



Riksrevisjonen

MOTTATT 04.06.2015

14/16076=6

Vår saksbehandler  
Kristin Weidemann 22241365  
Vår dato 29.05.2015 Vår referanse 2014/01186-44  
Deres dato Deres referanse

Utsatt offentlighet jf. rrevl. § 18(2)

HUSBANKEN  
Postboks 1404  
8002 BODØ

### Revisjon av regnskap og budsjett disponering for Husbanken 2014

Riksrevisjonen har revidert Husbankens årsregnskap for 2014 og kontrollert et utvalg disposisjoner som ligger til grunn for årsregnskapet.

Vår oppgave er ifølge lov av 7. mai 2004 nr. 21 om Riksrevisjonen § 9, jf. instruks om Riksrevisjonens virksomhet av 11. mars 2004 § 3, å kontrollere om regnskapet gir et riktig bilde av den økonomiske virksomheten, herunder:

- a) bekrefte at regnskapene ikke inneholder vesentlige feil og mangler, og
- b) kontrollere om de disposisjoner som ligger til grunn for regnskapet er i samsvar med Stortingets vedtak og forutsetninger og gjeldende regelverk, og om disposisjonene er akseptable ut fra normer og standarder for statlig økonomiforvaltning.

Revisjonen er utført i samsvar med lov og instruks om Riksrevisjonen og internasjonale standarder for offentlig revisjon (ISSAI).

a-I Årsregnskapet, jf. revisjonsberetning (vedlegg 1)

Etter Riksrevisjonens mening gir Husbankens årsregnskap i det alt vesentlige et dekkende bilde av virksomhetens disponible bevilgninger og regnskapsopplysninger som er rapportert til statsregnskapet, den finansielle stillingen per 31.12.2014 og av resultater og kontantstrømmer for det avsluttede regnskapsåret i samsvar med regelverk for statlig økonomistyring, herunder anbefalte statlige regnskapsstandarder i Norge.

b-I Disponering av bevilgningene, jf. revisjonsberetning (vedlegg 1)

Basert på vår revisjon av årsregnskapet som beskrevet ovenfor, og kontrollhandlinger vi har funnet nødvendig i henhold til ISSAI-ene, er vi ikke kjent med forhold som tilsier at virksomhetens disponering av bevilgningene er i strid med de administrative bestemmelsene om økonomistyring.

b-II. Riksrevisjonen har revidert Husbankens lånesystem og har følgende vesentlige merknader, jf. etterlevelsrapport (vedlegg 2)

**Konklusjon:**

Husbanken er det viktigste statlige organ for gjennomføring av regjeringens boligpolitikk. Lån og tilskudd som håndteres i lånesystemet utgjør en vesentlig del av bankens virksomhet. Revisjonen viser

- at tilgangskontroller og logging i lånesystem og underliggende infrastruktur har vesentlige mangler og at Husbanken dermed ikke etterlever krav i personopplysningsloven og økonomiregelverket
- mangler i implementering i sikkerhetssystemet Natural Security, som benyttes i samspill med lånesystemet, gir ikke de begrensningene i tilganger til funksjoner som er forutsatt av Husbanken
- at enkelte lån ikke er utmålt i tråd med regelverket, og det indikerer at systemet ikke sikrer mot at det fattes uhjemlede vedtak.

For øvrig viste en begrenset stikkprøvekontroll av beregning av renter, avdrag og lån for grunnlån ingen vesentlige avvik. Revisjonen viste også at avstemming mellom låne- og regnskapssystem gjennomføres i henhold til kravene.

Riksrevisjonen anbefaler at Husbanken vurderer følgende tiltak:

- begrenser tilganger til bankens systemer til kun det som er nødvendig for å gjennomføre den enkeltes oppgaver
- anvender logger aktivt for å oppdage eventuelle sikkerhetshendelser
- vurderer hvilke tiltak som må gjennomføres for at tilgangskontrollene til lånesystemets funksjoner skal fungere etter sin hensikt
- søker å bygge inn kontroller i lånesystemet for å begrense mulige uhjemlede vedtak.

Etter fullmakt

  
for Hans Conrad Hansen  
ekspedisjonssjef

  
Einar Sæther  
avdelingsdirektør

**Kopi til:** KOMMUNAL- OG MODERNISERINGSDEPARTEMENTET

**Vedlegg 1:** Revisjonsberetning for Husbanken 2014

**Vedlegg 2:** Etterleversrapport om Husbankens lånesystem for 2014

**Vedlegg 3:** Liste over korrespondanse



HUSBANKEN  
Org. nr.: 942114184

## Riksrevisjonens beretning

### Uttalelse om årsregnskapet

Riksrevisjonen har revidert Husbankens årsregnskap for 2014. Årsregnskapet består av ledelseskomentarer, oppstilling av bevilgnings- og artskontorrapportering med noter per 31.12.14 og oppstilling av virksomhetsregnskap med noter per 31.12.14.

### Virksomhetsledelsens ansvar for årsregnskapet

Virksomhetens ledelse er ansvarlig for at årsregnskapet gir et dekkende bilde i samsvar med regelverk for statlig økonomistyring i Norge, herunder statlige regnskapsstandarder (SRS), og for slik intern kontroll som ledelsen finner nødvendig for å muliggjøre utarbeidelsen av et årsregnskap som ikke inneholder vesentlig feilinformasjon, verken som følge av misligheter eller feil.

### Riksrevisjonens oppgaver og plikter

Riksrevisjonens oppgave er å gi uttrykk for en mening om dette årsregnskapet, på bakgrunn av vår revisjon. Vi har gjennomført revisjonen i samsvar med *lov og instruks om Riksrevisjonen* og internasjonale standarder for offentlig revisjon (ISSAI). Disse standardene krever at vi etterlever etiske krav og planlegger og utfører revisjonen for å oppnå betryggende sikkerhet for at årsregnskapet som er utformet for å gi et dekkende bilde ikke inneholder vesentlig feilinformasjon.

En revisjon innebærer utførelse av handlinger for å innhente revisjonsbevis for beløpene og opplysningene i årsregnskapet. De valgte handlingene avhenger av revisors skjønn, herunder vurderingen av risikoene for at årsregnskapet inneholder vesentlig feilinformasjon, enten det skyldes misligheter eller feil. Ved en slik risikovurdering tar revisor hensyn til den interne kontrollen som er relevant for virksomhetens utarbeidelse av et regnskap som gir et dekkende bilde, med det formål å utforme revisjonshandlinger som er hensiktsmessige etter omstendighetene, men ikke for å gi uttrykk for en mening om effektiviteten av virksomhetens interne kontroll. En revisjon innebærer også en vurdering av hensiktsmessigheten av regnskapspolicyene som er brukt, og rimeligheten av regnskapsestimer som er utarbeidet av ledelsen, så vel som en vurdering av presentasjonen av årsregnskapet.

Etter Riksrevisjonens oppfatning er innhentede revisjonsbevis tilstrekkelig og hensiktsmessig som grunnlag for vår konklusjon.

### **Konklusjon**

Etter Riksrevisjonens mening gir Husbankens årsregnskap i det alt vesentlige et dekkende bilde av virksomhetens disponible bevilgninger og regnskapsopplysninger som er rapportert til statsregnskapet, den finansielle stillingen per 31.12.2014 og av resultater og kontantstrømmer for det avsluttede regnskapsåret i samsvar med regelverk for statlig økonomistyring, herunder anbefalte statlige regnskapsstandarder i Norge.

### **Uttalelse om øvrige forhold**

#### **Konklusjon knyttet til administrative bestemmelser om økonomistyring**

Basert på vår revisjon av årsregnskapet som beskrevet ovenfor, og kontrollhandlinger vi har funnet nødvendig i henhold til ISSAI-ene, er vi ikke kjent med forhold som tilsier at virksomhetens disponering av bevilgningene er i strid med de administrative bestemmelsene om økonomistyring.

Oslo; 29.05.2015

Etter fullmakt

  
Hans Conrad Hansen  
ekspedisjonssjef

  
Einar Sæther  
avdelingsdirektør



**Riksrevisjonen**

Vår referanse 2014/01186-44

Utsatt offentlighet jf. rrevl. § 18(2)  
Unntatt offentlighet jf. offl. § 13

HUSBANKEN  
Org. nr.: 942114184

# Etterlevelsesrapport om Husbankens lånesystem for 2014

**Mottaker: Husbanken**

**Revisjonen er gjennomført i samsvar med Riksrevisjonen lov og instruks og bygger på ISSAI 400 /4200, INTOSAI's internasjonale standarder for etterlevelsesrevisjon.**

## **Innhold**

<b>1. Innledning</b> .....	3
<b>2. Revisjonens mål og omfang</b> .....	3
<b>3. Revisjonskriterier</b> .....	5
<b>4. Metode</b> .....	8
<b>5. Funn</b> .....	10
<b>6. Konklusjon</b> .....	23
<b>7. Anbefaling</b> .....	25

## 1. Innledning

Husbanken er det viktigste statlige organ for gjennomføring av regjeringens boligpolitikk<sup>1</sup>. Banken skal supplere det ordinære kredittmarkedet og gi lån til formål som er samfunnsøkonomisk og fordelingspolitisk ønskelige. Husbanken gir lån til privatpersoner, kommuner og virksomheter. De viktigste låneordningene er grunnlån og startlån. Grunnlån skal bidra til miljøeffektivitet og universell utforming i ny og eksisterende bebyggelse, skaffe boliger til vanskeligstilte og sikre nødvendig boligforsyning. Startlån skal hjelpe vanskeligstilte på boligmarkedet. I tillegg gis kompensasjon for utgifter til renter til investering i skole- og svømmeanlegg og istandsetting av kirke og kirkeinventar. Enkelte av lånene gis i kombinasjon med tilskudd. Grunnlån er den økonomisk vesentligste av Husbankens låneordninger. For den enkelte mottaker, som ofte er vanskeligstilt, er det viktig at vilkårene innlagt i systemet er korrekte og rettferdige.

I 2014 er det utbetalt 17,5 mrd. kroner i lån fra Husbanken (kap 2412.90), og innkomet om lag 13,8 mrd. kroner i renter (kap 5615.80: 3,6 mrd. kroner) og avdrag (kap 5312.90: 10,2 mrd. kroner). Årlig utbetales 5 000-10 000 nye lån og tilskudd, under om lag 15 ulike låne- og tilskuddsordninger. Husbanken forvalter totalt 53 645 lån pr 31. desember 2014. På samme tidspunkt er utestående låneportefølje 135,6 mrd. kroner.

Hils/Vinnbin er hovedsystemet for kundeadministrasjon, saksbehandling og forvaltning av lån og tilskudd (eksklusiv Bostøtte) samt for kompensasjonsordningene i Husbanken. Lånesystemet er, ved siden av å være et støttesystem for saksbehandling og forvaltning av lån, et forsystem med vesentlige leveranser til Husbankens regnskapssystem.

