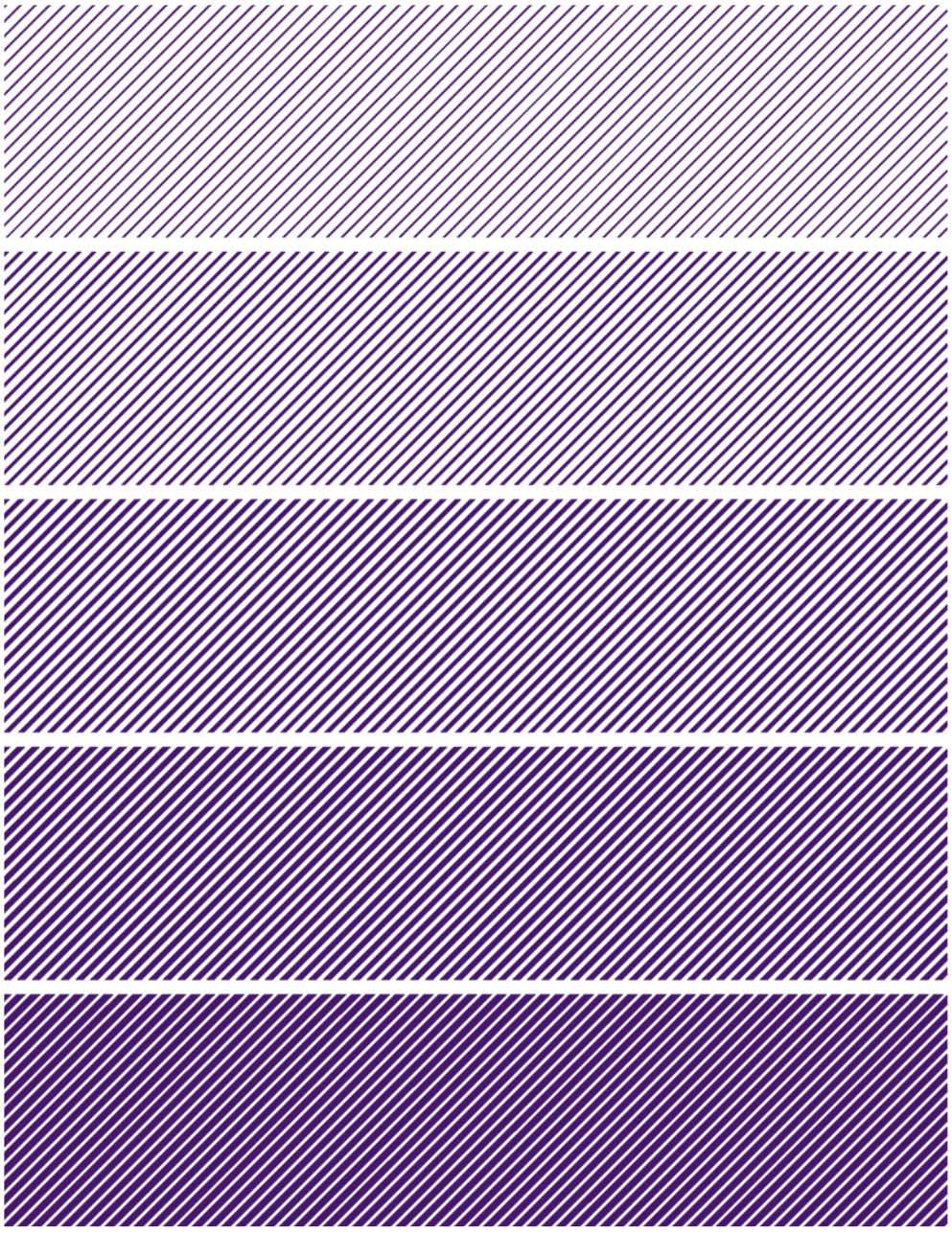
FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Fellesrapport

IKT-Risiko i regnskapsførerselskaper

Tematilsyn 2015



DATO:
15. april 2016

NUMMER:
15/5273

SEKSJON/AVDELING:
REVISJON OG REGNSKAPSFØRING, MARKEDSTILSYN

Innhold

1 Bakgrunn, formål og gjennomføring

Bakgrunnen for at IKT-risiko ble valgt som tema, er fordi dette normalt er en betydelig risiko i autoriserte regnskapsførerselskaper. Finanstilsynet viser til at regnskapsførerselskaper i stor grad benytter maskin- og programvareteknologi i virksomheten, og at det kan få stor betydning for oppdragsgiverne dersom disse hjelpemidlene svikter. Svikt kan for eksempel medføre at oppdragsgiverne ikke får oppdatert regnskapsinformasjon når de trenger det, eller at de ikke får utført oppgaver som ordre og fakturering som foretas gjennom regnskapsførerselskapets systemer.

Et formål med tematilsynet er å få en oversikt over IKT-systemene i regnskapsfører-selskapene. Et annet formål er å øke bevisstheten rundt IKT-risiko i selskapene og hos andre aktører som leverer tjenester til regnskapsførerbransjen. Et tredje formål er å øke regnskapsførerselskapenes oppmerksomhet rettet mot viktigheten av å etterleve forskrift om risikostyring og internkontroll av 22. september 2008 nr. 1080 (risikostyringsforskriften). Grunnen til at dette er viktig, er fordi etterlevelse av forskriften vil gi styret og daglig leder et godt utgangspunkt for en forsvarlig håndtering av IKT-risikoen og andre risikoer i virksomheten.

Tematilsynet ble gjennomført i oktober og november 2015. Alle regnskapsførerselskaper måtte besvare et spørsmålsskjema i Altinn. Enkeltpersonforetak var ikke omfattet av tilsynet.

