Høringsutkast til Norsk bokføringsstandard NBS 1

Sikring av regnskapsmateriale

(November 2012, oppdatert mars 2014 ~~og,~~ april 2015 og oktober 2024)

Innhold

1. Innledning og virkeområde

Bokføringsloven og ~~–~~ forskriften stiller krav til sikring av oppbevaringspliktig regnskapsmateriale. Disse kravene er i hovedsak overordnede, og gir liten veiledning om hvilke konkrete vurderinger den bokføringspliktige bør gjennomføre~~,~~ og hvilke sikringstiltak som bør iverksettes. Standarden omhandler kriterier som må oppfylles for at sikringen av regnskapsmaterialet skal anses å være betryggende.

Standarden omhandler
- generelle sikringstiltak,
- sikkerhetskopiering av elektronisk regnskapsmateriale, og
- lukking av regnskapsperioder ved elektronisk oppbevaring av bokførte opplysninger.

Denne standarden består av grunnleggende prinsipper og nødvendige handlinger (skrevet med uthevet skrift), med tilhørende veiledning i form av forklarende og annen tekst inkludert vedlegg. Grunnleggende prinsipper og nødvendige handlinger må leses i sammenheng med den forklarende og utfyllende teksten som gir veiledning for anvendelsen.

2. Lov og forskrift

Bokføringsloven § 4 nr. 9 krever at regnskapsmaterialet på en forsvarlig måte skal sikres mot urettmessig endring, sletting eller tap.

Etter bokføringsloven § 13 tredje og fjerde ledd skal oppbevaringspliktig regnskapsmateriale oppbevares ordnet og være betryggende sikret mot ødeleggelse, tap og endring. Regnskapsmaterialet skal i hele oppbevaringsperioden kunne fremlegges for offentlig kontrollmyndighet i en form som muliggjør etterkontroll, være tilgjengelig i lesbar form og kunne skrives ut på papir.

I henhold til bokføringsforskriften § 7-1 ~~første ledd~~ skal regnskapsmaterialet oppbevares på en måte som opprettholder lesekvaliteten i hele oppbevaringsperioden. Bokføringsforskriften § 7-2 stiller krav til sikkerhetskopiering av elektronisk regnskapsmateriale~~, og § 7-6 har krav om lukking av regnskapsperioder ved elektronisk oppbevaring av bokførte opplysninger~~. Når bokførte opplysninger oppbevares elektronisk, skal regnskapsperiodene lukkes innen de fristene som fremgår av bokføringsloven § 7 annet ledd, jf. bokføringsforskriften § 7-6 første ledd.

3. Begreper

Med «regnskapssystem» menes et system bestående av en eller flere komponenter som muliggjør produksjon av pliktig regnskapsrapportering, jf. bokføringsloven § 3, og spesifikasjoner av pliktig regnskapsrapportering, jf. bokføringsloven § 5, og som er innrettet slik at opplysningsplikten kan ivaretas.[1]

[1] Jf. bokføringsloven § 4 nr. 1.

Med «oppbevaringsløsning» menes et system bestående av en eller flere komponenter som benyttes til oppbevaring av regnskapsmateriale som skal sikres i samsvar med denne standarden. Oppbevaringsløsningen kan være en integrert del av regnskapssystemet eller en selvstendig løsning.

Med «multisky-løsning» menes å benytte mer enn to skyleverandører i den samlede oppbevaringsløsningen.

Blokkjedeteknologi, eller blockchain, er en måte å lagre data på i en digital journal som er spredt over mange datamaskiner. Hver "blokk" i "kjeden" inneholder en rekke godkjente transaksjoner, koblet sammen gjennom bruk av kryptografiske elementer (hash). Hver gang en ny transaksjon utføres, registreres den på hver brukers kopi av journalen, noe som gjør det nesten umulig å endre tidligere poster uten at alle kopier endres samtidig. En blokkjede kan inneholde oppbevaringspliktig regnskapsmateriale, for eksempel EHF-dokumenter[2], dokumentasjon av betalinger i kryptovaluta, utleggs- og reiseregninger og husleieavtaler med månedlige betalingsplaner.

Med «ASP» (Application Service Provider) menes en aktør som tilbyr digitale tjenester, for eksempel regnskapssystem og kontorprogramvare, samlet via internett på servere ASP-leverandøren kontrollerer. Brukeren får tilgang til alle nødvendige tjenester via ASP-innloggingen, i motsetning til skytjenester hvor brukeren går til de enkelte leverandørenes websider.

~~3.~~4. Omfanget av regnskapsmateriale som skal sikres

Sikring av regnskapsmateriale skal omfatte alt ~~oppbevaringspliktig~~ regnskapsmateriale som kreves oppbevart etter bokføringsloven ~~§ 13 første ledd og~~ , bokføringsforskriften og god bokføringsskikk.

Alt oppbevaringspliktig regnskapsmateriale etter bokføringsloven § 13 første ledd må sikres på en betryggende måte mot urettmessig endring, sletting, tap og ødeleggelse.
I tillegg inneholder bokføringsforskriften enkelte særskilte bestemmelser om oppbevaring, spesielt i kapittel 7 *Oppbevaring og elektronisk tilgjengelighet* og kapittel 8 *Tilleggsbestemmelser og særlige regler for enkelte næringer og bransjer.*
Sikringsbestemmelsene gjelder tilsvarende for regnskapsmateriale som kreves oppbevart med hjemmel i bokføringsforskriften.

Sikringsbestemmelsene gjelder også for regnskapsmateriale som kreves oppbevart etter god bokføringsskikk, herunder dokumentasjon av gjennomførte risikovurderinger for bokføringspliktige med elektronisk oppbevaring, jf. denne standardens punkt 7.2.5.

Regnskapsmateriale som ikke er oppbevaringspliktig etter ~~lov eller forskrift~~bokføringsloven, bokføringsforskriften og god bokføringsskikk, omfattes ikke av kravene til sikring.

[2] Salgsdokumenter i Elektronisk HandelsFormat.

Bokføringsforskriften § 7-7 annet ledd bestemmer at kravene til sikkerhetskopiering i § 7-2 gjelder tilsvarende for bokførte opplysninger som holdes elektronisk tilgjengelig etter bokføringsloven § 13b. I tillegg gjelder kravet i bokføringsforskriften § 7-1, som medfører at bokførte opplysninger som holdes elektronisk tilgjengelig skal lagres på en måte som opprettholder lesekvaliteten i hele lagringsperioden. Øvrige krav til sikring i ~~lov, forskrift~~bokføringsloven, bokføringsforskriften og denne ~~standard~~standarden gjelder ikke for bokførte opplysninger som utelukkende holdes elektronisk tilgjengelig etter bokføringsloven § 13b. Det henvises til NBS 3 *Elektronisk tilgjengelighet i 3,5 år* for ytterligere veiledning.