I styringsreferat mellom Kommunal- og regionaldepartementet og Husbanken av 30. mai 2012 omtales at det er høy risiko for manglende måloppnåelse innenfor Husbankens ansvarsområde dersom modernisering av ikt-systemene ikke gjennomføres. Referatet viser til oversendt risiko- og sårbarhetsanalyse for ikt-modernisering i Husbanken (kalt SIKT). Fra SIKT fremkommer at "Flere av dagens løsninger bygger på gammel teknologi som det er vanskelig å oppdrive kompetanse på. Det vil heller ikke være mulig å gjennomføre større endringer på løsningene knyttet til lån og tilskudd med dagens plattform".

## 2. Revisjonens mål og omfang

Formålet med revisjonen er å vurdere om Husbanken har etablert en internkontroll i og i tilknytning til bankens lånesystem som forhindrer uautoriserte endringer av informasjon om lån og sikrer korrekt beregning, regnskapsføring, utbetaling av lån og innbetaling av renter og avdrag. Kontrollen av beregninger av lån, renter og avdrag er i denne revisjonen avgrenset til grunnlån.

### **Problemstillinger**

1. Utmåles grunnlån og fastsettes renter og avdrag i tråd med lov om Husbanken, forskrift om grunnlån fra Husbanken, lov om renter ved forsinket betaling m.m. og forskrift om rente- og avdragsvilkår for lån i Husbanken?

---

<sup>1</sup> Prop. 1 S KMD (2014-2015)

Underproblemstillinger;

### *1.1 Fastrente*

Er rentepåslaget ved inngåelse av fastrente i henhold til søknadstidspunkt jf. forskrift om rente- og avdragsvilkår for lån i Husbanken?

### *1.2 Avdragsfri periode*

Er fastsatt periode for avdragsfrihet i samsvar med forskrift om rente- og avdragsvilkår for lån i Husbanken?

### *1.3 Avdragstid*

Er fastsatt periode for lånets avdragstid i samsvar med forskrift om rente- og avdragsvilkår for lån i Husbanken?

### *1.4 Gebyrer*

Fastsettes gebyrene i tråd med forskrift om rente- og avdragsvilkår for lån i Husbanken, også der lånet splittes i en fast og en flytende del, eller i flere dellån?

### *1.5 Over/underkurs*

Blir over/underkurs beregnet i tråd med forskrift om rente- og avdragsvilkår for lån i Husbanken?

### *1.6 Forsinkelsesrente*

Blir forsinkelsesrente fastsatt i tråd med lov om renter ved forsinket betaling m.m.?

### *1.7 Låneutmåling*

Følger Husbanken grensene for låneutmåling når det innvilges grunnlån, jf. bestemmelsene i Husbankens retningslinjer (det følger av forskrift om grunnlån fra Husbanken at Husbanken kan gi retningslinjer)?

### *1.8 Arealgrenser*

Følger Husbanken arealgrensene når det innvilges grunnlån, jf. bestemmelsene i Husbankens retningslinjer (det følger av forskrift om grunnlån fra Husbanken at Husbanken kan gi retningslinjer)?

### *1.9 Tilleggssikkerhet*

Følger Husbanken kravene til tilleggssikkerhet for lån til andre enn personlige låntakere, jf. bestemmelsene i Husbankens retningslinjer (det følger av forskrift om grunnlån fra Husbanken at Husbanken kan gi retningslinjer)?

### *1.10 Betalingsutsettelse*

Benytter Husbanken virkemidlene for personer med betalingsproblemer i samsvar med forskrift om rente- og avdragsvilkår for lån i Husbanken?



2. Er informasjonssikkerhet ved forvaltningen av lån i samsvar med krav i personopplysningsloven og økonomiregelverket i staten?

Har Husbanken etablert tilgangskontroller/adgangskontroller og logging i samsvar med gjeldende regelverk:

- 2.1 i lånesystemet Hils/Vinnbin?
- 2.2 i sikkerhetssystemet Natural Security som begrenser tilgangen til lånesystemet?
- 2.3 i databasen Adabas hvor dataene til lånesystemet er lagret?
- 2.4 på serveren hvor programmene og databasen til lånesystemet ligger?
- 2.5 ved identitetsadministrasjon basert på katalogtjenesten Active Directory?
- 2.6 som en del av fysisk sikkerhet?

3. Er Husbankens internkontroll ved utbetaling av lån i samsvar med krav i økonomiregelverket i staten?

Sikrer Husbankens internkontroll:

- 3.1 arbeidsdeling ved vedtak om tilsagn, bevilgning og utbetaling av lån?
- 3.2 at det er samsvar mellom regnskapsført utbetaling/innbetaling av lån/rente/avdrag i Agresso og beregnet lån/rente/avdrag i lånesystemet?

### 3. Revisjonskriterier

1. Utmåles grunnlån og fastsettes renter og avdrag i tråd med lov om Husbanken, forskrift om grunnlån fra Husbanken, lov om renter ved forsinket betaling m.m. og forskrift om rente- og avdragsvilkår for lån i Husbanken?

Ved revisjonen er følgende regelverk lagt til grunn som revisjonskriterier;

I lov om Husbanken av 29. mai 2009 fremkommer det av § 1 at Husbanken blant annet skal forvalte låne- og tilskuddsordninger. Lovens § 8 sier at Husbanken skal forrente lån etter vedtak i Stortinget. I forskrift om grunnlån av 22. desember 2004 § 5 heter det at Husbanken kan gi nærmere retningslinjer om lån og låneutmåling. Husbanken har utarbeidet retningslinjer og veiledning for grunnlån. I forskrift om rente og avdragsvilkår for lån i Husbanken av 25. mai 2011 fremkommer bestemmelser knyttet til rentefastsettelse for Husbankens låneordninger og i Lov om renter ved forsinket betaling m.m. av 17. desember 1976 reguleres vilkår for forsinkelsesrente.

Årlige effektive renter før gebyrer, som danner grunnlag for faste og flytende renter, beregnes av FIN. Husbanken beregner nominelle renter, jf. forskrift om rente og avdragsvilkår for lån i Husbanken § 4, siste ledd.

Revisjonskriteriene er presisert i følgende underproblemstillinger;

#### 1.1 Fastrente

Etter forskrift om rente og avdragsvilkår for lån i Husbanken § 4 fremgår det at lånesøknader om fastrente innkommet fra 14. oktober 2013 til 8. november 2013 får 0,75 prosent rentepåslag fra 1. mars 2014. Fastrentelån inngått før 14. oktober 2013 får rentepåslag 0,5 prosent. Fra 1. mars 2014 er rentepåslaget 1 prosent.

### *1.2 Avdragsfri periode*

Forskrift om rente og avdragsvilkår for lån i Husbanken § 9c sier at lån kan gis med inntil 8 års avdragsfrihet. Av § 12 fremkommer at Husbanken kan fravike rente- og avdragsvilkårene på utbetalte lån i individuelle tilfeller. Ved midlertidige betalingsvansker kan Husbanken innvilge utsettelse med betaling av rente og avdrag.

### *1.3 Avdragstid*

Forskrift om rente og avdragsvilkår for lån i Husbanken § 9b sier at lån kan gis med 30 års avdragstid. Grunnlån til utleieboliger kan gis med inntil 50 års løpetid.

### *1.4 Gebyrer*

Forskrift om rente og avdragsvilkår for lån i Husbanken § 11 gir Husbanken fullmakt til å fastsette gebyr for å dekke andre omkostninger innenfor rammer som fastsettes av departementet. I henhold til ulovfestede forvaltningsrettslige prinsipper er det forbud mot usaklig forskjellsbehandling. Gebyrkostnader for den enkelte låntaker skal være forutberegnelig.

### *1.5 Over/underkurs*

Etter forskrift om rente og avdragsvilkår for lån i Husbanken § 8 skal det ved førtidig tilbakebetaling av lån med fast rente og ved overgang fra fast til flytende rente i bindingsperioden, beregnes over- eller underkurs, jf. forskrift om kredittavtaler mv. § 9. Det tas utgangspunkt i årlige effektive renter avrundet til én desimal før gebyrer, som er beregnet av Finansdepartementet og publisert på Husbankens nettsider. Den årlige effektive renten før gebyrer vil fremgå av kundens låneavtale.

### *1.6 Forsinkelsesrente*

I forskrift om rente og avdragsvilkår for lån i Husbanken § 2, 3 ledd fremkommer det at ved betalingsmislighold gjelder lov av 17. desember 1976 nr. 100 om renter ved forsinket betaling m.m. (forsinkelsesrenteloven). I lovens § 3 omhandles størrelsen på forsinkelsesrenten.

### *1.7 Låneutmåling*

Av lov om Husbanken § 8 fremkommer at Husbanken kan gi lån. Av forskrift om grunnlån § 5 fremkommer at Husbanken kan gi nærmere retningslinjer. Ifølge Husbankens retningslinjer for grunnlån punkt 9d kan grunnlån normalt utgjøre inntil 80 prosent av de prosjektkostnader Husbanken godkjenner. Ifølge Husbankens retningslinjer for grunnlån punkt 9b kan ikke fellesgjelden ved grunnlån til borettslag utgjøre mer enn 75 prosent av kostnadsoverslaget i bygge- og finansieringsplanen.

### *1.8 Arealgrenser*

Av lov om Husbanken § 8 fremkommer at Husbanken kan gi lån. Av forskrift om grunnlån § 5 fremkommer at Husbanken kan gi nærmere retningslinjer. Ifølge Husbankens retningslinjer for grunnlån punkt 8 fremkommer arealgrenser for låneutmåling i 2014.

### 1.9 Tilleggssikkerhet

Av lov om Husbanken § 8 fremkommer at Husbanken kan gi lån. Av forskrift om grunnlån § 5 fremkommer at Husbanken kan gi nærmere retningslinjer. Ifølge Husbankens retningslinjer for grunnlån punkt 6 kan Husbanken kreve tilleggssikkerhet for lån til andre enn personlige låntakere.

### 1.10 Betalingsutsettelse

I forskrift om rente og avdragsvilkår for lån i Husbanken, § 12, 1.ledd 2. setning står det at Husbanken kan innvilge utsettelse med betaling av rente og avdrag. Avdrag kan legges til lånet. Husbankens praksis må være forutberegnelig og enhetlig, jf. kravene til god forvaltningsskikk.

## 2. Er informasjonssikkerhet ved forvaltningen av lån i samsvar med krav i personopplysningsloven og økonomiregelverket i staten?