Spørsmålene er knyttet til:

- Risikovurdering og -styring
- Regnskaps- og oppdragsstyringssystemer
- Utkontraktering av IKT-virksomhet
- Sikkerhet
- Endringer i IKT-systemer
- Drift og vedlikehold av IKT-systemer
- Håndtering av alvorlige driftsavbrudd
- Forholdet til oppdragsgiverne

De fleste spørsmålene gjelder plikter som følger direkte av regnskapsførerlovgivningen[1], herunder standarden GRFS[2], og av risikostyringsforskriften. Øvrige spørsmål knyttet seg til vurderinger og handlinger som Finanstilsynet mener kan bidra til oppfyllelsen av krav i lovgivningen.

Spørreskjemaet ble sendt til 2885 regnskapsførerselskaper. 2788 selskaper har svart. Av de som ikke har svart er det ca. 70 selskaper som slettet autorisasjonen som regnskapsførerselskap, enkelte selskaper har fått fritak fra plikten til å besvare, mens resterende 11 har mottatt vedtak om tilbakekall av autorisasjonen som regnskapsførerselskap som følge av manglende besvarelse. Enkelte av disse vedtakene er påklaget.

I tillegg ba Finanstilsynet 18 leverandører av IKT-systemer til regnskapsførerbransjen om å sende inn de standardavtaler som benyttes. Dette for å se om avtalene er utformet slik at de tar hensyn til de pliktene som påhviler regnskapsførerselskapene. Finanstilsynet mottok til sammen 17 avtaler fra 8 forskjellige leverandører.

[1] Lov om autorisasjon av regnskapsførere av 18. juni 1993 nr. 109 og forskrift om autorisasjon av regnskapsførere mv. av 8. februar 1999 nr. 196

[2] God regnskapsføringsskikk (GRFS), Standard av juni 2014, oppdatert november 2014

2 Regnskapssystemer og oppdragsstyringssystemer

For å få en oversikt over IKT-systemene, ble regnskapsførerselskapene bedt om å opplyse hvilke systemer som benyttes i virksomheten innenfor de fem områdene; bokføring, fakturering, lønn, årsoppgjør og ligningspapirer. I tillegg ble selskapene bedt om å opplyse hvilke oppdragsstyringssystemer som benyttes.

Svarene viser at flertallet av regnskapsførerselskapene benytter ett system innenfor hvert av de fem leveranseområdene.

Flertallet av regnskapsførerselskapene benytter også bare ett oppdragsstyringssystem.

Fordelingen fremkommer av følgende tabell:

Tabell 1

Antall systemer per selskap (%):	1	2	3	4	5	6	7	Har ikke
Bokføring	79,3	12,7	3,3	1,3	0,4	0,04	0,04	2,8
Fakturering	82,2	10,6	2,8	0,6	0,2			3,7
Lønn	87,1	6,1	0,9	0,1				5,8
Årsoppgjør/Ligningspapirer	86,7	7,9	0,6	0,1				4,8
Oppdragsstyring	82,6	7,7	1,1	0,04				8,6

Finanstilsynet har ingen kommentarer til dette, ut over å vise til at IKT-risikoen normalt vil øke med antall systemer i regnskapsførerselskapet, og at dette kan gi økte utfordringer knyttet til styring og kontroll av risiko.

For å få en oversikt over hvor mange ulike regnskapssystemer som er tatt i bruk innenfor hvert av de fem leveranseområdene, stilte Finanstilsynet spørsmål om hvilke systemer som benyttes.[3] Spørsmålet gjelder systemene som sådanne, ikke hvem som leverer eller eier systemet.[4] Tilsvarende gjelder for oppdragsstyringssystemer.

Svarene viser at det benyttes mange ulike systemer[5] innenfor hvert av de fem leveranseområdene. Det samme gjelder for oppdragsstyringssystemene. Flere av disse systemene er bare tatt i bruk av noen få regnskapsførerselskaper.

[3] De mest vanlige systemene var angitt i en rullgardin, og med felt for angivelse av andre systemer.
[4] En leverandør kan levere eller være eier av flere ulike regnskapssystemer eller oppdragsstyringssystemer.
[5] Se fotnote 4.

Følgende tabell viser antall systemer per leveranseområde og hvilken prosentvis dekning de ni største systemene har:

Tabell 2:

Systemer for:	Antall systemer	1-3 største (%)	4-9 største (%)	Andre (%)
Bokføring	86	38	40	22
Fakturering	95	38	34	28
Lønn	50	66	27	7
Årsoppgjør/Ligningspapirer	14	74	25	1
Oppdragsstyring	63	81	7	12

Finanstilsynet har merket seg at det er svært få som opplyser at de benytter egenutviklede systemer for bokføring, fakturering, lønn, årsoppgjør og ligningspapirer.

Når det gjelder oppdragsstyringssystem, opplyser 8 % av regnskapsførerselskapene at de benytter et egenutviklet system. Svarene tyder på at disse ofte er basert på tilpasninger gjort i et standard kontorstøttesystem.

3 Risikohåndtering

Den overordnede risikoen i et regnskapsførerselskap er at oppdragsavtalene og regnskapsførerlovgivningen, herunder god regnskapsføringsskikk, ikke etterleves. De underliggende risikoene knyttet til strategiske, operasjonelle og juridiske forhold, er av betydning for den overordnede risikoen. Av disse underliggende risikoene er IKT-risikoen en vesentlig risiko for regnskapsførerselskaper. En forsvarlig håndtering av IKT-risikoen innebærer at risikoen på sentrale områder må identifiseres og vurderes løpende. Både sannsynligheten for at risikoen inntreffer og konsekvensen av det må inngå i vurderingen. Dersom risikoen vurderes til å være "for stor", må den styres gjennom risikoreduserende tiltak. Det må videre kontrolleres at tiltakene virker som forutsatt.