Dersom bokførte opplysninger oppbevares elektronisk som grunnlag for utarbeidelse av spesifikasjoner av pliktig regnskapsrapportering~~,~~ (jf. bokføringsloven § 13 første ledd nr. 2), gjelder kravene til sikring på samme måte som for annet oppbevaringspliktig regnskapsmateriale. I slike tilfeller vil det som et ledd i sikringen være krav om lukking av regnskapsperioder~~, jf.~~ etter bokføringsforskriften § 7-6, se punkt ~~89~~ i denne standarden.

~~4.~~5. Sikringsformål og sikringstiltak

Oppbevaringspliktig regnskapsmateriale skal sikres på en måte som forhindrer urettmessig endring, sletting, tap og ødeleggelse, eller på en måte som gjør det mulig å oppdage urettmessig endring, sletting tap eller ødeleggelse og å gjenskape regnskapsmaterialet. Gjenskaping skal skje på en måte som sikrer integriteten til regnskapsmaterialet.

Tiltak for sikring av oppbevaringspliktig regnskapsmateriale kan ha tre formål:

- Tilgjengelighet - sikre at regnskapsmaterialet er tilgjengelig for autoriserte personer ved behov.
- Integritet - sikre nøyaktighet og fullstendighet av regnskapsmaterialet, sikkerhet mot uautorisert endring og sporbarhet av endringer.
- Konfidensialitet - sikre at kun autoriserte brukere har tilgang til regnskapsmaterialet.

Manglende konfidensialitet vil ha liten effekt i forhold til ~~formålet~~de primære formålene med bokføringsreglene[3] ~~.~~, som er

- å etablere grunnlag for å produsere pliktig regnskapsrapportering og spesifikasjoner av denne regnskapsrapporteringen, og
- å muliggjøre kontroll av og innsyn i løpende transaksjoner og grunnlaget for pliktig regnskapsrapportering.[4]

Mulighetene til å produsere pliktig regnskapsrapportering og spesifikasjoner, og mulighetene til å kunne kontrollere bokføringen, svekkes normalt ikke ved at uautoriserte får innsyn i regnskapsmaterialet. Konfidensialitet som sikringsformål omtales derfor ikke i det videre. ~~Mangler knyttet til integritet og tilgjengelighet vil derimot påvirke oppfyllelsen av formålet med regelverket direkte.~~ Det gjøres likevel oppmerksom på at andre ~~regelsett~~regelverk kan inneholde krav til konfidensialitet for opplysninger som kan foreligge i det oppbevaringspliktige regnskapsmaterialet. Dette gjelder for eksempel

[3] ~~Jf. NOU 2002: 20 *Ny bokføringslov* punkt 11.5.3.~~
[4] Jf. NOU 2002: 20 *Ny bokføringslov* punkt 11.5.3, jf. punkt 4.1.4.

personopplysningsloven~~, personopplysningsforskriften, verdipapirhandelloven, forskrift om sikkerhetsgraderte anskaffelser mv.~~.[5]

Mangler knyttet til integritet og tilgjengelighet vil derimot påvirke oppfyllelsen av formålet med bokføringsregelverket direkte.

I bokføringsloven § 4 nr. 9 og § 13 tredje ledd er sikringsformålene knyttet til type hendelser som kan true regnskapsmaterialets integritet og tilgjengelighet. Hendelsene deles inn i

- endring ~~–~~ regnskapsmaterialet er tilgjengelig, men integriteten er ikke intakt,
- sletting ~~–~~ elektronisk regnskapsmateriale er ikke lenger tilgjengelig,
- ødeleggelse ~~–~~ regnskapsmaterialet er ikke tilgjengelig/lesbart på grunn av for eksempel brann eller vannskade, og
- tap - regnskapsmaterialet er ikke tilgjengelig på grunn av for eksempel tyveri.

Det finnes i utgangspunktet to grunntyper av sikringstiltak:

- Tiltak som forhindrer urettmessig endring, sletting, ødeleggelse og tap.
- Tiltak som oppdager og korrigerer urettmessig endring, sletting, ødeleggelse og tap (gjenskaper regnskapsmaterialet med integriteten i behold).

Sikringstiltak som skal sørge for at urettmessig endring, sletting, ødeleggelse og tap ikke forekommer, vil være *forhindrende* eller *preventive* sikringstiltak. I mange tilfeller vil forhindrende sikringstiltak være mindre kostnadskrevende enn korrigerende tiltak, i tillegg til at regnskapsmaterialet vil være tilgjengelig for kontroll til ~~en hver~~enhver tid. Et eksempel på et forhindrende tiltak er å begrense tilgang til å gjøre endringer i elektronisk regnskapsmateriale ved å innføre krav til brukernavn og passord.

Korrigerende sikringstiltak kjennetegnes ved at det i tillegg til å konstatere at urettmessig endring, sletting, ødeleggelse eller tap har funnet sted, konstateres at regnskapsmaterialet kan gjenskapes/gjenopprettes med integriteten i behold. Et eksempel på et korrigerende sikringstiltak er å legge tilbake en sikkerhetskopi etter harddiskkrasj. For elektronisk regnskapsmateriale finnes det sikringsalternativer hvor sporing og/eller logging kan benyttes til å avdekke endringer mv., og også til å gjenskape den opprinnelige informasjonen. Det er ut fra en kost-nytte vurdering ikke hensiktsmessig å stille krav til sporbarhet av endringer, så lenge forhindrende sikringstiltak er iverksatt. Sporing/logging kan likevel benyttes som sikringstiltak.

~~5.~~6. Grad av sikring

Den bokføringspliktige skal gjennomføre tiltak som reduserer risikoen for urettmessig endring, sletting, ødeleggelse og tap av oppbevaringspliktig regnskapsmateriale til et akseptabelt nivå.

[5] Lov 15.06.18 nr. 38 som gjennomfører EUs personvernforordning (GDPR) i norsk rett.

Betryggende oppbevaring innebærer at regnskapsmaterialet er sikret på en rimelig måte mot ~~tyveri, brann og annen~~ tilsiktet eller utilsiktet endring, sletting, ødeleggelse[6]~~.~~ eller tap.[7]

Det er i de fleste tilfeller ikke ~~snakk om en~~mulig å eliminere risiko for sletting, endring, tap eller ødeleggelse helt. Dette vil bli for byrdefullt og kostbart. At kravet til sikring ikke er absolutt ~~sikring, som kan være urimelig byrdefull og kostbar for den bokføringspliktige. Konklusjonen~~ følger også av ordlyden i bokføringsloven § 4 nr. 9 og § 13 tredje ledd, som krever henholdsvis «forsvarlig» og «betryggende» sikring. ~~Rimelig grad av sikring oppnås når risikoene for urettmessig endring, sletting, tap eller ødeleggelse av regnskapsmaterialet er redusert til et akseptabelt nivå.~~Sikringstiltak mot risikoer skal være tilstrekkelig til at den gjenværende risikoen er akseptabel.