I lånesystemet Hils/Vinnbin behandles personopplysninger, f.eks. fødselsnummer og informasjon om den enkeltes økonomiske situasjon og boforhold. Bestemmelser i medhold av personopplysningsloven er dermed anvendt som revisjonskriterier. Samtidig er Hils/Vinnbin et viktig grunnlag for økonomiske disposisjoner i Husbanken og et grunnlag for virksomhetens regnskap. Systemet er derfor også vurdert opp mot Økonomiregelverket i Staten (økonomiregelverket), jf. Bestemmelser om økonomistyring i staten (bestemmelsene) punkt 4.3.1 hvor det legges til grunn at et økonomisystem inkluderer blant annet hjelpesystem som produserer eller påvirker innholdet i bokførte transaksjoner.

I personopplysningsloven § 13 settes krav om at den som behandler personopplysninger gjennom planlagte og systematiske tiltak skal sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet. Lovkravet er spesifisert i forskrift til loven. I økonomiregelverket § 14 fastslås at alle virksomheter skal etablere rutiner og systemer som har innebygd internkontroll, som er spesifisert i bestemmelsene.

### Tilgangs- og adgangskontroller

Det skal treffes tiltak mot uautorisert endring av personopplysninger der integritet er nødvendig i følge personopplysningsforskriften § 2-13. Det er i forskriften § 2-14 understreket at sikkerhetstiltak skal etableres med formål å hindre sikkerhetsbrudd. I personopplysningsforskriften § 2-10 settes det krav til tiltak som sikrer mot uautorisert fysisk adgang til utstyr som brukes for å behandle personopplysninger.

Ifølge bestemmelsene punkt 4.3.6 skal økonomisystemet ha et sikkerhetsnivå som er tilpasset virksomhetens aktiviteter, hvor det er tatt hensyn til risiko og vesentlighet. Tilgangskontroller skal sikre systemets funksjoner og data mot uautorisert endring (dataintegritet). Alle brukere skal ha en personlig identifikasjon og det skal kunne tildeles tilgangsrettigheter tilpasset brukernes oppgaver.

### Logging

Sikkerhetstiltak skal gjøre det mulig å oppdage uautorisert bruk av informasjonssystemet og forsøk på slik bruk, jf. personopplysningsforskriften § 2-14. Her er videre presisert at forsøk på uautorisert bruk av informasjonssystemet skal registreres.

Bestemmelsene punkt 4.3.6 setter også krav til logging. Økonomisystemet skal ha funksjonalitet for logging av alle vesentlige funksjoner. Det skal etableres sikre

prosedyrer, herunder logging, knyttet til eventuelle endringer av lagrede data utenom applikasjonens normale funksjoner.

### 3. Er Husbankens internkontroll ved utbetaling av lån i samsvar med krav i økonomiregelverket i staten?

I økonomireglementet § 14 fastslås at alle virksomheter skal etablere rutiner og systemer som har innebygd internkontroll, som er spesifisert i bestemmelsene. Av bestemmelsene punkt 2.4 *Internkontroll* fremkommer at virksomhetens ledelse har ansvar for å påse at internkontrollen er tilpasset risiko og vesentlighet, at den fungerer på en tilfredsstillende måte og at den kan dokumenteres.

#### 3.1 *Arbeidsdeling ved vedtak om tilsagn, bevilgning og utbetaling av lån?*

For å kunne utøve nødvendig internkontroll skal det være rutiner og systemer med blant annet forsvarlig arbeidsdeling, jf. bestemmelsene punkt 2.4, tredje avsnitt bokstav c. Av bestemmelsene punkt 2.5.2.1 *Budsjett disponeringsmyndighet* og punkt 2.5.2.2 *Attestasjon* fremgår at utbetalingene skal bekreftes/attesteres før utbetaling finner sted.

#### 3.2 *Samsvar mellom regnskapsført utbetaling/innbetaling av lån/rente/avdrag i Agresso og beregnet lån/rente/avdrag i lånesystemet?*

Det framgår av bestemmelsene punkt 4.3.2 *Funksjonalitet for bokføring og registrering*, at når økonomisystemet består av flere moduler skal systemet sikre korrekt overføring mellom modulene, jf. punktets tredje avsnitt.

## 4. Metode

Vi har lagt følgende metode til grunn for de nummererte problemstillingene og revisjonskriterier overfor:

1. Utmåles grunnlån og fastsettes renter og avdrag i tråd med lov om Husbanken, forskrift om grunnlån fra Husbanken, lov om renter ved forsinket betaling m.m. og forskrift om rente- og avdragsvilkår for lån i Husbanken?

Revisjonen startet opp med et møte med Husbanken for å oppnå forståelse av lånesystemet. I dialog med Husbanken har vi forsøkt å bestille relevante data som grunnlag for analyse og kontroll, for deretter å avklare tolkning av innhentede data og i enkelte tilfeller gjennomføre oppslag i lånesystemet i arbeidsmøter med Husbanken. Det er i tillegg sendt enkelte avklaringer og spørsmål til Husbanken, som er besvart i brev.

Vi har mottatt data knyttet til totalt 13 345 løpende grunnlån fra innføring av grunnlån i 2004 og avgrenset til 31. oktober 2014. Dataene har vi analysert for ekstremverdier og for å kunne svare på hver enkelt av underproblemstillingene. Hvert enkelt utvalg som er testet er avhengig både av forekomst innenfor den enkelte underproblemstilling, og avgrenses i noen tilfeller av når gjeldende regel ble innført.

Vi har blant annet innhentet historiske fastrenter og forsinkelsesrenter og vurdert opp mot søknadstidspunkt, for å avgjøre om fastrentesats er i samsvar med grunnlaget som

er benyttet for fastrentelån og forsinkelsesrente ilagt. Vi har etterregnet rente og avdrag for enkelte lån vurdert opp mot vilkårene for lånene gitt fra Husbankens lånesystem, for å se om vi kommer frem til samme terminbeløp som Husbanken.

## 2. Er informasjonssikkerhet ved forvaltningen av lån i samsvar med krav i personopplysningsloven og økonomiregelverket i staten?

For å besvare problemstillingen er det foretatt kontroller av tilgangskontroller/adgangskontroller og logging på flere nivåer:

1. i lånesystemet Hils/Vinnbin
2. i sikkerhetssystemet Natural Security som begrenser tilganger i lånesystemet
3. i databasen Adabas hvor dataene til lånesystemet er lagret
4. på serveren hvor programmene og databasen til lånesystemet ligger
5. ved identitetsadministrasjon ved hjelp av katalogtjenesten Active Directory
6. fysisk sikkerhet, med spesiell vekt på sikring av adgang til rom der server til lånesystemet Hils/Vinnbin er plassert

Revisjonen har vært basert på å møte Husbanken for å oppnå forståelse av systemet, hente ut relevante data som grunnlag for analyse og kontroll, for deretter å diskutere tolkning av innhentede data med Husbanken der det er nødvendig.

Det er innhentet data om oppsett, tilganger og logging av systemet på alle nivåer nevnt innledningsvis. Innhentede data inkluderer:

- retningslinjer for sikkerhet og relevante risikovurderinger
- oversikt over hvem som har tilgang til serverrommet der server for lånesystemet er plassert, samt logg for tilgang til rommet for den nærmest foregående perioden
- et uttrekk av alle attributter fra katalogtjenesten Active Directory som i Husbanken bl.a. benyttes til å administrere brukeridenter og autentisere brukere ved innlogging
- uttrekk av passordoppsett og brukeridenter fra operativsystemet på server for lånesystemet
- oppsett av logger fra Active Directory og fra operativsystemet på serveren
- eksempler på logger fra Active Directory og fra operativsystemet på serveren
- filer som viser samspillet mellom Active Directory og serveren når brukere logger seg på lånesystemet
- skjermbildeutskrift som viser hvilke brukeridenter som er medlem av de enkelte grupper i Natural Security
- skjermbildeutskrift fra Natural Security som viser hvilke funksjoner/menypunkter de enkelte grupper av brukeridenter ikke har tilgang til i lånesystemet
- regneark som viser funksjoner/menypunkter i lånesystemet
- rapport som viser verdiene i saksbehandlerregisteret i lånesystemet, som styrer hvem som har tilgang til å innstille og fatte vedtak om tilsagn lån, innstille og vedta bevilgning lån, samt innstille og vedta utbetaling lån

De innhentede dataene er analysert ved at det er trukket ut viktige parametere som er vurdert i forhold til kriteriene. Videre er det foretatt sammenstillinger mellom de ulike dataene nevnt over.

Fysisk sikkerhet er vurdert ved å observere implementerte sikkerhetstiltak ved revisjonsbesøk i enhetene i Drammen og Bodø.

### 3. Er Husbankens internkontroll ved utbetaling av lån i samsvar med krav i økonomiregelverket i staten?

Vi har innhentet beskrivelser av hvordan arbeidsdeling er implementert i Husbankens rutiner og i lånesystemet. Arbeidsdeling som fremgår ut fra rutinene er sett i sammenheng med tilgangsrettigheter i lånesystemet ut fra innhentede data, jf. omtale under metode for problemstilling 2.

Under revisjonsbesøk ved Husbankens regnskapsenhet, som er lokalisert ved Husbankens Regionkontor Bodø, har vi vurdert internkontrollen knyttet til overføring mellom forsystemet Hils/Vinnbin til regnskapssystemet Agresso for lån og tilskudd (eksklusiv Bostøtte). Deretter har vi kontrollert om internkontrollen knyttet til utbetaling av tilskudd (eksklusiv Bostøtte), som har parallell prosedyre som ved utbetaling av lån, samsvarer med arbeidsdelingen skissert av Husbanken for vedtak av tilsagn, vedtak av bevilgning og vedtak av utbetaling.

Vi valgte pr utgangen av oktober 25 tilfeldige utbetalingsdatoer for tilskudd. For de utvalgte datoene kontrollerte vi til sammen 35 utbetalte tilskudd i Hils/Vinnbin. For de 35 tilskuddene vi kontrollerte, ble blant annet rutinen for vedtak av tilsagn, vedtak av bevilgning og vedtak av utbetaling vurdert i form av attestasjonskontroll og kontroll av gjennomført budsjett disponeringsutførelse.

For de samme 25 tilfeldig valgte datoene for utbetalte tilskudd, kontrollerte vi overføringen fra Hils/Vinnbin til Agresso for både lån og tilskudd.

I tillegg er to månedssavstemminger mellom Hils/Vinnbin og Agresso kontrollert.

## 5. Funn

Revisjonen gir følgende funn for de nummererte problemstillingene, revisjonskriterier og metoder overfor:

1. Utmåles grunnlån og fastsettes renter og avdrag i tråd med lov om Husbanken, forskrift om grunnlån fra Husbanken, lov om renter ved forsinket betaling m.m. og forskrift om rente- og avdragsvilkår for lån i Husbanken?