3.1 Styring av IKT-risiko og internkontroll

Regnskapsførerselskaper er underlagt forskrift om risikostyring og internkontroll (risikostyringsforskriften) av 22. september 2008, jf. § 1 nr. 12. En systematisk tilnærming til risikohåndtering i samsvar med forskriften, vil bidra til en forsvarlig risikohåndtering, også av IKT risikoen. Risikohåndtering i samsvar med forskriften er et nyttig verktøy for styret og ledelsen, forutsatt at systemet tilpasses virksomheten og at det foretas reelle og egne vurderinger. Dersom risikostyringsdokumentet utarbeides bare for å oppfylle et "formalkrav", vil det ikke være til hjelp i virksomheten.

Selv om ikke IKT-forskriften[6] gjelder for autoriserte regnskapsførerselskaper, vil den gi veiledning til hvordan IKT-risiko kan håndteres på en god måte i regnskapsførervirksomheten.

[6] Forskrift av 21. mai 2003 nr. 630 om bruk av informasjons- og kommunikasjonsteknologi

Nærmere krav til IKT-virksomheten i regnskapsførerselskapene fremgår av GRFS punkt 2.8, som omhandler konkrete risikoreduserende tiltak.

Tematilsynet inneholder spørsmål for kontroll av at risikostyringsforskriften etterleves. Spørsmålene og svarene fremgår av følgende tabell:

Tabell 3:

	JA (%)	NEI (%)
Har styret påsett at regnskapsførerselskapet har hensiktsmessige systemer for risikostyring og internkontroll på IKT-området?	97	3
Har daglig leder sørget for å etablere en forsvarlig risikostyring og internkontroll på IKT-området?	98	2
Vurderes IKT-risikoen årlig?	94	6
Vurderes IKT-risikoen ved større endringer?	95	5
Utarbeider daglig leder, minst årlig, en samlet vurdering av risikosituasjonen?	94	6
- Styrebehandles vurderingen?	94	6
Vurderes internkontrollen minst årlig?	93	7
- Dokumenteres vurderingen?	82	18
Foreligger det en skriftlig avtale med leverandøren(e)?	92	8*

** Svaret kan være påvirket av at det, ved kjøp av "online" brukerlisenser, ikke inngås en tradisjonell avtale. Finanstilsynet legger til grunn at kravet om skriftlig avtale i disse tilfellene er oppfylt dersom regnskapsførerselskapet oppbevarer dokumentasjon som viser hva som er kjøpt, når og på hvilke vilkår.*

Risikostyringsforskriften gjelder for alle regnskapsførerselskaper. Finanstilsynet forutsetter derfor at de regnskapsførerselskapene som har svart nei, har sørget for å bringe forholdet i orden.

3.2 Vurdering av IKT-risiko

For å kunne håndtere risikoene i virksomheten på en god måte, må de identifiseres. En identifisering av de konkrete risikoene forutsetter at det foreligger et forsvarlig vurderingsgrunnlag. Dette må utarbeides med tanke på hvordan egen virksomhet faktisk er.

Tematilsynet inneholdt spørsmål om forhold Finanstilsynet mener normalt må inngå i vurderingen av IKT-risikoen i alle regnskapsførerselskaper. Spørsmålene og svarene fremgår av følgende tabell:

Tabell 4:

Inngår følgende elementer i risikovurderingen:	JA (%)	NEI (%)
Oversikt over alle IKT-systemene	97	3
Oversikt over utkontraktert virksomhet	88	12
Vurdering av om IKT-virksomheten oppfyller krav i lovgivningen, herunder GRFS	93	7
Sikkerhet i IKT-systemene	96	4
Behovet for interne retningslinjer for medarbeideres tilgang til og bruk av IKT-systemer	80	20*
Endringer i IKT-systemene	85	15
Drift og vedlikehold av IKT-systemene	95	5
Håndtering av alvorlige driftsavbrudd	91	9
Hvem i regnskapsførerselskapet som følger opp at systemene i avtalene ivaretar lovmessige, driftsmessige og sikkerhetsmessige krav	95	5
Hvordan regnskapsførerselskapet skal håndtere en situasjon der nøkkelperson(er) på IKT-området slutter	78	22*

** Alle spørsmålene måtte besvares. Det antas at de fleste regnskapsførerselskaper med bare en ansatt har svart nei på disse spørsmålene.*

Det er positivt at så mange regnskapsførerselskaper opplyser at ovennevnte forhold inngår i vurderingen av IKT-risikoen. Finanstilsynet forutsetter at de som har svart nei på disse spørsmålene, gjør en fornyet vurdering som minst inkluderer alle de nevnte forhold.

Finanstilsynet er innforstått med at tematilsynet ikke sier noe om kvaliteten i de vurderingene som er gjort på de enkelte områdene.

3.3 Risikoreduserende tiltak

Det er IKT-risiko i alle regnskapsførerselskaper og flere av disse er vesentlige. Dersom en kombinasjon av sannsynlighet og konsekvens innebærer at regnskapsførerselskapet konkluderer med at risikoen er "for stor", må den styres gjennom risikoreduserende tiltak. Slike risikoreduserende tiltak kan enten ha som mål å redusere sannsynligheten for at risikoen materialiserer seg eller være tiltak for å unngå alvorlige konsekvenser. Det må følges opp at de risikoreduserende tiltakene virker som forutsatt.

Tematilsynet inneholder spørsmål for å kontrollere om regnskapsførerselskapet har iverksatt slike risikoreduserende tiltak som Finanstilsynet mener er nødvendige i tilnærmet alle regnskapsførerselskaper. Spørsmålene dekker også tiltak som følger av lovgivning, herunder GRFS.