Hva som er et akseptabelt risikonivå drøftes i punkt ~~6~~7.2.3.

~~6.~~7. Risikovurdering

Bokføringspliktige virksomheter har ulike risikoer knyttet til oppbevaringen av regnskapsmaterialet, og tiltakene som iverksettes for å sikre regnskapsmaterialet må tilpasses dette. Enkelte risikoer knyttet til oppbevaringen er likevel grunnleggende for de fleste virksomheter. For slike risikoer behøver hver enkelt virksomhet ikke nødvendigvis å gjennomføre egne vurderinger, men kan basere seg på et definert sett med risikoer og mulige sikringstiltak. Slike risikoer er definert i punkt ~~6~~7.1. For mer komplekse oppbevaringsløsninger vil det i større grad være nødvendig å gjennomføre egne risikovurderinger, og iverksette tilpassede sikringstiltak.

~~Kompleksiteten i oppbevaringsløsningen er avhengig av teknologien som benyttes, hvor det kan skilles mellom ulike oppbevaringsmedier.~~ En risikovurdering må ta høyde for den underliggende teknologien. Bruk av skytjenester for bokføring, med tilhørende oppbevaringsløsninger, er mer vanlig enn lokal digital lagring og fysisk oppbevaring på papir. Regnskapsmateriale vil også kunne oppbevares på ulike skytjenester den bokføringspliktige benytter, utover skytjenester for bokføring. En multisky-løsning kan være risikoreduserende (regnskapsmateriale spredt på flere løsninger), men kan også være risikoøkende ved at oppbevaringsstedet for de enkelte skyløsningene kan være uklart for den bokføringspliktige. Bruk av standardiserte løsninger som er anerkjente i markedet vil ofte ha en lavere iboende risiko enn egenutviklede løsninger eller løsninger med liten utbredelse. En oppbevaring på blokkjedeteknologi vil styrke integriteten til regnskapsmaterialet, med lavere risiko for manipulering av innholdet. Bruk av systemer for logging av endringer i regnskapsmateriale som oppbevares kan være risikoreduserende tiltak.

Risiko for tap av regnskapsmateriale kan oppstå som en effekt av trussel om cyberangrep. Løsepengevirus kan gjøre regnskapsmateriale utilgjengelig, kanskje også sikkerhetskopien. Rutiner og verktøy for å hindre cyberangrep vil være risikoreduserende tiltak. Hacking av IT-løsninger kan medføre endring i, ødeleggelse eller tap av regnskapsmateriale, både for

[6] ~~Jf. NOU 2002: 20 *Ny bokføringslov* punkt 3.2.6.2~~
[7] Jf. NOU 2002: 20 *Ny bokføringslov* punkt 3.2.6.2

originaler og sikkerhetskopier. Sikkerhetsløsninger mot hacking og atskilte sikkerhetskopier kan være risikoreduserende tiltak.

Det er vanligvis enklere å forhåndsdefinere risikoer og sikringstiltak for virksomheter som oppbevarer regnskapsmaterialet på papir, enn for virksomheter som benytter elektroniske oppbevaringsmedier. I det videre er det derfor skilt mellom

- oppbevaring på papir ~~eller papirlignende medier~~, med forhåndsdefinerte risikoer og mulige sikringstiltak
- elektronisk oppbevaring, hvor det bør gjennomføres en risikovurdering og iverksettes tilpassede sikringstiltak

En bokføringspliktig kan oppbevare deler av regnskapsmaterialet på papir ~~eller papirlignende medier~~, mens andre deler av regnskapsmaterialet oppbevares elektronisk. I slike tilfeller vil ulike krav gjelde for forskjellige deler av den bokføringspliktiges regnskapsmateriale, avhengig av oppbevaringsmedium ~~(~~, jf. punkt ~~6~~7.1 og ~~6~~7.2~~)~~.

~~6~~7.1 Oppbevaring på papir ~~eller papirlignende medier~~

Bokføringspliktige med oppbevaring på papir ~~eller papirlignende medier~~ skal i rimelig grad sikre regnskapsmaterialet mot

- **brannskade,**
- **vann- og fuktskader,**
- **fjerning,**
- **vanskelig gjenfinning - mangelfull orden i oppbevaringen, og**
- **manglende lesbarhet.**

~~**Ved oppbevaring på papirlignende medier skal den bokføringspliktige gjennomføre sikkerhetskopiering av regnskapsmaterialet.**~~

~~Ved oppbevaring av regnskapsmateriale på papir vil det være behov for enkelte sikringstiltak, selv om det normalt anses å være~~Det er normalt enklere å sørge for betryggende sikring av papirbasert regnskapsmateriale enn elektronisk regnskapsmateriale.

I vedlegg 1 finnes en del eksempler på sikringstiltak for bokføringspliktige med oppbevaring på papir, innenfor de ulike risikokategoriene. Disse risikoene og sikringstiltakene vil være aktuelle også for de fleste bokføringspliktige som benytter elektronisk oppbevaring, jf. punkt 7.2.

Kravet til sikring av regnskapsmateriale på papir mot manglende lesbarhet må ses i sammenheng med kravet i bokføringsforskriften § 5-13 om at dokumentasjon av bokførte opplysninger og dokumentasjon av balansen som utstedes på papir, skal utstedes med en papir- og trykkvalitet som sikrer lesbarheten i hele oppbevaringsperioden.

Bokføringspliktige som ~~benytter elektroniske medier som i stor grad kan likestilles med oppbevaring på papir, kan i utgangspunktet legge de samme kravene til grunn som ved oppbevaring på papir. Slike løsninger benevnes *papirlignende medier*. Dette vil gjelde elektronisk oppbevaring som innehar begge av de følgende egenskapene:~~

- Oppbevaring av elektroniske filer som har papirlignende egenskaper. Med dette menes at filene
  a) ikke er enklere å redigere enn oppbevarer regnskapsmateriale på papir (som kan skannes, redigeres og skrives ut på nytt),
  b) er direkte lesbare når de åpnes i standard programvare (programvare som er allment tilgjengelig, også for offentlig kontrollmyndighet), og
  c) enkelt kan skrives ut på papir.

  Dette vil typisk gjelde for billedfiler, for eksempel regnskapsmateriale som er lagret som eller skannet til pdf, jpg, tif eller lignende formater. Salgsdokumenter som oppfyller kravet i bokføringsforskriften § 5-2-9 om at salgsdokumenter som utstedes elektronisk skal utstedes i et filformat som ikke enkelt lar seg redigere i allment kjent sluttbrukerverktøy for tekstbehandling, regneark, e-post mv. uten at endringen fremgår direkte av salgsdokumentet, tilfredsstiller også kravet i bokstav a) over.

- Filer som nevnt i forrige punkt skal oppbevares på et ikke slettbart medium, slik at de ikke enkelt kan endres og/eller erstattes. Et eksempel på dette er bruk av DVD-R-plater. DVD-RW kan ikke brukes som oppbevaringsmedium, da innholdet på slike DVD-plater lar seg overskrive eller slette.