Vi har kontrollert beregning av renter og avdrag for to lån som ikke har betalingsavvik, med både fast og flytende rente, og kommet frem til samme rente og avdrag som Husbanken har beregnet. Vi har etterberegnet terminbeløp for 4 låntakere med betalingsavvik, og ikke funnet vesentlig avvik i forhold til Husbankens fastsatte terminbeløp.

### 1.1 Fastrente

Fra Husbankens analyse av lånevirkksomheten pr 30.06.2014 finner vi at fastrenteavtaler i porteføljen (målt i kroner) over tid har holdt seg på et nivå på rundt 60 prosent. For grunnlån er det løpende 4 582 fastrenteavtaler for utvalgsperioden 2004 fram til 31. oktober 2014.

Kontrollen er gjennomført ved å koble historiske fastrenter mot tidspunkt for oppstart av fastrentelån. For enkelte lån viste det seg at låntaker hadde mottatt tilbud om fastrente for signering på et tidligere tidspunkt enn tidspunkt for når løpetid for fastrenten startet. Ved oppslag i Husbankens lånesystem på to lån har vi sett at fastrente styres av tilbudt fastrente fra Husbanken, og at denne gjelder uavhengig av

om fastrenten fram til igangsettelse av fastrente er økt/reduisert i forhold til oversendt tilbud. Vi har ikke funnet avvik på fastsatt fastrente, vurdert opp mot historisk fastrente og tilbud om fastrenteavtale.

Tilsvarende har vi kontrollert for varierende påslag på fastrente fra 1. mars 2014, som følger av tidspunkt for inngåelse av fastrente, jf. forskrift om rente og avdrag vilkår for lån i Husbanken, § 4. I vårt utvalg gjelder dette 61 forekomster som har fått rente fra perioden mellom 14. oktober 2013 og 1. mars 2014. Husbanken har innvilget fastrente og påslag etter vilkår som fremgikk av tilbudet til låntaker. Vi har gjennomført oppslag i Husbankens lånesystem på to lån, og ikke funnet avvik på fastsatt påslag på fastrente inngått i omtalte periode, når vi tar hensyn til tidspunkt for tilbudt fastrente.

### 1.2 Avdragsfri periode

Av 13 345 grunnlån, har 5 lån blitt innvilget negativ avdragsfrihet på inntil ett år. Dette skyldes feilregistreringer ifølge Husbanken. Revisjonen viser at dette ikke gir økonomiske konsekvenser. 24 lån har fått innvilget mer enn 8 års avdragsfrihet, hvorav et lån er innvilget 10 års avdragsfrihet, og ett annet lån 11 års avdragsfrihet. Oppslag i lånesystemet viste at det var gjort særskilte vurderinger i disse tilfellene. Husbanken kan etter bestemmelsene i Lov om Husbanken § 8 gi utsettelse på betaling av renter og avdrag.

### 1.3 Avdragstid

Det fremkommer av forskrift om rente og avdragsvilkår for lån i Husbanken § 9b at lån, med unntak av grunnlån til utleieboliger, ikke kan gis med lenger enn 30 års avdragstid. Av utvalget på 13 345 lån var det 8 som hadde 50 års avdragstid og ikke gjaldt utleieboliger. Alle lånene var knyttet opp mot en opprinnelig felles søknad fra en samlet foreldregruppe for funksjonshemmede barn. De framtidige beboerne (unntatt én under 18 år) mottok stønader som *unge uføre*.

Byggeprosessen var ifølge Husbanken halvveis fullført da Husbanken ble oppmerksom på at de framtidige beboerne ville få vanskeligheter med å betjene det framtidige grunnlånet med en nedbetalingstid på 30 år, fordi påregnet momsrefusjon ikke ble gitt.

For å unngå fremtidig mislighold og bidra til at låntakerne kunne få bo i de spesialtilpassede boligene ønsket Husbanken på et tidlig tidspunkt å finne en løsning. Det ble vurdert som mest formålstjenlig å utvide nedbetalingstiden til 50 år. Intern retningslinje HB 5 D. 31 (6.2006) omtaler virkemidler ved betalingsproblemer. Ifølge punkt 8.1 i retningslinjen kan Husbanken gå utover grensen på 30 års avdragstid der det er vanskelig å finne andre løsninger på et betalingsproblem. Husbanken viser til at retningslinjen også kan benyttes ved forventet mislighold.

### 1.4 Gebyrer

I henhold til lånevilkår på Husbankens websider er dette kr 600 for etablering, kr 30 for termin, kr 50 for andre varsel, samt kr 150 for tredje varsel. Etableringsgebyr fastsettes på kun ett dellån, selv om låntaker har flere dellån. Dette gjelder f. eks dersom lånet er delt i to lån der et lån løper med fast rente og et lån løper med flytende rente. Låntaker belastes ett termingebyr, ved flere dellån. Purregebyr belastes på neste mulige termin. Vi har kontrollert 6 låntakere for riktig gebyrfastsettelse, og ikke oppdaget avvik i forhold til Husbankens retningslinjer for gebyrfastsettelse.

### 1.5 Over/underkurs

Informasjon om rentene publiseres på Husbankens webside, og fremkommer også mer utfyllende i Åpenhetsbrev - Husbanken, fastsatt av FIN 23. juni 2010, hvor det fremkommer at kvalitetssikrede renteobservasjoner skal legges ut på Husbankens

internettside. Med utgangspunkt i renteobservasjonene beregnes en årlig effektiv rente og aktuelle nominelle renter etter betalingsfrekvens. Dette gir mulighet for at hver enkelt låntaker selv kan kontrollere at renten som betales er i tråd med forutsetningene. For 2014 er det 94 lån som har brutt fastrenteavtalen og fått beregnet over/underkurs (brudd gjennomført fra 1. februar 2014 til 1. januar 2015).

Husbanken benytter i beregningen *ny rente*, et veid gjennomsnitt av rentesatsene for avtaler som er kortere og lengre enn gjenstående løpetid. Vi har lagt Husbankens beregnet *ny rente* til grunn i vår beregning av over/underkurs for 7 lån. Vi har ikke funnet vesentlig avvik i forhold til Husbankens beregnede over/underkurs for de 7 kontrollerte lånene.

### 1.6 Forsinkelsesrente

Vi har kontrollert ilagt forsinkelsesrente mot historisk forsinkelsesrente for alle Grunnlån som har blitt tillagt forsinkelsesrente i perioden 2013 og fram til 31. oktober 2014. I perioden har 1 009 unike lånummer blitt tillagt forsinkelsesrente, totalt 14 843 terminer er tillagt forsinkelsesrente innenfor perioden. Utvalget inkluderer også ett lån som var ilagt forsinkelsesrente i 2012. Forsinkelsesrente for det ene lånet med forsinkelsesrente i 2012 og lånene med beregnet forsinkelsesrente i første halvår 2013 er ilagt forsinkelsesrente i samsvar med historisk forsinkelsesrente. Det samme gjelder forsinkelsesrente ilagt fra 1. desember 2013 og fram til 1. november 2014. Lånene som er belastet forsinkelsesrente fra 1. juli 2013 og fram til 1. desember 2013 har fått tillagt forsinkelsesrente som er ett prosentpoeng lavere enn vedtatt forsinkelsesrente (8,5 prosent fremfor 9,5 prosent). Dette skyldes at Husbanken ikke fanget opp at påslaget på Norges Bank sin styringsrente ble økt fra 1. juli 2013, fra 7 til 8 prosent, jf. endring i lov om renter ved forsinket betaling. Husbanken har ikke sendt justerte krav til låntakerne som ble ilagt lavere forsinkelsesrente, til sammen 429 forekomster. Totalt ilagt for lav forsinkelsesrente vurderes uvesentlig.

### 1.7 Låneutmåling

Ved oppføring av utleieboliger vil grunnlån normalt utgjøre inntil 80 prosent i forhold til prosjektkostnader. Vi har undersøkt 10 forekomster som har 100 prosent låneutmåling i forhold til prosjektkostnader, dels gjennomført som oppslag i lånesystemet ved besøk hos Husbanken, dels har Husbanken sendt skriftlig redegjørelse. For 6 av lånene var dokumentasjonen fjernarkivert, og ifølge Husbanken har arkivleverandør kvittert for mottak, men finner ikke igjen 2 av sakene. For disse to tilfellene har Husbanken lagt informasjon i Hils/Vinnbin til grunn. Av de 10 kontrollerte er 6 av sakene tilfredsstillende redegjort for av Husbanken.

Et lån dreier seg om utleie av studentboliger, der egne retningslinjer for tilskudd til studentboliger fra Husbanken punkt 6.3 kommer til anvendelse, dvs. prosjekter som har fått tilskudd kan fullfinansieres med grunnlån i Husbanken under forutsetning av at kvalitetskravene i retningslinjene for Grunnlån punkt 7 er oppfylt. Lånet er vedtatt fullfinansiert av regionstyret (Region øst). Det påregnes i vedtaket fra regionstyret at det endelige forholdet mellom lån og tilskudd vil bli ca. 60 prosent dersom Kunnskapsdepartementet (KD) bevilger tilskudd til studentboligene. KD avslo senere søknaden om tilskudd grunnet høye kostnader.

De øvrige lånene dreier seg om kommunal utleiebolig, der tildelt boligtilskudd gir rett til fullfinansiering. For ett lån svarer Husbanken at ifølge deres tilsagnsbrev om tilskudd til utleieboliger forutsettes det at det inngås avtale mellom eier og kommune om bruk av boligene, og kommunal tildelingsrett i minst 20 år. Det skal også tinglyses en heftelse på eiendommen vedrørende bruk og kommunal tildelingsrett, og heftelsen skal ikke kunne slettes uten kommunens og Husbankens samtykke. I følge Husbanken redegjør kommunen for Husbankens forutsetninger i brev til låntaker, før lånets igangsettelse.



Ved Husbankens attestasjonskontroll knyttet til utbetaling er dokumentasjon på tinglyst servitutt ikke etterlyst, og det foreligger per i dag ingen tinglyste servitutter.

For det andre lånet svarer Husbanken at det ikke framgår av Husbankens tilsagn om boligtilskudd til utleie, og heller ikke av lånetilsagnet for grunnlån, at det skal inngås avtale mellom kommunen og eier og at det skal tinglyses en servitutt vedrørende bruk og tildelingsrett. Det foreligger ingen tinglyst servitutt på eiendommen/seksjonene.

For det tredje lånet skriver Husbanken at de antar det er foretatt en feilregistrering og at hvis dette er tilfelle, så utgjør finansieringen 94 prosent.