3.3.1 Informasjonssikkerhet

Med informasjonssikkerhet mener Finanstilsynet sikkerheten i systemene (teknologiske barrierer), og påvirkning av ansattes adferd i bruken av systemene.[7]

Sikkerhet i systemene:
Tilnærmet alle opplyser at behovet for teknologiske barrierer er vurdert, jf. følgende tabell:

Tabell 5:

	JA (%)	NEI (%)
Behovet for virusbeskyttelse	99	1
Behovet for brannmur	98	2
Behovet å begrense tilgangen til ulike deler av IKT-systemene	90	10*

** Alle spørsmålene måtte besvares. Manglende vurdering kan skyldes at regnskapsførerselskapet bare har en ansatt.*

Tematilsynet viser at de fleste har vurdert behovet for tilgangsstyring. Tilgangsstyring er spesielt viktig dersom regnskapsførerselskapet behandler regnskapsinformasjon som kan være sensitiv i markedet, for eksempel der oppdragsgiver er børsnotert. Finanstilsynet ser at behovet for tilgangsstyring vil kunne variere avhengig av regnskapsførerselskapets størrelse og organisering, men det bør alltid vurderes når flere har tilgang til systemet. For eksempel trenger den enkelte medarbeider bare tilgang til opplysninger om egne oppdragsgivere. Plikt til tilgangsbegrensning kan også følge av personopplysningsloven.

38 % av regnskapsførerselskapene har opplyst at oppdragsgiverne har tilgang til regnskapsførerselskapets systemer. I disse tilfellene er det sentralt at regnskapsførerselskapet vurderer hvilken tilgang oppdragsgiver skal ha. Det må sikres at oppdragsgiver ikke har tilgang til taushetsbelagt informasjon eller informasjon ut over det som er bestemt. Det er viktig at tilgangsbegrensningen kontrolleres, særlig gjelder dette etter endringer i systemet.

Ansattes bruk av systemene:
Teknologiske barrierer som virusbeskyttelse, brannmur og begrensning av tilgang til ulike deler av IKT-systemene er ikke alene tilstrekkelig risikoreduserende tiltak. Slike tiltak må suppleres med retningslinjer for ansattes bruk av IKT.

[7] GRFS punkt 2.8.5

Følgende tabell viser hvor mange som har utarbeidet interne retningslinjer for ansattes bruk av IKT:

Tabell 6:

Har selskapet interne retningslinjer for:	JA (%)	NEI (%)
Håndtering av eposter, lenker og minnepinner med ukjent innhold	72	28
Bruk av andre enheter (mobiltelefoner, nettbrett m.m.)	58	42
Medarbeideres bruk av fildelings- og oppbevaringstjenester som ikke er avtalefestet i regnskapsførerselskapet	64	36

Finanstilsynet mener at retningslinjer for ansattes bruk av IKT er nødvendig fordi det bidrar til å skape bevissthet knyttet til den risikoen som ligger i bruk av slike hjelpemidler. Dette gjelder uavhengig av størrelsen på regnskapsførerselskapet, også selskaper der det bare er en ansatt.

Av de selskapene som svarer at de har interne retningslinjer, er det 25 % som svarer at retningslinjene ikke er skriftlige. 2 % svarer at det ikke følges opp at retningslinjene etterleves. For at risikoen i praksis skal begrenses, må regnskapsførerselskapet følge opp medarbeidernes adferd. Uten skriftlige retningslinjer vil det være vanskelig å reagere.

Regnskapsførerselskapet må også forsikre seg om at oppdragsgivere som har tilgang til systemene er forpliktet til å følge de retningslinjer og rutiner som ivaretar regnskapsførerselskapets behov for informasjonssikkerhet.

3.3.2 Drift og vedlikehold av IKT-systemer

At systemene ikke virker som forutsatt og at informasjon går tapt er en sentral risiko. Retningslinjer som bidrar til å sikre en stabil, planlagt og forutsigbar drift, er et nødvendig risikoreduserende tiltak. [8] Slike retningslinjer bør omfatte alle sentrale forhold som kan medføre at systemet ikke fungerer. Uten rutiner som bidrar til å sikre driften og vedlikehold av systemene kan ikke driften av regnskapsførervirksomheten anses som forsvarlig. [9]

13 % opplyser at de ikke har retningslinjer for drift og vedlikehold av IKT-systemene. Dette er uheldig, også i små regnskapsførerselskaper. Slike retningslinjer kan være nødvendig dersom nøkkelpersoner ikke er i stand til å utføre sine oppgaver slik at en annen må overta for å ivareta oppdragsgivers interesser. Finanstilsynet forutsetter at regnskapsførerselskaper som ikke har retningslinjer for drift og vedlikehold fastsetter slike.

Svaret kan dekke manglende interne retningslinjer for drift og vedlikehold for eksempel av standard "online" brukerlisenser, og der regnskapsførerselskapet har lagt til grunn at risikoen er forsvarlig håndtert av systemleverandøren. I så fall må avtalen med leverandøren være så klar at det ikke er behov for supplerende interne retningslinjer i regnskapsførerselskapet og forholdet må inngå i regnskapsførerselskapets risikovurdering.

[8] GRFS punkt 2.8.4 og 2.8.5.
[9] GRFS punkt 2.1

For at de interne retningslinjene for drift og vedlikehold av IKT-systemer skal anses som forsvarlige, må enkelte sentrale forhold være dekket. 87 % svarte at de har retningslinjer for drift og vedlikehold. Hva retningslinjene dekker, fremkommer av følgende tabell:

Tabell 7:

Dekker retningslinjene eller eventuell utkontrakteringsavtale:	**JA (%)**	**NEI (%)**
Sikkerhetskopiering	99	1
Tilbakelegging av data	97	3
Oppdatering av programvare	97	3
Oppdatering av virusprogramvare	98	2
Sletting av tilgang til IKT-systemene ved opphør av ansettelsesforhold	91	9
At IKT-systemene til enhver tid ivaretar sikkerhetsmessige, lovmessige og driftsmessige krav	95	5
At eventuelle utkontrakteringsavtaler til enhver tid ivaretar sikkerhetsmessige, lovmessige og driftsmessige krav	79	21

** Alle spørsmålene måtte besvares. Manglende vurdering kan skyldes at regnskapsførerselskapet bare har en ansatt.*

Spørsmålet i tematilsynet dekket bare sletting av tilgang til IKT-systemene ved opphør av ansettelsesforhold. Sletting av tilgang til IKT-systemene ved opphør av kundeforhold der oppdragsgiver har hatt tilgang til regnskapsførerselskapets systemer, er imidlertid også svært viktig.