Bruk av papirlignende medier vil medføre behov for noen særskilte sikringstiltak, blant annet
- sikkerhetskopiering etter bokføringsforskriften § 7-2 (se punkt 6.2.6.4),
- oppbevaring av maskin- og programvare for lesing og utskrift av regnskapsmaterialet i hele oppbevaringsperioden, og
- vurdering av oppbevaringsmediets levetid.

Disse tre sikringstiltakene bidrar til å sikre lesbarhet og mulighet for etterkontroll av regnskapsmateriale som oppbevares på papirlignende medier.

I vedlegg 1 finnes en del eksempler på sikringstiltak for bokføringspliktige med oppbevaring på papir eller papirlignende medier, innenfor de ulike risikokategoriene. Disse risikoene og sikringstiltakene vil være aktuelle også for de fleste bokføringspliktige som benytter elektronisk oppbevaring, jf. punkt 6.2.

Bokføringspliktige som oppbevarer regnskapsmaterialet på papir eller papirlignende medier har ikke krav om å dokumentere en vurdering av risikoer knyttet til oppbevaring av regnskapsmateriale.

67.2 Elektronisk oppbevaring

Bokføringspliktige med elektronisk oppbevaring skal gjennomføre en risikovurdering. Risikovurderingen skal bestå av en oversikt over uønskete hendelser som utgjør en risiko knyttet til regnskapsmaterialets tilgjengelighet og integritet, med vurderingen beskrivelse av sannsynlighetsannsynligheten for og konsekvenskonsekvensene av at hendelsene. Videre skal risikovurderingen beskrive iverksatte tiltak inntreffer. Tiltak iverksatt for å redusere slik risiko til et akseptabelt nivå skal være inkludert i risikovurderingen.

~~Elektronisk oppbevaring av regnskapsmateriale omfatter all lagring på elektroniske medier som ikke faller inn under definisjonen av papirlignende oppbevaring i punkt 6.1.~~

For å sørge for betryggende sikring av elektronisk regnskapsmateriale, ~~vil~~er det ~~være~~ nødvendig å gjennomføre en vurdering av risikoen for urettmessig endring, sletting, tap eller ødeleggelse av regnskapsmaterialet. En risikovurdering er en vurdering av sannsynlighet for og konsekvens av uønskete hendelser som kan påvirke regnskapsmaterialets integritet og tilgjengelighet. Vurderingen vil normalt ta høyde for de tiltakene som er satt i verk for å redusere risikoen til et akseptabelt nivå.

Hvilket regnskapsmateriale som omfattes av risikovurderingen er definert i punkt ~~3~~4.

Risikovurderingens omfang og innhold tilpasses blant annet

- virksomhetens art og størrelse,
- omfanget av oppbevaringspliktig regnskapsmateriale,
- kompleksiteten av regnskapssystemet og tilhørende oppbevaringsløsning,
- valgte filformater og oppbevaringsmedier~~,~~ (harddisker, servere, virtuelle servere, skytjenester), og
- antall og type oppbevaringssteder, jf. for eksempel multisky-løsninger.

Den bokføringspliktige står fritt til å velge metode for risikovurdering, forutsatt at vurderingen omfatter sannsynligheter for og konsekvenser av uønskete hendelser, og beskriver iverksatte sikringstiltak.

Vedlegg 2 inneholder noen eksempler på risikoer som kan være aktuelle å vurdere. ~~Risikoene~~I tillegg er det ofte aktuelt å ta inn risikoene og sikringstiltakene som er beskrevet i vedlegg 1 ~~er ofte aktuelle å ta inn~~ som en del av risikovurderingen.

~~6~~7.2.1 Sannsynlighet

Fastsettelse av sannsynlighet innebærer vurdering av hvor ofte en uønsket hendelse inntreffer eller forventes å inntreffe. Vurderingen bør ta høyde for sikringstiltak som er innført for å forhindre at hendelsen inntreffer. Mulige sannsynlighetsutfall er som følger:

Lav sannsynlighet:	Hendelsen inntreffer aldri, eller forventes aldri å inntreffe.
Middels sannsynlighet:	Hendelsen inntreffer sjelden, eller forventes å inntreffe sjelden.
Høy sannsynlighet:	Hendelsen inntreffer ofte, eller forventes å inntreffe ofte.

Forventningen til hvor ofte en hendelse vil inntreffe påvirkes både av forhindrende sikringstiltak som er iverksatt og andre forhold, for eksempel erfaringer og statistikk.

~~6~~7.2.2 Konsekvens

Konsekvensvurderingen vil først og fremst omfatte i hvilken grad den bokføringspliktige kan gjenopprette regnskapsmaterialet etter at en uønsket hendelse har inntruffet. Gjenoppretting innebærer å gjøre regnskapsmaterialet tilgjengelig for kontroll, på en måte som sikrer integriteten. Vurderingen bør ta høyde for korrigerende sikringstiltak som er innført for å redusere konsekvensene av at hendelsen inntreffer.

~~Tidsaspektet~~Tidsbruk spiller en rolle i konsekvensvurderingen. Etter at det er avklart hvorvidt det er mulig å gjenopprette regnskapsmaterialet, må det vurderes hvor lang tid den bokføringspliktige vil bruke på gjenopprettingen. Det vil være forskjell på ~~hvorvidt regnskapsmaterialet kan gjøres tilgjengelig innen kort tid (for eksempel gjennom gjenoppretting fra sikkerhetskopi), eller om gjenopprettingen tar lenger tid (for eksempel gjennom gjenskaping fra ødelagte harddisker eller ny bokføring av transaksjoner og andre regnskapsmessige disposisjoner).~~om

- regnskapsmaterialet kan gjøres tilgjengelig innen kort tid, for eksempel gjennom gjenoppretting fra sikkerhetskopi, eller om
- gjenopprettingen tar lenger tid, for eksempel gjennom
  - gjenskaping fra ødelagte harddisker,
  - retting av feil på servere og virtuelle servere, eller
  - ny bokføring av transaksjoner og andre regnskapsmessige disposisjoner.