Ifølge retningslinjer for grunnlån punkt 9b skal fellesgjeld utgjøre mindre enn 75 prosent av kostnadsoverslaget i bygge- og finansierungsplanen ved utbetaling av grunnlån. Denne begrensningen ble iverksatt fra 1. januar 2014. To lån har fått tilsagn i 2014 og av disse har ett lån fått låneutmåling på 78 prosent, som er over fastsatt grense på 75 prosent.

### 1.8 Arealgrenser

Utvalget på 13 345 grunnlån er sortert på ekstremverdier. 3 boliger er registrert med areal 1-4 kvadratmeter. Husbanken svarer at de 3 prosjektene som er registrert med 1-4 kvadratmeter er feilregistreringer som ikke er fanget opp i saksbehandlingsprosessen. Revisjonen viser at feilregistreringene ikke gir økonomiske konsekvenser. Feilregistreringene påvirker imidlertid boligstatistikken i form av høyere kvadratmeterpris.

Krav til maksimumsareal er avhengig av boligtype og ble innført fra og med 2014, jf. retningslinjer for grunnlån punkt 8. Når reglene for maksimumsareal ble fastsatt i februar 2014 var det ikke gitt nærmere omtale av arealregler for grunnlån til kjøp/utbedring eller overgangsordninger/unntaksbestemmelser. Sommeren 2014 ble det avklart at for nybygg er arealgrensene absolutte, mens for grunnlån til kjøp og utbedring er arealgrensene veiledende. Samtidig fastslo Husbanken i retningslinjene at lånesøknader som hovedregel skulle avgjøres etter de regler som gjaldt når søknaden behandles, uavhengig av når søknaden kom inn til Husbanken. Imidlertid åpnes det for unntak dersom det vil virke urimelig å avgjøre en søknad etter retningslinjer som ble fastsatt etter at søknaden ble mottatt i Husbanken, såfremt dette ikke strider mot forskrift om grunnlån eller instruks fra departementet. I retningslinjene fremgår det også at Husbanken i særskilte tilfeller kan fravike retningslinjene i forbindelse med pilot- eller forbildeprosjekter som vurderes som særlig viktig å få gjennomført.

6 personkunder er gitt tilsagn i 2014 for boliger større enn maksimumsarealet på 150 kvadratmeter. Husbanken har begrunnet disse tilfellene slik:

- Et tilsagn er gitt fordi det lå i et distrikt hvor det er vanskelig å få finansiering i private banker. Boliger i distriktene var ett av de høyest prioriterte formålene for grunnlån i 2014. Lav kjøpesum medførte at Husbanken ikke vurderte boligens areal som en relevant avslagsgrunn.
- Et tilsagn er gitt for å trygge en uholdbar midlertidig bosituasjon for en person med nedsatt funksjonsevne. I samarbeid med boligkonsulenten i kommunen valgte Husbanken, ut fra en helhetsvurdering, å gjøre unntak fra retningslinjene for grunnlån og startlån og innvilget 80 prosent grunnlån til kjøp og utbedring. Maksimumsgrense for areal ble ikke vurdert som relevant avslagsgrunn, fordi grensene er veiledende for grunnlån til kjøp og utbedring.
- Et tilsagn er gitt til et utbedringsprosjekt hvor arealreglene ikke er absolutte. Tilsagn begrunnes også ut fra at eneboligen er et typisk kataloghus fra 80-tallet og de valgte løsningene har stor overføringsverdi til andre eneboliger som skal oppgraderes.

- Et tilsagn ble gitt fordi Husbanken vurderte kjøp og utbedring som ett billigere alternativ i forhold til en eventuell nyetablering i distriktet, og at saksgangen hadde startet i 2013. Boligetablering i distriktene var i 2014 et prioritert satsningsområde for grunnlån.
- Et tilsagn ble gitt fordi det tidligere var gitt tilsagn til et identisk hus fra samme utbygger hvor søknaden ble mottatt like før reglene om maksimumsgrense for areal hadde trådt i kraft. Husbanken fant det ikke rimelig overfor søker (utbygger) at en tilfeldighet skulle medføre to helt ulike utfall i to saker som i praksis var helt like. Det ble valgt å følge god forvaltningskikk og også innvilge lån til sist ankomne søknad.
- Et tilsagn ble gitt i 2013, men medførte ved en feil fra Husbankens side at det ble utbetalt for lavt beløp. Nytt tilsagn på gjenværende beløp måtte innvilges, og ble følgelig ikke vurdert i henhold til arealgrensene.

#### Om regelverket – arealbestemmelser og overgangs- og unntaksbestemmelser:

Husbanken innførte arealregler i forbindelse med revisjon av retningslinjer og veileder i 2014. Disse ble offentliggjort på Husbankens webside 5. februar 2014.

Arealreglene var rettet mot nybyggprosjekter. Retningslinjer og veileder (02.2014) inneholdt ikke nærmere omtale av arealregler for grunnlån til kjøp/utbedring eller overgangsordninger/unntaksbestemmelser. Det ble derfor behov for å nyansere arealreglene til kjøps- og utbedringsprosjekter. I tillegg var det nødvendig å unnta prosjekter som hadde vært i prosess med Husbanken før arealreglene ble innført. I februar ble det blant annet besluttet at arealreglene for kjøps- og utbedringslån skulle være veiledende.

Retningslinjer og veileder ble derfor revidert sommeren 2014 hvor følgende ble tatt inn i pkt 8. *Vurdering av areal og kostnader:*

*«For nybygg er arealgrensene absolutte. For grunnlån til kjøp og grunnlån til utbedring er arealgrensene veiledende».*

På samme tidspunkt ble retningslinjene og veilederen for grunnlån supplert med et nytt pkt 12. *Overgangs- og unntaksbestemmelser:*

*«Lånesøknader avgjøres som hovedregel etter de regler som gjelder når søknaden avgjøres, uavhengig av når søknaden kom inn til Husbanken. Dersom det vil virke urimelig å avgjøre en søknad etter retningslinjer som ble fastsatt etter at søknaden ble mottatt i Husbanken, kan det gjøres unntak fra de nye kravene. Dette kan blant annet gjelde prosjekter som over lang tid er planlagt i samarbeid med Husbanken etter tidligere retningslinjer. Forannevnte gjelder ikke dersom det strider mot forskrift om grunnlån eller instruks fra departementet.*

*Husbanken kan i særskilte tilfeller fravike retningslinjene dersom det ikke strider mot forskrift om grunnlån eller instruks fra departementet. Som særskilt tilfelle kan anses pilot- eller forbildeprosjekter som Husbanken vurderer som særlig viktig å få gjennomført.»*

#### **1.9 Tilleggssikkerhet**

Ifølge Husbankens retningslinjer for grunnlån punkt 6 kan Husbanken kreve tilleggssikkerhet for lån til andre enn personlige låntakere. Vi har valgt ut de 4 høyeste lånebeløpene til låntakere som er registrert med organisasjonsnummer. Av disse har tre ikke garanti, og 1 lån har et garantibeløp som ikke står i forhold til lånesum. Vi har i møte med Husbanken gjennomført oppslag i lånesystemet. Ett lån er gitt til studentboliger i Oslo og to til kommunale utleieboliger i Oslo med 20 års kommunal tildelingsrett. Husbanken krever ikke tilleggssikkerhet for studentboliger eller kommunale utleieboliger med kommunal tildelingsrett, da risikoen vurderes av

Husbanken som lav. Låntakeren med uvesentlig garantibeløp, viser seg å være til privat utbygger. Husbanken har i brev av 19. mars vist til at garantibeløpet er feilregistrert i Hils (garantibeløp er registrert med kr 156 926,- og skal være 156 926 000,-).

### 1.10 Betalingsutsettelse

Vi har fått oversendt filer med lånekunder som er innvilget utsettelse på terminbeløp i 2014. Ved oppslag av enkelte av disse lånenummerne hos Husbanken ser vi at det er enkelte kunder som har inngått mange betalingsavtaler. Filen med betalingsutsettelse på terminbeløp viser at i overkant av 700 låntakere har innvilget til sammen om lag 2 200 betalingsutsettelse for 2014. For 2014 viser Husbanken til at kun ett lånenr har fått innvilget tilleggs lån etter individuell vurdering.

## 2. Er informasjonssikkerhet ved forvaltningen av lån i samsvar med krav i personopplysningsloven og økonomiregelverket i staten?

### Beskrivelse av Husbankens ikt-miljø for forvaltning av lån

Lånesystemet Hils/Vinnbin består av lånesaksbehandlingssystemet Hils fram til utbetaling. Ved utbetaling overføres de fleste metadata knyttet til lån og tilskudd over til Vinnbin, som defineres som reskontrosystemet (eller terminregisteret). Hils/Vinnbin betraktes imidlertid av Husbanken som ett system.

Lånesystemet ble opprinnelig utviklet for og kjørt på en stormaskinløsning, men ble konvertert til operativsystemet Linux i 2006. Lånesystemet og tilknyttet database ligger nå begge på samme server. Autentisering av brukere til denne serveren skjer ved en integrasjon mot katalogtjenesten Active Directory, som er en del av bankens Windows-miljø. Brukeren behøver ikke oppgi brukerid og passord på nytt ved pålogging til lånesystemet. Autentiseringen ved påloggingen på serveren legges til grunn også her.

En bruker må være registrert i sikkerhetssystemet Natural Security for å få tilgang til Hils/Vinnbin. Natural Security gir i utgangspunktet brukeren tilgang til alle funksjoner/menypunkter, men Husbanken har innskrenket dette ved å definere funksjoner/menypunkter som ulike grupper av brukere ikke har tilgang til.

Tilgangsstrukturen i Hils/Vinnbin baserer seg videre på et saksbehandlerregister. Her defineres det om brukeren kun har lesetilgang, kan saksbehandle/innstille, gjøre vedtak eller utbetale lån.

Oppsummert må en bruker dermed ha følgende tilganger for å kunne benytte Hils/Vinnbin:

- ha en aktiv brukerident og være lagt inn i gruppe for tilgang til Linux i Active Directory
- være registrert som bruker i Natural Security
- være registrert i saksbehandlerregisteret i Hils/Vinnbin.

### 2.1 Lånesystemet Hils/Vinnbin

#### Tilgangskontroller

Saksbehandlerregisteret i lånesystemet angir hvilke brukere som har tilgang til:

- å se informasjon om lån
- saksbehandle og innstille til vedtak om lån
- å fatte vedtak om lån
- vedta utbetaling av lån

Det må dessuten oppgis et eget passord for å vedta utbetaling av et lån.