3.3.3 Endringer i IKT-systemer

Retningslinjer for endringshåndtering er et nødvendig risikoreduserende tiltak for å sikre en stabil, planlagt og forutsigbar drift. Slike retningslinjer bør omfatte alle endringer som kan påvirke IKT-systemene.

41 % opplyser at de ikke har retningslinjer for endringer i IKT-systemene. Forklaringen på at tallet er høyt, kan være at regnskapsførerselskapene ikke selv endrer systemene og at de ikke anser systemendringer som gjøres av leverandør for å være en risiko i egen virksomhet. Dette er uansett en risiko i regnskapsførerselskapet, jf. nærmere om utkontraktering i kapittel 4. Behovet for retningslinjer og hvordan disse skal utformes vil variere.

Spørsmålene i tematilsynet dekker sentrale elementer som normalt må inngå i de retningslinjene for endring av IKT-systemene som skal etableres i alle regnskapsførerselskaper.

Svarene fra de 59 % som opplyser å ha retningslinjer for endring av IKT-systemene, fremkommer av følgende tabell:

Tabell 8:

Dekker retningslinjene:	JA (%)	NEI (%)
At det skjer en vurdering av risikoen og konsekvensen av endringene før de gjennomføres	97	3
At vurderingen inkluderer eventuell betydning for sikkerhetsløsninger og nødvendig oppdatering av denne	96	4
Vurdering av tilgangskontroller	96	4
Testing	93	7
Opplæring	92	8
Dokumentasjon av endringen	84	16

Dokumentasjon av endringer vil bidra til å kunne avdekke om endringer i systemene kan være årsaken til feil og problemer som oppstår.

3.3.4 Håndtering av alvorlige driftsavbrudd

Alvorlige driftsavbrudd utgjør en risiko i regnskapsførerselskaper. Konsekvensene av ikke å kunne levere i henhold til oppdragsavtalene, kan bli store både for regnskapsførerselskapet og oppdragsgiverne. Regnskapsførerselskaper skal derfor ha en dokumentert plan for driftsavbrudd på IKT-området for å kunne håndtere driftsproblemer knyttet til maskin- og programvare.[10] (Beredskapsplan). Planen må oppdateres og den må være testet.

39 % opplyser at de ikke har en dokumentert plan for driftsavbrudd på IKT-området. Finanstilsynet forutsetter at de regnskapsførerselskapene som har svart at de ikke har en tilfredsstillende beredskapsplan, har bragt dette forholdet i orden og at planen er testet. Planen må oppdateres løpende.

For at en beredskapsplan skal være forsvarlig, må den dekke enkelte sentrale elementer og den må være oppdatert. Tematilsynet inneholdt derfor spørsmål for kontroll av dette.

Svarene fra de 61 % som opplyser at de har en dokumentert beredskapsplan fremkommer av følgende tabell:

Tabell 9:

Inneholder planen:	JA (%)	NEI (%)
Klare kriterier for når den skal iverksettes	93	7
Detaljert beskrivelse av hvordan gjenoppretting av IKT-systemene skal skje	87	13
Beskrivelse av når og hvordan ansatte skal informeres	83	17*
Beskrivelse av når og hvordan berørte oppdragsgivere skal informeres	81	19
Beskrivelse av hvordan driftskontinuitet skal sikres dersom ekstern IKT-leverandør skulle få problemer med å levere tjenestene	77	23
Krav til oppdatering av planen	81	19

** De som svarte at de hadde en dokumentert plan, måtte besvare spørsmål om hva den dekker. De som har svart nei på dette spørsmålet kan være selskaper med bare en ansatt.*

[10] GRFS punkt 2.8.5. og GRFS punkt 2.1.

At beredskapsplanen ikke virker som forutsatt er i seg selv en risiko. For at en beredskapsplan skal fungere som et risikoreduserende tiltak, må den derfor testes. Av de 61 % av selskapene som svarte at de har en dokumentert plan, er svarene på testing lite tilfredsstillende, jf. følgende tabell:

Tabell 10:

Testes planen:	JA (%)	NEI (%)
Årlig?	53	47
Ved større endringer?	60	40

3.3.5 Konklusjon

Svarene i tabell 4, jf. punkt 3.2, viser at mange regnskapsførerselskaper har inkludert sentrale elementer i grunnlaget for vurderingen av IKT-risikoen i regnskapsførerselskaper. Dette er bra. Det kan imidlertid stilles spørsmål ved kvaliteten av vurderingene ut fra de svarene som er gitt på hvilke risikoreduserende tiltak som er iverksatt, jf. omtalen i punkt 3.3 og tabellene 5 – 10. Etter Finanstilsynets syn vil forsvarlig vurdering normalt føre til en konklusjon om at det er behov for tilnærmet alle de risikoreduserende tiltakene som er dekket av spørsmålene. Flere av tiltakene er uansett et krav etter GRFS. Fordi GFRS utfyller lovkravet om "god regnskapsføringsskikk", er manglende gjennomføring av disse tiltakene et lovbrudd.