Mulige konsekvenskategorier er som følger:

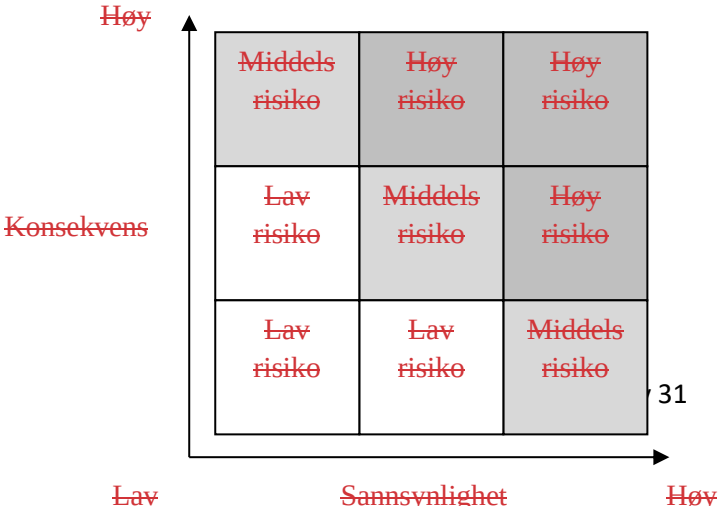
Lav konsekvens:	Regnskapsmaterialet kan gjenopprettes innenfor forholdsvis kort tid.
Middels konsekvens:	Regnskapsmaterialet kan gjenopprettes, men det tar noe mer tid.
Høy konsekvens:	Regnskapsmaterialet kan ikke gjenopprettes, eller kan gjenopprettes uten at integriteten kan verifiseres.

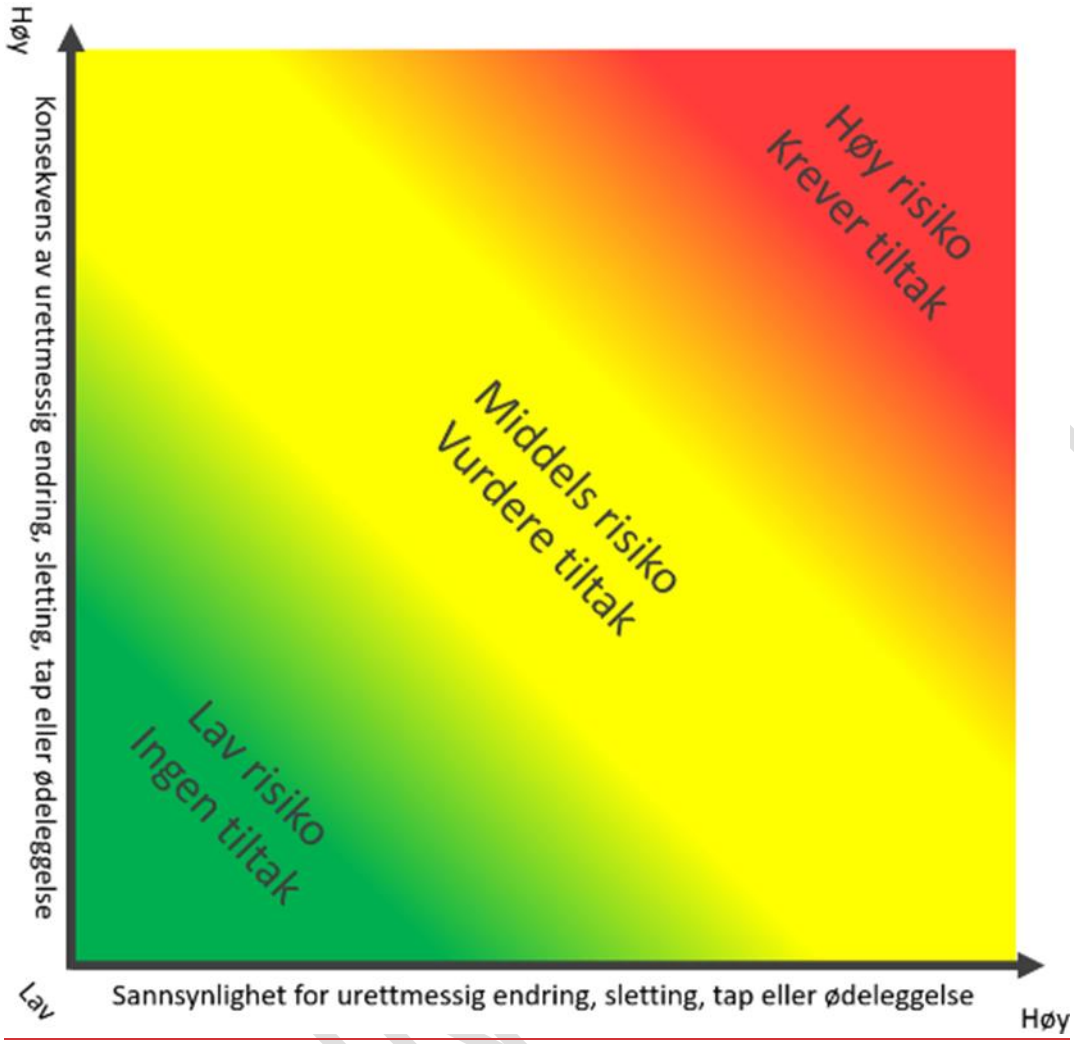
Hva som er kort tid for gjenoppretting er en vurderingssak, men offentlige kontrollmyndigheter bør normalt kunne forvente at regnskapsmaterialet legges frem innen noen dager etter en forespørsel. For uønskede hendelser som inntreffer mer enn sjelden bør sikringstiltakene medføre at regnskapsmaterialet kan gjenopprettes raskt~~, mens for~~. For uønskede hendelser som inntreffer sjelden eller aldri, vil det være akseptabelt at gjenoppretting tar noe lenger tid. Det bør kunne forventes at nyere regnskapsmateriale kan gjenskapes raskere enn eldre regnskapsmateriale. Dette vil for eksempel gjelde regnskapsmateriale for inneværende regnskapsår, som skal benyttes til utarbeidelse av årsregnskap, ~~ligningsoppgaver~~skattemeldinger og annen pliktig regnskapsrapportering.

~~6~~7.2.3 Akseptabelt risikonivå

For å gjennomføre en kvalifisert risikoanalyse må et akseptabelt risikonivå defineres, jf. punkt ~~5.~~6.

Det er den enkelte bokføringspliktige som definerer ~~et slikt nivå~~nivået for betryggende og forsvarlig sikring av regnskapsmaterialet. Følgende slutninger vil normalt trekkes basert på ulike kombinasjoner av sannsynlighet for og konsekvens av uønskede hendelser:





Lav risiko: Risiko for urettmessig endring, sletting, ødeleggelse og tap av oppbevaringspliktig regnskapsmateriale er på et akseptabelt nivå. Ytterligere tiltak er ikke nødvendig.

Middels risiko: Den bokføringspliktige bør vurdere ytterligere tiltak, og utdype hvordan risikoen vil reduseres til et lavt nivå. Alternative tiltak og kost-nytte bør vurderes.

Høy risiko: Risiko for urettmessig endring, sletting, ødeleggelse og tap av oppbevaringspliktig regnskapsmateriale er ikke på et akseptabelt nivå. Ytterligere sikringstiltak skal etableres.

Gjennomførte sikringstiltak for å redusere risikoen til et akseptabelt nivå skal dokumenteres som en del av risikovurderingen, jf. punkt 7.2.5.