Revisjonen viser flere svakheter knyttet til administrasjon av saksbehandlerregisteret:

- Passord som brukes for å vedta utbetaling av lån må legges inn i selve programkoden. Dette gir risiko at flere enn brukeren kan få kjennskap til passordet og vanskeliggjør en sikker passordadministrasjon.
- Analyse av logger fra server for lånesystemet viser at 28 prosent av de personlige brukeridentene i saksbehandlerregisteret ikke hadde vært logget inn mot lånesystemet i perioden 1. oktober 2014 til 12. februar 2015. Det indikerer at mange brukere i registeret ikke har behov for tilgangen.
- Analyse av data fra saksbehandlerregisteret viser at det er flere ansatte i administrative seksjoner som har rettigheter til å saksbehandle eller vedta tilsagn om lån, som antas ikke å være en del av deres arbeidsoppgaver. Svar ved revisjonsbesøk indikerer at dette skyldes mangelfull oppdatering av saksbehandlerregisteret ved endring i arbeidsoppgaver.
- Når en person avslutter sitt arbeidsforhold i Husbanken skal det legges inn en sluttdato i saksbehandlerregisteret. 48 brukeridenter fikk registrert sluttdato 21. eller 22. januar 2015. Dette viser at banken ikke har etterlevd rutiner for å registrere sluttdato når saksbehandlere slutter, men at det er forsøkt å rydde opp i etterslepet dette har medført i januar 2015.

#### Sikring av kommunikasjon ved pålogging mot lånesystemet

Lånesystemet ble utviklet for et stormaskinmiljø og senere konvertert til å kjøre på maskiner med operativsystemet Linux. Som en følge av dette benytter Husbanken terminalemulatorer ved pålogging mot systemet. Utskrifter fra skjermbilder viser at det er anvendt terminalemulator hvor kommunikasjon skjer basert på en kommunikasjonsprotokoll der all datatrafikk foregår åpent og ukryptert. Dette gir risiko for at noen kan fange opp datatrafikken og lese all kommunikasjon, inkludert passord og potensielt sensitive data.

Ved revisjonsbesøket ble det opplyst at Husbanken har vurdert risiko knyttet til bruk av denne kommunikasjonsprotokollen og identifisert en terminalemulator som bygger på sikrere teknologi. Det ble opplyst at enkelte ansatte i banken hadde tatt i bruk ny terminalemulator.

#### Sporbarhet/logging

Alle endringer i innstillinger, vedtak og andre viktige hendelser i en saksgang i lånesystemet logges/journalføres.<sup>2</sup> Det skal dermed i ettertid være mulig å se hvem som har foretatt endringer av et lån. Krav til sporbarhet i saksbehandlingen synes dermed etterlevd.

### *2.2 Natural Security*

#### Tilgangskontroller

Lånesystemet Hils/Vinnbin er programmert i språket Natural. For at en person skal få tilgang til systemet, må brukeridenten være registrert i sikkerhetssystemet Natural Security. Hvilke funksjoner/menypunkter den enkelte brukerident har tilgang til er styrt gjennom Natural Security. Det spesielle her er at Husbanken må definere hvilke funksjoner/menypunkter en gruppe identer ikke har tilgang til, i stedet for å definere hvilke funksjoner man har tilgang til. Systemets virkemåte kan hevdes å gjøre administrasjon av dette mer krevende for Husbanken.

Brukeridentene i Natural Security er plassert i grupper. Husbanken har i revisjonsbesøk opplyst at brukerne var delt i 80-90 grupper, men at dette ble ryddet opp i 2011. Husbanken benytter nå aktivt 14-15 grupper. Ingen av de utnyttede gruppene er

<sup>2</sup> Brev fra Husbanken til Riksrevisjonen 12. desember 2014

imidlertid slettet. Dette gir et mer uoversiktlig bilde av sikkerheten i systemet og risiko for at noen har større tilganger enn nødvendig.

Husbanken har oversendt en oversikt over grupper som er i bruk og hvilke oppgaver medlemmene i gruppene skal ha. Videre har banken oversendt oversikt over regler som er lagt inn i Natural Security for å begrense hvilke funksjoner/menypunkter de enkelte grupper har tilgang til. Gjennomgang av begrensningene av tilgang til funksjoner/menypunkter, viser at det ikke er samsvar mellom tilganger og beskrivelser av grupper. Som eksempel har grupper som er beskrevet å være kun for saksbehandlere uten fullmakt til vedtak, ikke blitt hindret tilgang til funksjoner/menypunkter som brukes til å vedta tilsagn om lån.

Gjennomgang av hvilke funksjoner/menypunkter de enkelte grupper ikke har tilgang til viser videre at nærmere 40 prosent av begrensningene angitt i Natural Security ikke fungerer. Dette skyldes at de viser til funksjoner/menypunkter som ikke finnes i henhold til mottatte oversikter. Det er indikasjoner på at Husbanken ikke har holdt reglene oppdatert når det har skjedd endringer i programmet. Lånesystemet er gammelt og basert på en teknologi hvor det er begrenset tilgang på kompetanse i Norge. Husbankens utfordringer med å vedlikeholde tilgangsregler, og også tilgangsgrupper slik nevnt over, kan ses i sammenheng med utfordringer med å få tilgang til kompetanse.

Sammenstilling av hvem som har de ulike roller i saksbehandlerregisteret med medlemskap i grupper i Natural Security viser flere tilfeller der det ikke er logiske sammenhenger. Dette viser utfordringer med administrasjonen av rettigheter i Natural Security og saksbehandlerregisteret. Det viser også at skillelinjene i rettigheter mellom de ulike tilgangsgruppene i Natural Security ikke er klare. Eksempler på manglende logisk sammenheng er:

- Av 105 brukeridenter som er plassert i gruppe HLS3 i Natural Security (beskrevet å være saksbehandlere uten fullmakt til å gjøre vedtak), har 21 fullmakt til å gjøre vedtak og 7 kun spørretilgang i saksbehandlerregisteret.
- Av 51 brukeridenter som er plassert i gruppe HLS4 i Natural Security (saksbehandlere med fullmakt til å gjøre vedtak), har 17 kun fullmakt til å saksbehandle i saksbehandlerregisteret.
- Av 24 brukeridenter som kun har tilgang til spørrebilder i følge Natural Security, har 14 saksbehandlerrett eller fullmakt til å gjøre vedtak i saksbehandlerregisteret.

Administrator i Natural Security er en rolle som gir rettigheter til å gi og endre tilganger definert i systemet. Mottatt dokumentasjon viser at 17 brukeridenter er gitt administratorrett som medlem av gruppen Natural Syssec. Dette inkluderer to ikke-personlige identer, to identer til personer som har sluttet i Husbanken og en ekstern konsulent. Dokumentasjon viser at ytterligere to personer har administratorrolle i forhold til terminregnskapet. Arbeidsdeling beskrevet av Husbanken under revisjonsbesøk ga ikke forklaring til hvorfor så vidt mange personer er gitt administratorrettigheter.

#### Logging i Natural Security

Bruk av administratorrolle i Natural Security for endringer av autorisasjoner blir logget av systemet. Mottatt eksempel på rapport fra logg viser at den inneholder kun begrenset informasjon, f.eks. kun at det er foretatt endringer for en gruppe eller en link, men ikke hva som var verdi før og etter endring. Det er ikke lagt frem revisjonsbevis for rutinemessig gjennomgang av loggen. Ved revisjonsbesøk ble det opplyst at logg ble gjennomgått ved behov.

### 2.3. Databasen Adabas

#### Tilgangskontroller

Natural Security regulerer tilgangen til programmene som utgjør lånesystemet, men ikke til selve databasen. Det er ikke tilrettelagt for tilgangskontroller direkte knyttet til informasjon i databasen Adabas.

Tilleggsproduktet Adabas Security kan benyttes for å sikre databasen på ulike måter, ved mer detaljerte tilgangsregler, kryptering eller passordbeskyttelse. Husbanken anvender ikke dette produktet. Filene i databasen består av er imidlertid beskyttet av operativsystemet slik at kun en brukerident kan skrive til filene. Logg viser at denne ikke-personlige brukeridenten ble brukt til pålogging 357 ganger i 2014. Det er ikke mulig å fastslå hvem som har logget på med brukeren, men det er opplyst at det er ansatte i IT-seksjonene som har tilgang til den.

I teorien kan flere ulike programmer benyttes til å lese og endre data i databasen, ikke bare Hils/Vinnbin. Husbanken har opplyst at kun Adabas SQL Gateway anvendes i tillegg til selve lånesystemet. Adabas SQL Gateway aksesserer databasen for å hente ut informasjon til bankens datavarehus. Husbanken har satt opp et eget tilgangskontrollsystem som en del av Adabas SQL Gateway. Tilgangskontrollene er satt opp slik at Adabas SQL Gateway kun kan lese fra databasen. Administratorer i IT-seksjonene har adgang til å gjøre endringer i oppsettet av Adabas SQL Gateway.

### 2.4 Server for lånesystemet

#### Tilgangskontroller mv.

Siden Active Directory brukes for autentisering av vanlige brukere, er det få brukeridenter som er definert direkte på serveren for lånesystemet. Brukeridenter definert direkte på serveren er i hovedsak ikke-personlige identer med store rettigheter.

Krav til passord mv. ved pålogging mot server for lånesystemet har blitt vurdert ut fra uttrekk av data fra systemet. Kravene til passordlengde og kompleksitet er i samsvar med Husbankens retningslinjer. Revisjonen viser imidlertid at passord for identene på server ikke har vært skiftet på lang tid. For eksempel var ikke passordet til superbrukeren med høyest rettigheter på serveren, blitt endret siden august 2012. For de andre identene ble passord endret i 2013. Disse passordene utløper aldri, slik at det ikke er krav til endring av passord.

Analyse av logg viser at den ikke-personlige brukeridenten med høyest rettigheter på systemet har blitt benyttet til pålogging 127 ganger i løpet av 2014. Det vises også til omtale av annen ikke-personlig brukerident i punkt 2.3 over. Bruk av ikke-personlige brukeridenter gir usikkerhet med hensyn til hvem som reelt har tilgang til høyt privilegerte rettigheter, samt gjør det vanskelig å spore hvem som har foretatt endringer i systemet.

Kontroll av logg for bruk av systemet viser videre sesjoner hvor brukeridenter er pålogget systemet i lange perioder. Logg fra databaseserveren viser brukersesjoner hvor en personlig brukerident er pålogget opp til 58 døgn. De lengste sesjonene er ofte foretatt av brukeridenter tilknyttet ansatte ved Husbankens IT-seksjoner for drift og utvikling eller høyt privilegerte ikke-personlige brukeridenter.

#### Logging

Tilgangskontroller skal hindre at feil og uregelmessigheter oppstår, mens logging er grunnlaget for å oppdage slike hendelser dersom noe skulle skje. Logging gir også sporbarhet for endringer og hvem som har utført disse.