4 Særlig om utkontraktering

4.1 Generelt

Utkontraktering innebærer at deler av virksomheten utføres av andre enn regnskapsførerselskapet selv. Dette gjelder også dersom et regnskapsførerselskap setter ut hele eller deler av IKT-driften. Utkontraktering er særlig regulert i risikostyringsforskriften.[11]

Det er ofte knyttet løsninger for lagring av opplysninger og for drift til standardsystemer eller oppdragsstyringssystemer. Kjøp av slike tjenester innebærer at regnskapsførerselskapet har utkontraktert lagring og drift til systemleverandøren. Lagringen kan gjelde regnskapsinformasjon, oppdragsdokumentasjon eller annet. Også bruk av fildelings- og oppbevaringstjenester som ikke er knyttet til et system eller oppdragsstyringssystem[12], er utkontraktering.

Tematilsynet inneholdt spørsmål om regnskapsførerselskapet har utkontraktert hele eller deler av sin IKT-virksomhet. Forklaringen på at bare 68 % av regnskapsførerselskapene svarer at de har utkontraktert IKT-driften, er trolig at ikke alle regnskapsførerselskapene har et bevisst forhold til at deler av virksomheten faktisk er utkontraktert. I det følgebrevet som Finanstilsynet sendte ut til alle regnskapsførerselskapene i forbindelse med tematilsynet, ble det forklart at det også var utkontraktering når eksterne påtok seg lagring av opplysninger og drift. En eventuell misforståelse knyttet til hva som er utkontraktering er uheldig, fordi det kan forlede regnskapsførerselskapene til å tro at de ikke har ansvar også for den delen av virksomheten.

[11] Se § 5.
[12] For eksempel Jottacloud, Dropbox, OneDrive eller iCloud.

Av de 68 % av de regnskapsførerselskapene som svarer at de har utkontraktert IKT-virksomhet, viser tabellen under hvilke deler som er utkontraktert:

Tabell 11

Utkontraktert oppgave	Andel (%)
Lagring av oppdragsdokumentasjon	70
Lagring av regnskapsmateriale	71
Drift	94
Annet	39
Utkontrakterte oppgaver innenfor alle ovenfor nevnte områder	28

98 % av de som svarer at de har utkontraktert IKT-virksomhet har opplyst at de legger vekt på om leverandøren har tilstrekkelig kapasitet.

92 % svarer at de legger vekt på kompetanse.

83 % svarer at beslutningsgrunnlaget ikke inkluderer spørsmålet om leverandøren er sertifisert[13] eller spørsmålet om leverandørens revisor har avgitt en attestasjon knyttet til kontroller i systemleverandørens virksomhet [14]. Finanstilsynet mener at vurderingen av om tjenesteleverandørenes virksomhet er underlagt slik kvalitetstesting, bør inngå i beslutningsgrunnlaget for valg av tjenesteleverandør fordi det kan gi en sikkerhet for leveransen. Sertifisering innebærer imidlertid ikke i seg selv at alle lovmessige krav som gjelder for regnskapsførerselskaper er oppfylt.

4.2 Utkontrakteringsavtalene

Selv om hele eller deler av IKT-driften utføres av andre, er det regnskapsførerselskapet som i forhold til oppdragsgiver og andre fullt ut har ansvaret for at IKT-virksomheten oppfyller alle lovmessige krav som gjelder for en regnskapsførervirksomhet[15]. Dette ansvaret gjelder uavhengig av hvordan det kontraktsmessige ansvaret mellom regnskapsførerselskapet og leverandørene er regulert i avtalen dem i mellom.

Regnskapsførerselskapenes mulighet til å styre og kontrollere IKT-risikoen knyttet til utkontraktert virksomhet, vil være avhengig av hvilke rettigheter og plikter som fremgår av avtalene som inngås med systemleverandørene og andre det utkontrakteres til. En eventuell klargjøring og reforhandling av avtalene kan derfor være et viktig risikoreduserende tiltak. Finanstilsynet er innforstått med at det kan være vanskelig for et regnskapsførerselskap alene å kreve endringer i systemleverandørenes standardavtaler, men ansvaret for utkontraktert virksomhet påligger likevel regnskapsførerselskapet.

Finanstilsynet forutsetter at de regnskapsførerselskapene (8 %) som har svart at utkontrakteringsavtalene ikke foreligger skriftlig, har formalisert avtalene, jf. kravet om skriftlighet i risikostyringsforskriften.[16]

[13] For eksempel etter ISO 27001 informasjonssikkerhet
[14] ISAE 3402 som dekker kontroller hos en serviceorganisasjon
[15] God regnskapsføringsskikk (GRFS), punkt 2.8.6.
[16] Risikostyringsforskriften § 5 første ledd, annet punktum.

For å få en oversikt over hvilke rettigheter utkontrakteringsavtalen gir regnskapsførerselskapene og om det er et behov for klargjøring eller reforhandling, inneholder tematilsynet spørsmål rettet mot enkelte konkrete forhold som Finanstilsynet mener bør gjenspeiles i avtalene.

Finanstilsynet har sammenlignet svarene fra regnskapsførerselskapene med de 17 standardkontraktene som er innhentet fra flere av de mest brukte systemleverandørene. Disse standardavtalene dekker både bokføringssystemer, faktureringssystemer, årsoppgjør, ligningspapirer og lønn. Avtalene dekker også oppdragsstyringssystemer. Ut fra Finanstilsynets kunnskap om systemene gjennom tilsynsvirksomheten, også på andre områder enn regnskapsføreområdet, er det grunn til å tro at de innhentede avtalene langt på vei er representative, også for avtaler som benyttes av systemleverandører som valgte ikke å besvare Finanstilsynets henvendelse.