Å definere akseptabelt risikonivå på denne måten innebærer ikke at avvik ikke kan inntreffe. Som beskrevet i punkt ~~5~~6 kreves det rimelig, ikke absolutt, sikring av regnskapsmaterialet. Det kan inntreffe hendelser hos alle bokføringspliktige ~~inntreffe hendelser~~ som er så spesielle at det ikke kunne forventes at risikovurderingen dekket disse (hendelser den bokføringspliktige ikke har forutsett), eller at etablerte sikringstiltak viser seg ikke å være like

effektive som forutsatt. Dette betyr i seg selv ikke at den bokføringspliktige ikke har gjennomført tilstrekkelig sikring av regnskapsmaterialet. I slike tilfeller bør den bokføringspliktige om mulig gjennomføre korrigerende tiltak for å håndtere den konkrete hendelsen som har inntruffet, samt revurdere risikoen knyttet til den uønskete hendelsen med henblikk på videre sikring av regnskapsmaterialet.

Et eksempel kan være at sikring mot sletting av bokførte opplysninger gjennomføres ved bruk av sikkerhetskopi. Det inntreffer et diskkrasj, hvor samtlige bokførte opplysninger blir slettet (kan ikke gjenopprettes). Til tross for at rutinene for sikkerhetskopiering har vært testet med gode resultater, fungerer ikke sikkerhetskopien når den behøves. Et korrigerende tiltak kan da være å ~~bokførte~~bokføre alle transaksjoner og andre regnskapsmessige disposisjoner på nytt, basert på dokumentasjonen av bokførte opplysninger. Deretter må det opprinnelige sikringstiltaket, som ikke fungerte, vurderes på nytt. Kanskje er det behov for ny maskin- eller programvare for sikkerhetskopiering, eller utvidet testing av rutinen for sikkerhetskopiering.

~~6~~7.2.4 Ajourhold av risikovurderingen

Risikovurderingen skal holdes à jour.

Dersom det skjer endringer i virksomheten som påvirker sikringen av regnskapsmaterialet, blir det nødvendig å oppdatere risikovurderingen. Eksempler på slike endringer kan være

- nye lokaler for oppbevaring av regnskapsmateriale,
- ~~bytte av system for elektronisk oppbevaring, eller~~
- bytte av regnskapssystem og/eller oppbevaringsløsning, herunder overgang fra regnskapssystem på egne servere til skytjenester,
- nye former for regnskapsmateriale, og
- nye rutiner for sikkerhetskopiering.

Det kreves kun ajourhold av risikovurderingen når det skjer endringer. Det kreves ikke periodisk ajourhold av risikovurderingen med faste intervaller, for eksempel årlig.

~~6~~7.2.5 Dokumentasjon av risikovurdering og sikringstiltak

Bokføringspliktige med elektronisk oppbevaring skal dokumentere gjennomførte risikovurderinger~~.~~ og sikringstiltak. Oppbevaringsperioden for dokumentasjonen følger av bokføringsloven § 13 annet ledd første punktum.

For å underbygge at regnskapsmaterialet er betryggende og forsvarlig sikret, ~~vil~~er det ~~være~~ nødvendig å dokumentere risikovurderingen som er gjennomført. Dokumentasjon av risikovurderingen ~~bør~~ oppbevares på samme måte som øvrig oppbevaringspliktig regnskapsmateriale.

Hvis leverandøren av oppbevaringsløsningen har gjort tilgjengelig en beskrivelse av risikoer og sikringstiltak knyttet til integritet og tilgjengelighet ved oppbevaring i løsningen, er det naturlig å bruke denne som grunnlag for den bokføringspliktiges egen risikovurdering.

Det vil i mange tilfeller være praktisk å oppbevare dokumentasjonen av risikovurderingen sammen med lignende former for dokumentasjon, for eksempel

- eventuell dokumentasjon av kontrollsporet etter bokføringsloven § 6 tredje ledd og NBS 2 *Kontrollsporet* punkt 3,
- dokumentasjon av rutinen for lukking av regnskapsperioder etter bokføringsforskriften § 7-6 annet ledd, som omhandlet i punkt ~~8~~9.8, og
- beskrivelse av kassasystem og lønnssystem etter bokføringsforskriften § 5-3-~~4~~15 tredje ledd og § 5-6 siste ledd.

~~6~~7.2.6 Elementer som påvirker behovet for sikring

Nedenfor er det konkretisert enkelte risikoforhold som ofte er relevante i forhold til sikring av regnskapsmateriale som oppbevares elektronisk. Det understrekes at den bokføringspliktige selv må gjennomføre egne vurderinger basert på virksomhetens type, omfang, lokalisering mv.

Det er ~~fem~~seks overordnede risikoforhold som påvirker behovet for sikringstiltak:
1. Oppbevaringsstedets beskaffenhet.
2. Fysisk tilgang til regnskapsmaterialet.
3. Logisk tilgang til regnskapsmaterialet.
4. Regnskapsmaterialets tilgjengelighet og lesbarhet.
5. Mulighet for gjenfinning av regnskapsmaterialet.
6. Bruk av skytjenester.

Videre har ulike oppbevaringsmedier karakteristika som påvirker risikobildet, og behovene for sikringstiltak:
- Frittstående PC ~~som ikke er i nett~~.
- PC eller server i nett (intranett og/eller internett), hos den bokføringspliktige eller hos ekstern leverandør (~~webhotell, ASP'er~~skytjenester, ASP mv.).
- Portabel disk, herunder eksterne harddisker og minnepinner.
- ~~CD/DVD-plate.~~

~~6~~

7.2.6.1 *Oppbevaringsstedets beskaffenhet*

Oppbevaringsstedet skal være egnet til betryggende sikring av elektronisk regnskapsmateriale.

Den bokføringspliktige bør utøve en normal aktsomhet mot skader forårsaket av fukt, brann, avmagnetisering, støv og lignende forhold som kan forringe lesbarheten til det elektroniske mediet i oppbevaringstiden.

Oppbevaringsstedet bør ikke være særlig risikoutsatt for vannskade. Oppbevaring av elektroniske medier bør ikke skje direkte på gulv, for å redusere risiko for vannskader. Dette er særlig aktuelt i områder med flomrisiko eller nær vannkilder som kan skade regnskapsmaterialet.

Oppbevaringsstedet bør ikke være særlig risikoutsatt for brann. Risiko for brann kan reduseres ved å ha ryddige oppbevaringslokaler, samt ved å fjerne åpne varmekilder og annet

som kan starte en brann. Et varslingsanlegg kan redusere konsekvensene av en eventuell brann ved at den blir oppdaget på et tidligere tidspunkt, og dermed ikke får like stort omfang. Der det benyttes vannbaserte brannslukkingssystemer (sprinkleranlegg) i lokalet, bør oppbevaringsmediet beskyttes for å begrense skader ved en vannbasert slukking.