I Husbankens retningslinjer for sikkerhet<sup>3</sup> er det slått fast at for å kunne foreta kontroller i ettertid, gjennomføres logging av hendelser som har betydning for sikkerheten. Det er nevnt av- og påloggingstidspunkt og endringer i autorisasjoner. Tilgangsligger skal i følge retningslinjene gjennomgås jevnlig av it-drift for å sjekke unormale hendelser og forsøk på misbruk.

Gjennomgang av loggoppsett og loggfiler viser at sikkerhetsloggen (audit log) er aktivert, men det er ikke satt noen regler for hva som skal logges. Dermed logges kun et fåtall hendelser som ikke er konfigurert av banken, hovedsakelig knyttet til på- og avlogging. Videre er sikkerhetsloggen satt opp slik at den roteres (overskrives) når de fem loggfilene er fulle. Innhentede loggfiler viser at loggen kan gå full i løpet av et par døgn ved normal drift og dermed kan bli overskrevet. Husbanken har i tillegg backup som kan gi tilgang til loggene i ytterligere 30 dager.

Rutinemessig oppfølging av logger er nødvendig for å fange opp eventuelle uberettigede aktiviteter, sikkerhetsbrister m.m. Det er ikke lagt frem revisjonsbevis for rutinemessig gjennomgang av loggene. Ved revisjonsbesøk ble det opplyst at logger blir gjennomgått ved behov. Nytteverdien av loggene må også sees i sammenheng med bruk av ikke-personlige identer for administrasjon av systemet. Dette fører til at det er vanskelig å identifisere hvem som har foretatt endringer.

### *2.5 Katalogtjenesten Active Directory*

Katalogtjenesten Active Directory benyttes i Husbanken blant annet til å administrere brukeridenter og til å autentisere brukere ved pålogging. Det betyr at for eksempel krav til passord er definert her. Revisjonen av tilgangskontroller med basis i Active Directory omfatter fire ulike kontroller dekket i egne punkter nedenfor:

- bruk av administratorroller
- brukere med påloggingsinformasjon til låneserver
- ikke-personlige brukere
- krav til passord

#### Bruk av administratorroller i Active Directory

Administratorroller i katalogtjenesten Active Directory gir de høyest privilegerte brukerrettighetene og svært vide tilganger til å foreta endringer. Ut fra data hentet ut fra Husbankens systemer har vi analysert bruken av administratorroller.

Fjorten personlige brukeridenter har administratorroller i Husbanken. Dette inkluderer ni som er "Schema administrator", en rolle som skal brukes for å vedlikeholde selve oppsettet av Active Directory og som i følge leverandøren Microsoft ingen behøver å ha bortsett fra når det skal gjøres større endringer i systemet. Rolle som administrator gir større rettigheter enn hva som er nødvendig for å gjennomføre de aller fleste av IT-personalets arbeidsoppgaver.

Husbanken opplyste ved revisjonsbesøk at den er i ferd med å etablere et rollebasert rettighetsoppsett med mindre rettigheter til daglig bruk for IT-personell. Dette skal minske bruken av administratorroller. Det ble opplyst at ny policy for dette skal besluttes i april 2015.

Det er videre seks serviceidenter, som programmer bruker for å autentisere seg, som er gitt rettigheter som administrator i Husbanken. Dette gir programmene større rettigheter enn nødvendig. Husbanken har opplyst at banken arbeider med å redusere rettighetene til disse serviceidentene.

---

<sup>3</sup> Intern retningslinje HB 1.D.6.4 Driftsplanlegging og sikkerhet punkt 4.5

### Brukere med påloggingsinformasjon til låneserver

Hvilke brukere som har tilgang til serveren for lånesystemet bestemmes i Active Directory. Husbanken legger da inn verdier for aktuelle brukere som benyttes ved pålogging mot låneserveren.

Data hentet ut fra Active Directory viser at det er 341 aktive brukeridenter som er definert med nødvendige verdier for pålogging mot låneserveren. Logg fra låneserveren viser at 115 av disse ikke har logget på etter 1. januar 2014. 76 av brukeridentene er ikke i saksbehandlerregisteret og kan derfor ikke benytte lånesystemet. Ubenyttede tilgangsrettigheter til server for lånesystemet indikerer at det ikke er behov for disse.

### Ikke-personlige identer

Uttrekk av informasjon fra Active Directory viser at det er 768 brukeridenter i Husbanken som det er mulig å bruke for å logge seg på virksomhetens nettverk. Om lag halvparten av disse er brukeridenter som ikke er knyttet direkte til en ansatt i Husbanken, dvs. ikke-personlige brukeridenter.

Det er nødvendig med en del ikke-personlige brukeridenter som f.eks. kan benyttes av programmer i automatiserte rutiner. Analyse av brukere i Husbanken viser imidlertid grupper av brukeridenter hvor behov for bruk ikke er klar:

- Det er 34 identer hvor ordet "test" inngår i navnet.
- Det er 40 kursidenter som ikke er knyttet til person
- Det er en rekke brukeridenter er knyttet til seksjoner, rom, utlånte PC'er osv.

Ved revisjonsbesøk 9. mars 2015 opplyste Husbanken at et arbeid med å rydde opp i brukeridenter pågår og at man allerede har strammet inn på flere områder. Innstramming skjer både i form av å redusere rettigheter og å sperre identer for bruk.

Analyse av identer ut fra mottatte data viser at 134 av de 768 gyldige brukeridentene i Husbanken aldri har vært logget inn på, i tillegg til at 64 brukeridenter ikke har vært benyttet siden 1. januar 2014. Flertallet av disse er ikke-personlige brukeridenter. Ubenyttede tilgangsrettigheter til server for lånesystemet indikerer at det ikke er behov for disse.

Analyse viser videre at det er 293 brukeridenter hvor passord aldri utløper, dvs. man behøver aldri å endre passordet. Dette kan være en nødvendig funksjon for en del identer benyttet av programmer, men omfanget i Husbanken synes å gå utover dette. Brukeridenter hvor passord aldri utløper inkluderer f.eks. enkelte personlige brukere, en del konsulenter og identer knyttet til seksjoner/lokasjoner.

Ved installasjon av Active Directory skapes en ikke-personlig gjestekonto. Denne har få rettigheter, men muliggjør pålogging uten passord. Identen har ikke vært sperret for bruk i Husbanken. Forholdet ble tatt opp ved revisjonsbesøk 9. mars 2015, men det kunne ikke påvises noen årsak til at identen skulle være åpen for bruk i Husbanken.

### Krav til passord

Uttrekk av data fra Active Directory viser at Husbanken har satt krav til passord som omfatter passordlengde, kompleksitet, bytte av passord og sperring av brukerident ved mange mislykkede påloggingsforsøk. Kravet til passordlengde er kortere enn det som er angitt i retningslinjer for ikt-sikkerhet i Husbanken.<sup>4</sup> Videre viser oppsettet at brukeridenter kun sperres i en kortere periode dersom man overskrider antall lovlige mislykkede påloggingsforsøk. Kort periode med sperret ident muliggjør mange forsøk på å logge seg inn i systemet.

---

<sup>4</sup> Intern retningslinje HB 1.D.6.4 Driftsplanlegging og sikkerhet punkt 4.2



### Logging

Husbanken anvender det tradisjonelle loggoppsettet for Windows servere lagt til grunn i Windows server 2003 og tidligere. Fra og med Windows server 2008 er det tilgjengelig oppsett som gir mer finmasket kontroll av hva som logges og dermed mulighet til å øke relevant logging og minske støy fra logging av hendelser som er mindre interessante.

Uttrekk av informasjon fra systemet viser at det foretas logging av blant annet vellykkede pålogginger, endringer i brukere og grupper, samt endringer i policy for logging. Dermed logges det meste som kan forventes å identifisere hendelser som kan true systemets integritet. Imidlertid logges ikke mislykkede påloggingsforsøk hverken i domene eller på lokal maskin. Det kan gjøre det vanskeligere å fange opp eventuelle forsøk på uautorisert tilgang til Husbankens systemer.

Rutinemessig oppfølging av logger er nødvendig for å fange opp eventuelle uberettigede aktiviteter, sikkerhetsbrister m.m. Det er ikke revisjonsbevis for rutinemessig gjennomgang av loggene. Ved revisjonsbesøk ble det opplyst at logger blir gjennomgått ved behov.

## *2.6. Fysisk sikkerhet*

### Adgangskontroller

Husbanken har satt krav til fysisk sikkerhet for bl.a. datautstyr i interne retningslinjer.<sup>5</sup> Fysisk inspeksjon av serverrom ved bankens hovedkontor i Drammen viser at dette er sikret med et adgangskontrollsystem. Kontroll av utstedte adgangskort viste at kun ansatte med relevante arbeidsoppgaver har adgang til rommet. Serverrommet ligger i 2. etasje og har vinduer, dog ikke vinduer som kan åpnes. Husbanken har vurdert risiko knyttet til plasseringen av rommet. Når banken flytter senere i 2015 vil serverrommet plasseres mindre eksponert, opplyser Husbanken.

Ved vårt revisjonsbesøk ved Husbankens regionskontor i Bodø uke 9 var hverken byggets felles resepsjon i første etasje, eller Husbankens egen resepsjon på egen etasje bemannet. Dør til Husbankens lokaler var ikke låst i åpningstiden på kontrolltidspunktet. Dette gir risiko for at uvedkommende kan få tilgang til Husbankens lokaler og IT-utstyr.

### Logging

Husbanken foretar logging av adgang til serverrommet ved hjelp av adgangskortsystemet. Kontroll av loggen for en uke viste at kun autoriserte personer hadde gått inn i rommet.

Rutinemessig oppfølging av logger er nødvendig for å fange opp eventuelle uberettigede aktiviteter, sikkerhetsbrister m.m. Det er ikke lagt frem revisjonsbevis for rutinemessig gjennomgang av loggene. Rutinene vil dermed ikke fange det opp dersom et uautorisert kort brukes til å få adgang til rommet. Det er et kompensierende forhold at serverrommets beliggenhet fører til at ansatte i IT-seksjonene vil ha visuell oversikt over hvem som går inn i rommet i arbeidstiden.

## **3. Er Husbankens internkontroll ved utbetaling av lån i samsvar med krav i økonomiregelverket i staten?**

### *3.1 Arbeidsdeling ved vedtak om tilsagn, bevilgning og utbetaling av lån?*

I Husbanken behandles lån og tilskudd i en tre trinns modell for å generere en utbetaling av lån/tilskudd - tilsagn, bevilgning og utbetaling. Arbeidsdeling er sikret ved

<sup>5</sup> Intern retningslinje HB 1.D.6.4 Driftsplanlegging og sikkerhet punkt 8

at to personer er involvert på hvert enkelt trinn: for å vedta tilsagn, for å vedta bevilgning, og til slutt for å vedta utbetaling.<sup>6</sup> Den person som vedtar bevilgning (budsjettddisponerer) kan ikke også vedta utbetaling.