Finanstilsynets vurdering av standardavtalene avviker fra det regnskapsførerselskapene selv har svart, jf. punkt 4.2.1 – 4.2.4 i det følgende. Dette kan skyldes at enkelte regnskapsførerselskaper har forhandlet seg frem til vilkår som avviker fra de standardavtalene Finanstilsynet har mottatt. Finanstilsynet antar at det i så fall kun gjelder for et fåtall av regnskapsførerselskapene. Forklaringen kan være at regnskapsførerselskapene har tatt kontakt med sine systemleverandører, som da muntlig eller på annen måte har bekreftet at regnskapsførerselskapet har de rettighetene som Finanstilsynet etterspør, eller at de vil få det på anmodning. Selv om det fremkom i tematilsynet at spørsmålene gjaldt hva som faktisk sto i de avtalene som regnskapsførerselskapet hadde inngått, ser Finanstilsynet at fravær av de etterspurte kontraktsklausulene gjør det naturlig å kontakte den aktuelle systemleverandøren. Slik kontakt er positivt og særlig dersom regnskapsførerselskapene på denne måten har avklart forhold som ikke fremkommer uttrykkelig av avtalen. Finanstilsynet forutsetter at regnskapsførerselskapet i så fall følger dette opp overfor systemleverandøren slik at avklaringen eller rettigheten også formaliseres i avtalen eller i et tillegg til denne.

4.2.1 Avtaleklausuler om rett til innsyn og kontroll med den utkontrakterte virksomheten

For at regnskapsførerselskapets styre og ledelse skal kunne håndtere risikoen på IKT-området, må utkontrakteringsavtalene gi regnskapsførerselskapet rett til innsyn og kontroll med den utkontrakterte virksomheten.[17]

For at Finanstilsynet skal kunne gjennomføre hensiktsmessige tilsyn med regnskapsførerselskaper som har utkontraktert hele eller deler av IKT-virksomheten, må utkontrakteringsavtalene gi Finanstilsynet rett til opplysninger og tilsyn med den utkontrakterte virksomheten der Finanstilsynet finner det nødvendig.[18] Det er ikke bare rett til innsyn i opplysninger som regnskapsførerselskapene har lagret i systemet, men også rett til innsyn i selve systemene, inkludert den IKT-infrastrukturen som tjenesteleverandøren benytter seg av, og systemleverandørenes retningslinjer og rutiner.

[17] Risikostyringsforskriften § 5 første ledd
[18] Risikostyringsforskriften § 5 andre ledd

Regnskapsførerselskapenes vurdering av egne avtaler

Tabellen nedenfor viser regnskapsførerselskapenes vurdering av avtalene:

Tabell 12:

Avtalene er/gir rett til:	JA (%)	NEI (%)	DELVIS/IKKE ALLE (%)
Innsyn	66	25	9
Kontroll	69	25	6
Kreve at leverandør iverksetter tiltak	73	23	4
Opplysningsplikt ovenfor og tilsynsrett for Finanstilsynet	83	14	3
Opplysningsplikt for systemleverandør om endringer før de gjennomføres	76	17	7

Finanstilsynets vurdering av innhentede standardavtaler
Én av avtalene har en klausul som gir regnskapsførerselskapet rett til innsyn og kontroll hos systemleverandøren. De øvrige avtalene regulerer ikke forholdet.

Ingen av avtalene har en klausul som gir regnskapsførerselskapet rett til å kreve at systemleverandøren iverksetter tiltak for å sikre at systemet ivaretar krav som gjelder for regnskapsførerselskap.

Ingen av avtalene inneholder en klausul som gir Finanstilsynet rett til tilgang til opplysninger og tilsyn med den utkontrakterte virksomheten.

4.2.2 Avtaleklausuler om taushetsplikt og behandling av personopplysninger

Regnskapsførerselskaper er pålagt krav om taushetsplikt[19] og til behandling av personopplysninger[20]. Regnskapsførerselskapet skal inngå en databehandleravtale[21] med leverandør om behandling av personopplysninger.

Regnskapsførerselskapenes vurdering av egne avtaler
74 % av regnskapsførerselskapene svarer at utkontrakteringen av IKT-virksomhet innebærer at eksterne får tilgang til personopplysninger. 76 % opplyser at eksterne får tilgang til taushetsbelagt informasjon.

[19] Regnskapsførerloven § 10.
[20] Lov om behandling av personopplysninger av 14. april 2000 nr. 31, §§ 13 og 15 (heretter personopplysningsloven)
[21] https://www.datatilsynet.no/Sikkerhet-internkontroll/Databehandleravtale/

Tabellen nedenfor viser regnskapsførerselskapenes vurdering av om avtalene pålegger systemleverandørene samme taushetsplikt som gjelder for regnskapsførere, og om det inngås databehandleravtaler:

Tabell13:

Avtalene inkluderer:	JA (%)	NEI (%)	IKKE ALLE (%)
Taushetsplikt*	85	9	6
Databehandleravtale	56	40	4

**64 % svarer at avtalene pålegger leverandøren plikt til å varsle regnskapsførerselskapet dersom taushetsbelagt informasjon kommer på avveie. 5 % svarer at enkelte av de avtalene de har inngått pålegger leverandøren en slik plikt.*

Finanstilsynets vurdering av innhentede standardavtaler

Gjensidig taushetsplikt reguleres i ti av standardavtalene. To av avtalene regulerer kun regnskapsførerselskapets taushetsplikt ovenfor leverandøren. De øvrige avtalene regulerer ikke taushetsplikt.

I to av avtalene er det spesifisert at taushetsplikten også gjelder etter at avtalen er avsluttet. Ingen av avtalene spesifiserer at taushetsplikten medfører at leverandøren eller dennes medarbeidere ikke kan utnytte opplysninger i egen virksomhet eller i tjeneste eller arbeid for andre.

Behandling av personopplysninger er behandlet i ni av avtalene. I omlag halvparten av disse er ikke klausulene om behandling av personopplysninger dekkende i forhold til det som må inkluderes i en databehandleravtale.[22]

4.2.3 Avtaleklausuler om oppbevaring og tilgang

Utkontrakteringsavtalene inkluderer ofte lagring av elektronisk informasjon, herunder lagring av regnskapsførerselskapets oppdragsdokumentasjon og oppdragsgivers regnskapsmateriale. Regnskapsførerselskapene må sikre at utkontrakteringsavtalene gir regnskapsførerselskapet rett til oppbevaring av og tilgang til alt materialet i hele den perioden som er fastsatt i lov eller forskrift.[23] Dette innebærer at leverandøren må ha systemer for å kunne gjøre informasjonen tilgjengelig for regnskapsførerselskapet i hele oppbevaringsperioden. Systemleverandøren kan heller ikke ha tilbakeholdelsesrett i materialet.