Oppbevaring av elektroniske medier bør ikke skje i nærheten av magnetiske eller elektriske gjenstander som kan forringe lesekvaliteten over tid. Hvis det er risiko for ansamling av støv i lokalet, bør de elektroniske oppbevaringsmediene pakkes inn i egnet tett emballasje.

~~6~~Se punkt 7.2.6.6 om spesielle forhold ved bruk av skytjenester.

7.2.6.2 Fysisk tilgang til regnskapsmaterialet

Tilgang til oppbevaringsstedet

Oppbevaringsstedet skal være under den bokføringspliktiges kontroll, enten gjennom eierskap eller gjennom avtale, slik at tilgang kan begrenses til autoriserte personer.

Oppbevaringsstedet ~~bør~~skal være av en slik art at tilgang for allmennheten kan begrenses. Dette medfører at bruk av åpent tilgjengelige og usikrede lagerlokaler, uten muligheter for løpende tilsyn, ~~frarådes.~~ikke er tillatt.

Hvis den bokføringspliktige oppbevarer regnskapsmaterialet hos en ekstern part, bør tilgangen til oppbevaringsområdet begrenses til autoriserte personer hos den bokføringspliktige selv, og eventuelt autoriserte personer hos den eksterne parten.

I vedlegg 3 finnes eksempler på ulike oppbevaringssteder og fysiske sikringstiltak.

Se punkt 7.2.6.6 om spesielle forhold ved bruk av skytjenester.

Fysisk sikring av elektroniske oppbevaringsmedier

Elektronisk regnskapsmateriale skal sikres mot endring, sletting, tap eller ødeleggelse gjennom fysisk sikring av oppbevaringsmediet.

En PC eller en server antas å være tilstrekkelig sikret gjennom å være satt opp på et fast sted («koblet til veggen» med strømledning og nettkobling). ~~Det bør utvises større aktsomhet knyttet til en bærbar PC enn til en stasjonær PC.~~ Et eksempel på fysisk sikring av både bærbar og stasjonær PC er en ~~«Kensington Lock»,~~ vaier og kodelås som låser ~~fast~~ maskinen ~~med en vaier og kodelås~~ fast (for eksempel til et bord).

Mindre ~~,~~ og ikke minst portable ~~,~~ lagringsmedier bør oppbevares slik at de ikke kan observeres direkte, for eksempel i en skuff. I den grad det er mer enn et fåtall personer som har tilgang til lokalet, bør mediet låses ned eller sikres på tilsvarende måte.

Disse føringene kommer i tillegg til den generelle vurderingen av tilgang til oppbevaringsstedet.

~~6~~7.2.6.3 *Logisk sikring av elektronisk regnskapsmateriale*

Elektronisk regnskapsmateriale som oppbevares på PC, i nettverk, i en skytjeneste eller lignende, skal sikres mot endring eller sletting gjennom logisk sikring.

Logisk sikring dreier seg om å håndtere tilgang til systemer og informasjon, ut over den rent fysiske tilgangen til oppbevaringsmediet. Logisk sikring skjer normalt gjennom tilgangskontroller som styres av brukeridentifikasjon og tilhørende passord~~.~~, eventuelt kombinert med biometriske kontroller og multifaktorautentisering. Behov for logisk sikring vil imidlertid avhenge av hvilken type medium det elektroniske regnskapsmaterialet er lagret på.

Behovet for logisk sikring oppstår primært når regnskapsmaterialet er oppbevart på en PC eller server, enten de er frittstående, i nett, eller ~~på web-hoteller. For CD/DVD plater og for~~i skyløsninger. For portable disker (for eksempel eksterne harddisker og minnepinner) vil ikke behovet for logisk sikring være ~~tilstede~~til stede på samme måte. Her vil fysisk sikring være avgjørende, hvor en person først må skaffe seg adgang til oppbevaringsstedet, lokalisere og få tilgang til oppbevaringsmediet, for så å foreta fjerning, sletting eller endring av regnskapsmaterialet. ~~En problemstilling som tilsier~~En grunn til at det ikke anbefales å ha logisk sikring av frittstående elektroniske oppbevaringsmedier, er at administrasjon av brukeridentifikasjon og passord på slike medier er vanskelig å vedlikeholde i oppbevaringstiden. Online-systemer har normalt løpende opplegg for bytte av passord og administrasjon av brukeridentifikasjoner, med mulighet for overstyring av systemadministrator. På offline-medier vil ikke rutinene og kontrollen være tilsvarende, og det er mulig at passord ikke kan gjenfinnes for å få tilgang til det elektroniske regnskapsmaterialet i hele oppbevaringsperioden. Passord på offline medier vil med andre ord kunne redusere tilgjengeligheten til regnskapsmaterialet.

Elektronisk regnskapsmateriale for avsluttede regnskapsperioder kan holdes atskilt fra løpende bokføring ved å benytte en egen arkivkonto i systemet. Arkivkontoen bør kun ha som formål å beskytte tilgang til det elektroniske regnskapsmaterialet, og bør derfor ikke brukes til andre oppgaver. Det bør være begrensninger på hvem som får tilgang til arkivkontoen. Det optimale er at tilgang begrenses til en eller noen få personer utenfor regnskap og ledelse, dersom dette er praktisk gjennomførbart. Passordet til arkivkontoen bør ha en tilstrekkelig kvalitet, slik at det ikke kan gjettes, og bør endres regelmessig. Bruk av en separat arkivkonto medfører at det må en bevisst handling til for at en autorisert person skal kunne endre eller slette regnskapsmaterialet. Samtidig forhindrer den bokføringspliktige effektivt at uautoriserte personer får tilgang. Samme prinsipp vil gjelde for brukerkonto ~~på web-hotell~~i skyløsninger.

Uavhengig av om det benyttes en egen arkivkonto eller ikke, så bør tilgangen til det elektroniske regnskapsmaterialet begrenses til de som har tjenstlig behov for tilgang. Med tjenstlig behov menes at personen behøver tilgang til regnskapsmaterialet for å kunne utføre sitt arbeid. Det antas at flere personer vil ha tjenstlig behov for tilgang til regnskapsmaterialet før en regnskapsperiode avsluttes (innenfor ajourholdsfristen) enn etter at perioden er avsluttet. Videre antas behovet for tilgang å være ytterligere redusert etter utgangen av regnskapsåret, når årsregnskap og annen pliktig regnskapsrapportering er utarbeidet og

eventuell revisjon er gjennomført. ~~Mer enn tre til fire år etter utgangen av regnskapsåret er det normalt svært få personer som har tjenstlig behov for tilgang til regnskapsmaterialet.~~

Autoriserte personer er ofte nærmest til å manipulere det elektroniske regnskapsmaterialet. Dette kan for eksempel gjelde ledelsen, herunder regnskapsansvarlig. I større virksomheter vil det kunne etableres tilstrekkelig arbeidsdeling, slik at for eksempel IT-ansvarlig er den eneste som har tilgang til arkivet med regnskapsmateriale for avsluttede perioder. ~~IT-ansvarlig har normalt ingen direkte interesse i å modifisere det elektroniske regnskapsmaterialet, og har normalt ikke tilgang til å modifisere eventuelt annet regnskapsmateriale for å prøve å sikre samsvar mellom bokførte opplysninger og dokumentasjonen som underbygger opplysningene.~~ I mindre virksomheter kan det være vanskelig å skape denne arbeidsdelingen, men regnskapsmaterialet bør sikres gjennom arbeidsdeling på lik linje med nivået for arbeidsdeling på andre områder hos den bokføringspliktige.