For de 35 kontrollerte tilskuddene var det gjennomført arbeidsdeling med hensyn til tilsagn, bevilgning og utbetaling. Kontrollen omfattet også etterlevelse av krav til attestasjon og budsjettddisponering (vedtak om bevilgning). Det ble ikke funnet avvik fra kravene i økonomiregelverket ved kontroll av utvalget.

Kontroller i lånesystemet bidrar til å sikre arbeidsdeling ved behandling av lån. Samme person (brukerident) kan ikke både innstille og vedta i samme sak.<sup>7</sup> Systemet forutsetter at to medarbeidere har deltatt i prosessen for å ferdigstille en sak i de ulike vedtaksfaser i Hils. Det må dessuten oppgis et eget passord for å vedta utbetaling av et lån. Grunnlaget for å sikre arbeidsdelingen i lånesystemet er saksbehandlerregisteret, som angir hvilke brukere som har tilgang til å:

- saksbehandle og innstille til vedtak om lån
- fatte vedtak om lån
- vedta utbetaling av lån

Ifølge Husbankens interne retningslinjer er budsjettddisponeringsmyndighet for lån tildelt de enkelte regiondirektører.<sup>8</sup> Vedtak om utbetaling skal fattes i Forvaltningskontoret. Analyse av mottatt informasjon fra saksbehandlerregisteret viser at enkelte grupper ansatte har tilgangsrettigheter i lånesystemet som går på tvers av deres roller i forvaltningen av lån. Det kan bety at noen har tilgang til å gjennomføre funksjoner som bør skilles mellom:

- 24 brukeridenter har fått tildelt rettigheter til å legge inn passord for å utbetale lån. Dette er langt flere enn hva som er nødvendig ut fra virksomhetens rutiner og inkluderer blant annet seks ansatte ved regnskapsenheten i banken. I brev av 12. desember 2014 har Husbanken oppgitt at de som arbeider i regnskapsenheter ikke skal ha tilgang til lånesaksbehandlingsrutiner med oppdateringsfunksjon.
- Det er seks personer i seksjonene for IT-drift og -utvikling som har tilgang til å saksbehandle, vedta eller utbetale lån. Det indikerer mangler i arbeidsdelingen mellom primærvirksomhet og bankens IT-seksjoner.

### *3.2 Samsvar mellom regnskapsført utbetaling/innbetaling av lån/rente/avdrag i Agresso og beregnet lån/rente/avdrag i lånesystemet?*

Revisjonen viser ingen vesentlige avvik. Imidlertid innebærer det faktum at Hils/Vinnbin ikke periodiserer, og at det ikke kan tas ut rapporter fra Hils/Vinnbin til hver enkelt konto i saldobalansen knyttet til lån, at både avstemmingen og kontrollen med avstemmingen er utfordrende. Periodiseringsavviket svinger mellom månedene, og er erfaringsmessig størst ved årsskiftet. Ved årsskiftet utgjør periodiseringsavviket 116,9 mill. kroner mer ført i Agresso enn Hils/Vinnbin av den utestående låneporteføljen på 135,6 mrd. kroner.

<sup>6</sup> Brev fra Husbanken til Riksrevisjonen 12. desember 2014

<sup>7</sup> Brev fra Husbanken til Riksrevisjonen 12. desember 2014

<sup>8</sup> Intern retningslinje HB 1.D.2.1 og HB 1.D.2.20

## 6. Konklusjon

Husbanken er det viktigste statlige organ for gjennomføring av regjeringens boligpolitikk. Lån og tilskudd som håndteres i lånesystemet utgjør en vesentlig del av bankens virksomhet. Revisjonen viser

- at tilgangskontroller og logging i lånesystem og underliggende infrastruktur har vesentlige mangler og at Husbanken dermed ikke etterlever krav i personopplysningsloven og økonomiregelverket
- mangler i implementering i sikkerhetssystemet Natural Security, som benyttes i samspill med lånesystemet, gir ikke de begrensningene i tilganger til funksjoner som er forutsatt av Husbanken
- at enkelte lån ikke er utmålt i tråd med regelverket, og det indikerer at systemet ikke sikrer mot at det fattes uhjemlede vedtak.

For øvrig viste en begrenset stikkprøvekontroll av beregning av renter, avdrag og lån for grunnlån ingen vesentlige avvik. Revisjonen viste også at avstemming mellom låne- og regnskapssystem gjennomføres i henhold til kravene.

Nedenfor følger konklusjonene knyttet til hver enkelt problemstilling:

1. Utmåles grunnlån og fastsettes renter og avdrag i tråd med lov om Husbanken, forskrift om grunnlån fra Husbanken, lov om renter ved forsinket betaling m.m. og forskrift om rente- og avdragsvilkår for lån i Husbanken?

Fra utvalgene vi har trukket har vi ikke funnet vesentlige avvik i beregning av rente, avdrag, og utmåling av lån. Basert på de enkelte utvalgene viser revisjonen at Husbanken beregner rente og avdrag korrekt i tråd med regelverket fastsatt i forskrift om rente og avdragsvilkår for Husbankens låneordninger, og i lov om forsinket betaling m.m. for grunnlån.

Det er identifisert tilfeller med mangler i Husbankens dokumentasjon og hjemmelsgrunnlag knyttet til tilfeller der Husbanken har innvilget 100 prosent lånefinansiering. Det er også identifisert mangler ved hjemmelsgrunnlag knyttet til innvilgelse av 50 års avdragstid for grunnlån, og til innvilgelse av kjøp av boliger større enn 150 kvadratmeter.

2. Er informasjonssikkerhet ved forvaltningen av lån i samsvar med krav i personopplysningsloven og økonomiregelverket i staten?

Det er mangler i Husbankens tilgangskontroller som skal sikre lånesystemet og data mot uautoriserte endringer, jf. personopplysningsforskriften § 2-13 og bestemmelsene punkt 4.3.6. Tilgangsrettigheter i systemene er i mange tilfeller større enn arbeidsoppgavene til de enkelte brukerne burde tilsi. Brukeridenter og tilgangsrettigheter synes ofte ikke endret når noen slutter i stilling eller skifter arbeidsoppgaver. Mange har administratorrettigheter som gir få begrensinger både i Active Directory og i Natural Security.

Tilgangskontroller til meny punkter i lånesystemet implementert i Natural Security gir ikke de begrensninger som var tiltenkt og reflekterer ikke forskjeller i behov for tilgang for ulike brukergrupper. Lånesystemet er gammelt og basert på en teknologi hvor det er begrenset tilgang på kompetanse i Norge. Det er indikasjoner på at mangelfull tilgang på kompetanse om sikkerhetsløsning for lånesystemet kan ha bidratt til at tilgangskontrollene ikke fungerer som forutsatt. Mangler i tilgangskontroller gir risiko for at det kan skje både bevisst misbruk av Husbankens systemer og ubevisste feil som kan få konsekvenser for Husbankens kunder.

Fysisk sikring mot uautorisert adgang til utstyr som brukes for å behandle personopplysninger, jf. personopplysningsforskriften § 2-10, synes i hovedsak etterlevd. Adgangskontrollene ved bankens kontor i Bodø oppfylte ikke kravene på kontrolltidspunktet.

Husbanken gjennomfører i hovedsak logging i samsvar med kravene i personopplysningsforskriften § 2-14 og bestemmelsene punkt 4.3.6, men det er enkelte mangler i loggoppsettet på alle kontrollerte nivåer. Svakheter kan føre til at forsøk på uautorisert bruk av informasjonssystemet ikke blir registrert. Det er videre ikke lagt frem bevis for rutinemessige gjennomganger eller analyser av logger for å avdekke mulige sikkerhetsbrudd, slik interne retningslinjer legger til grunn. Logger gjennomgås kun ved behov. Resultatene indikerer mangler i Husbankens bevissthet rundt hva som bør logges og hvordan logger brukes. Manglende overvåking av systemer kan medføre at disse kompromitteres uten at dette oppdages.

### 3. Er Husbankens internkontroll ved utbetaling av lån i samsvar med krav i økonomiregelverket i staten?

Husbankens rutiner og lånesystem Hils/Vinnbin sikrer i utgangspunktet arbeidsdeling i henhold til bestemmelsene punkt 2.4 ved at det ikke kan gis tilsagn om, bevilges eller utbetales et lån uten at to personer har godtatt dette. Det er videre ikke oppdaget avvik i forhold til kravene i bestemmelsene om attestasjon og budsjett disponering. Det er imidlertid svakheter i tilgangsrettigheter i saksbehandlerregisteret som ikke reflekterer deling av arbeidsoppgaver, jf. at ansatte i IT-seksjoner for drift og utvikling har tilganger til å saksbehandle/vedta lån, mens ansatte i regnskapsenheten kan vedta utbetaling av lån.

Etter vår vurdering gir Husbankens rutiner for overføring av data fra forsystemet Hils/Vinnbin til regnskapssystemet Agresso tilfredsstillende sikkerhet for korrekt utbetaling av lån og tilskudd, jf. bestemmelsene punkt 4.3.2 *Funksjonalitet for bokføring og registrering*. Det faktum at Hils/Vinnbin ikke periodiserer innebærer imidlertid at avstemmingen mellom systemene er utfordrende å gjennomføre og kontrollere.

## 7. Anbefaling

Riksrevisjonen anbefaler at Husbanken vurderer følgende tiltak;

- begrenser tilganger til bankens systemer til kun det som er nødvendig for å gjennomføre den enkeltes oppgaver
- anvender logger aktivt for å oppdage eventuelle sikkerhetshendelser
- vurderer hvilke tiltak som må gjennomføres for at tilgangskontrollene til lånesystemets funksjoner skal fungere etter sin hensikt
- søker å bygge inn kontroller i lånesystemet for å begrense mulige uhjemlede vedtak.

Oslo; 29.05.2015

Etter fullmakt

  
for Hans Conrad Hansen  
ekspedisjonssjef

  
Einar Sæther  
avdelingsdirektør



HUSBANKEN  
Org.nr.: 942114184

Vedlegg 3

### **Oversikt over skriftlig kommunikasjon vedrørende resultater av revisjonen for regnskapsåret 2014**

- Innledende revisjonsbrev av 2. september 2014, 2014/01186-1
- Brev av 27. mars 2014 Etterlevelsesrevisjon om Husbankens lånesystem for 2014 - oversendelse av utkast rapport for kommentarer, 2014/01186-33
- Svarbrev av 13. april 2014 Etterlevelsesrevisjon om Husbankens lånesystem for 2014 - oversendelse av utkast rapport for kommentarer, 2014/01186-37