendes til betaling uden yderligere godkendelse.

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 Statens Digitale Indkøb

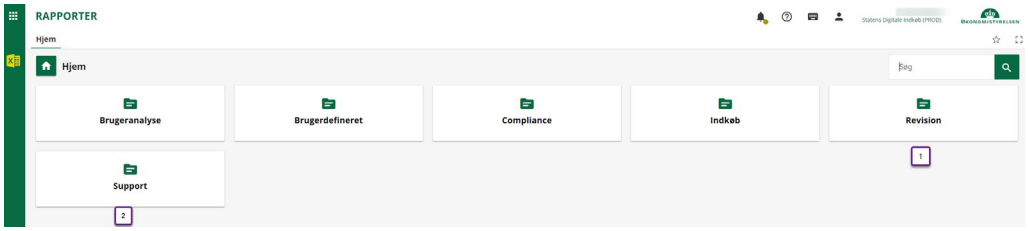
Roller der skal kontrolleres:

- Rolle: Lokal systemadministrator
- Rolle: Fakturagodkender
- Rolle: Ordregodkender

Følgende rapporter anvendes:

1. Administration - Rapporter – Revision – Gruppemedlemsskab, periode -> excel (viser de roller der er tildelt/slettet for den valgte periode).
2. Administration - Rapporter – Support – Gruppemedlemsskab, "Med underorganisationer" -> excel (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.

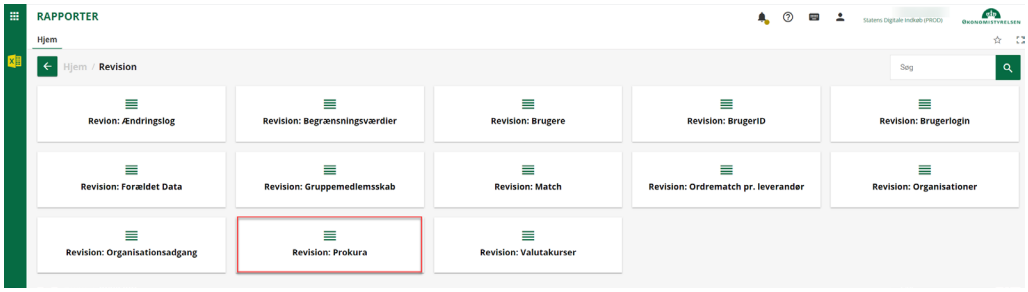
Kontrol 2: Om der er sket en tildeling af prokura til en lokal administrator, der har mulighed for at tildele sig selv rollen ordre/faktura Godkender, der ikke kan begrundes

En lokal administrator kan ikke danne transaktioner i Statens Digitale Indkøb, uden yderligere roller og prokura, og har som udgangspunkt heller ikke brug for denne adgang/prokura. 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.

Roller der skal kontrolleres:

Rolle: Lokal systemadministrator
Rolle: Ordregodkender
Rolle: Fakturagodkender

Følgende rapport anvendes: Administration – Rapporter – Revision - Prokura, Start – Slut periode -> Excel format
Rapporten skal trækkes på niveau: Højeste lokale organisationsniveau



Resultatet kommenteres med oplysning om, hvem der har fået rollen-/erne og prokura.

Dokumentationen bør indeholde en ledelsesmæssig beslutning.

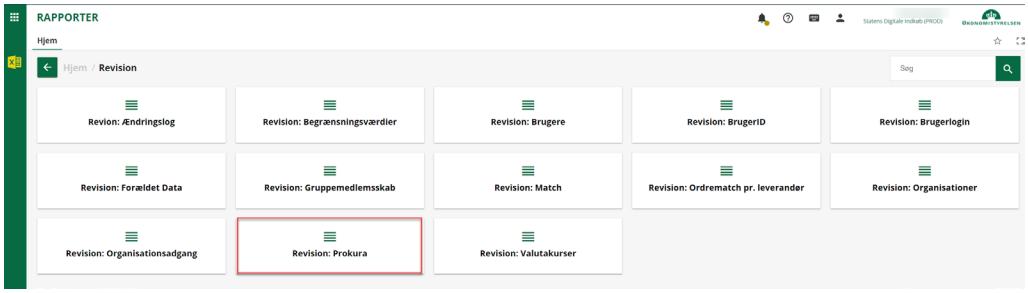
Kontrol 3: Om en lokal administrator har tildelt prokura til en anden bruger, der ikke kan begrundes

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

Roller der skal kontrolleres:

Rolle: Lokal systemadministrator

Følgende rapport anvendes:
Administration – Rapporter – Revision - Prokura, 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.

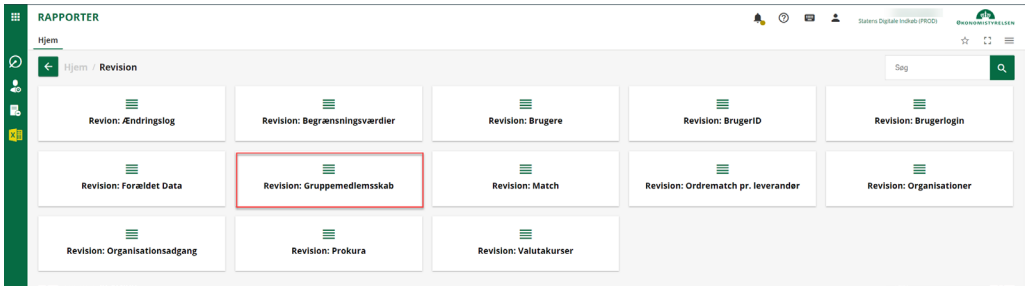
Roller der skal kontrolleres:

Rolle: Lokal systemadministrator

Følgende rapport anvendes:

Administration – 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

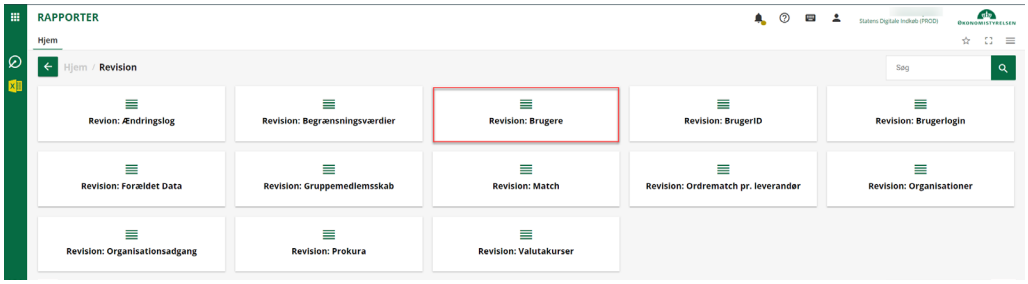
Lokal administrator har adgang til at rette notifikations-e-mail og nulstille password for andre brugere, hvorved det er muligt at logge på som en anden bruger, angive nyt password, og sørge for, at brugerens normale e-mail notifikationer fremsendes til anden bruger end den brugerkonto, der logges på med. Derved bliver det muligt at overtage prokura fra en given bruger på løsningen, uden at brugeren opdager det.
Det skal derfor kontrolleres om dette er sket, og om det kan begrundes.

Roller der skal kontrolleres:

Rolle: Lokal systemadministrator

Følgende rapport anvendes:

Administration – 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, kontroller 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
- Der er tegn på, at ændringen er sket inden for institutionens domæne
- Ændringen kan være udført i forbindelse med en ressortomlægning