Regnskapsførerselskapenes vurdering av egne avtaler

Tabell 14:

Gir avtalene rett til tilgang i hele oppbevaringsperioden for:	JA (%)	NEI (%)	IKKE ALLE (%)	DELVIS (%)
Regnskapsopplysninger med kontrollspor	70	4	2	24
Bokførte opplysninger (bilag/bokføringsgrunnlag)	63	3	2	32
Oppdragsdokumentasjon	72	3	1	24

[22] https://www.datatilsynet.no/Sikkerhet-internkontroll/Databehandleravtale/

[23] Forskrift om autorisasjon av regnskapsførere av 8. februar 1999 nr.196, § 3-2 og lov om bokføring av 19. november 2004 nr. 73, § 13.

Finanstilsynets vurdering av innhentede standardavtaler
Fem av avtalene regulerer oppbevaring og tilgang mens avtalen løper, ved at leverandøren har en plikt til å oppbevare data som er lastet opp eller produsert i systemet i henhold til gjeldende regelverk.

Elleve avtaler regulerer oppbevaring og tilgang ved avtalens opphør. Av disse gir fire av avtalene regnskapsførerselskapet rett til å få overført data eller kopi av data ved opphør. Tre av avtalene gir rett til fortsatt oppbevaring og tilgang mot betaling.

Fem av avtalene har ikke klausuler om oppbevaring og tilgang, verken i avtalens løpetid eller ved opphør.

4.2.4 Avtaleklausuler om opphør i særlige situasjoner

Med opphørsklausuler mener Finanstilsynet rett til å si opp avtalen. Det er viktig at regnskapsførerselskaper kan avslutte avtaler om levering av IKT-tjenester dersom tjenesten endres slik at regnskapsførerselskapet ikke kan oppfylle krav pålagt i lov og forskrift. Dette er særlig viktig dersom avtalen har lang ordinær oppsigelsestid.

Regnskapsførerselskapenes vurdering av egne avtaler

Tabell 15:

Opphørsklausul som særlig regulerer:	JA (%)	NEI (%)	IKKE ALLE (%)
Endringer som gjør at lovmessige krav ikke oppfylles	80	15	5
Urettmessig endring, herunder sletting	68	27	5
Urettmessig tilgang	65	27	8
Enkel gjenfinning	68	25	7
Lesbarhet og mulighet for etterkontroll	69	25	6
Mulighet for utskrift på papir ved elektronisk oppbevaring	69	27	4

Finanstilsynets vurdering av mottatte avtaler
Ingen av de mottatte avtalene har særlige klausuler som gir regnskapsførerselskapet en særlig rett til å heve avtalen på grunn av forhold som nevnt i forrige avsnitt. Finanstilsynet har ikke vurdert om det er naturlig å tolke enkelte av avtaleklausulene slik at de faktisk gir en særlig oppsigelsesrett ved ikke-oppfyllelse.

Svarene fra regnskapsførerselskapene kan skyldes at avtalene har en kort ordinær oppsigelsesfrist, og at de derfor ikke har vurdert behovet for en særlig oppsigelsesklausul.

4.2.5 Konklusjon

Etter Finanstilsynets syn er det behov for større bevissthet knyttet til det ansvaret regnskapsførerselskapene har for utkontraktert IKT-virksomhet og at avtalene er viktig for å kunne ivareta dette ansvaret. Finanstilsynet er kjent med at bransjeforeningene har iverksatt

arbeid for å sikre at avtalene på en bedre måte enn i dag setter regnskapsførerselskapene i stand til å ivareta sitt ansvar.

5 Oppsummering

IKT-risikoen er en risiko som skal håndteres i samsvar med risikostyringsforskriften. Svarene i tematilsynet viser at ikke alle regnskapsførerselskaper etterlever risikostyringsforskriften. Manglende risikostyring er alvorlig.

Videre er det uheldig hvis regnskapsførerselskapene oppfatter risikostyringsforskriften som et "formalkrav", fordi forskriften da ikke virker etter sin hensikt. Det er bare dersom det gjøres reelle vurderinger, ut fra den faktiske situasjonen i det enkelte regnskapsførerselskapet, at forskriften vil være et hjelpemiddel for styret og daglig leder til å ivareta det ansvaret de har etter regnskapsførerloven, selskapslovgivningen og annen relevant lovgivning. Etterlevelse av forskriften vil bidra til en forsvarlig risikostyring og internkontroll med hele regnkapsførerselskapets virksomhet, herunder IKT-driften enten den er utkontraktert eller ikke.

Det bildet tematilsynet gir, tilsier at en del regnskapsførerselskaper må gjøre grundigere vurderinger av behovet for å iverksette tiltak som kan redusere risikoen knyttet til de IKT-systemene som benyttes i virksomheten. Uansett må tiltak som skal iverksettes etter lovkravet om "god regnskapsføringsskikk" og GRFS, gjennomføres.

Tematilsynet gir også grunn til å tro at foreliggende avtaler mellom regnkapsførerselskapene og leverandører av IKT-systemer som selskapene benytter i sin virksomhet, ikke i tilstrekkelig grad gir regnskapsførerselskapene de rettigheter som er nødvendige for at de skal kunne oppfylle sine plikter etter lovgivningen, herunder ansvaret for risikostyring og internkontroll.

FINANSTILSYNET
Postboks 1187 Sentrum
0107 Oslo
POST@FINANSTILSYNET.NO
WWW.FINANSTILSYNET.NO