~~6~~Se punkt 7.2.6.6 om spesielle forhold ved bruk av skytjenester.

7.2.6.4 Regnskapsmaterialets tilgjengelighet og lesbarhet

Den bokføringspliktige skal sikre at elektronisk regnskapsmateriale er tilgjengelig for kontroll, er lesbart og kan skrives ut på papir i hele oppbevaringsperioden.

Flere produsenter av elektroniske oppbevaringsmedier garanterer et visst antall år lesbarhet på sine produkter (for eksempel ~~DVD-plater).~~frittstående harddisker eller minnepinner). Hvis produsenten oppgir at perioden for lesbarhet er minst like lang som oppbevaringsperioden for regnskapsmaterialet, trenger ikke den bokføringspliktige å gjennomføre ytterligere handlinger enn å sikre at alt regnskapsmateriale er lagt over på mediet, og at regnskapsmaterialet kan leses. Hvis produsenten ikke garanterer at mediet er lesbart i hele oppbevaringsperioden, bør den bokføringspliktige sikre at regnskapsmaterialet kopieres fra gammelt til nytt medium i løpet av oppbevaringsperioden. Frekvensen av kopieringen avhenger av hvor lenge oppbevaringsmediet forventes å være lesbart. Det er den bokføringspliktige selv som har ansvaret for å undersøke hvor ofte en slik kopiering bør gjennomføres.

Sikkerhetskopiering i henhold til bokføringsforskriften § 7-2 er et sikringstiltak som alle bokføringspliktige med elektronisk oppbevaring er pålagt å ~~implementere:~~gjennomføre.

> ~~*«Det skal foreligge en sikkerhetskopi av elektronisk regnskapsmateriale.*~~
>
> ~~*Sikkerhetskopiering skal skje så ofte som virksomhetens og transaksjonenes art og omfang tilsier og innen ajourholdsfristene i bokføringsloven § 7 annet ledd. Sikkerhetskopien skal oppbevares adskilt fra originalen. Testing av sikkerhetskopien skal skje minimum en gang i året.*~~
>
> ~~*Dersom regnskapsmateriale er erstattet ved overføring av regnskapsinformasjon til elektronisk medium med hjemmel i bestemmelser i eller i medhold av bokføringsloven, skal originalt regnskapsmateriale oppbevares til det er tatt sikkerhetskopi av det elektroniske regnskapsmaterialet.*~~

~~Det *skal foreligge en fortegnelse over regnskapsmateriale som er sikkerhetskopiert, hvor ofte sikkerhetskopiering gjennomføres og hvor originalen og sikkerhetskopien oppbevares. Fortegnelsen skal oppbevares i fem år etter regnskapsårets slutt.*~~

~~*Reglene i bokføringsloven § 13 og § 13b, og i denne forskrift om oppbevaringspliktig regnskapsmateriale, oppbevaringssted, oppbevaringstid, sikring og elektronisk tilgjengelighet gjelder tilsvarende for sikkerhetskopien som for originalen.»*~~

Sikkerhetskopiering er i hovedsak sikring av tilgjengelighet til elektronisk regnskapsmateriale, i tilfelle originalen slettes, tapes eller ødelegges. Det er ikke stilt krav om noen spesifikk metode for sikkerhetskopiering, som kan skje ved inkrementell metode (tar kun med endringer fra forrige sikkerhetskopiering) eller ved full metode (alle data kopieres hver gang). Full metode kan være enklere ved gjenoppretting, men kreves ikke hvis gjenoppretting fra inkrementell metode også er testet med betryggende resultat.

Hvor ofte elektronisk regnskapsmateriale bør sikkerhetskopieres må avgjøres i det enkelte tilfelle~~. Som for ajourholdsplikten etter~~, men sikkerhetskopiering skal uansett skje innen ajourholdsfristene i bokføringsloven § 7 annet ledd~~ kan det nok~~, jf. bokføringsforskriften § 7-2 annet ledd. Som for ajourholdsplikten kan det forventes at store foretak med mange transaksjoner har løpende sikkerhetskopiering~~ (speiling).~~. De aller minste foretakene, med årlig ajourhold av bokføringen, forventes heller ikke å gjennomføre sikkerhetskopiering mer enn en gang i året. Mengden transaksjoner og andre regnskapsmessige disposisjoner som må gjenskapes ved et tap av data vil være sentral i vurderingen. Hvis originalen ødelegges, bør det straks lages ny kopi av sikkerhetskopien. Den opprinnelige sikkerhetskopien vil være «originalen» frem til dataene er gjenopprettet. Den bokføringspliktige har således til enhver tid to eksemplarer av elektronisk regnskapsmateriale.

Sikkerhetskopien skal etter bokføringsforskriften oppbevares fysisk adskilt fra originalen, for å forhindre at begge utgavene ødelegges eller tapes ved en uønsket hendelse. Det er ikke stilt nærmere krav til denne adskillelsen i forskriften, men den bokføringspliktige må vurdere om adskillelsen er tilstrekkelig til at sikkerhetskopien ikke blir ødelagt eller fjernet selv om originalen blir det (for eksempel ved brann, vannskade, tyveri mv.). Fysisk adskillelse kan for eksempel skje gjennom oppbevaring av sikkerhetskopien i et annet bygg enn originalen, i brann-, vann og innbruddssikkert skap, eller på andre måter.

Tilgjengelighet til elektronisk regnskapsmateriale fordrer at den bokføringspliktige i hele oppbevaringsperioden har tilgang til nødvendig maskinvare, programvare (herunder eventuelle lisenser) og kompetanse (brukerveiledninger mv). I løpet av oppbevaringsperioden kan både maskinvare, programvare og personell være byttet ut, og den bokføringspliktige bør forsikre seg om at eldre regnskapsmateriale fortsatt kan leses og skrives ut på papir.

~~6~~Den bokføringspliktige kan sette bort oppbevaringen av regnskapsmaterialet til andre, for eksempel en regnskapsfører, systemleverandør eller skyleverandør. I slike tilfeller må den bokføringspliktige sørge for at tilgangen til regnskapsmaterialet ikke begrenses i løpet av oppbevaringstiden, verken for den bokføringspliktige selv eller for offentlige

kontrollmyndigheter.[8] Dette skjer vanligvis gjennom tydelig avtaleregulering, herunder av hvordan tilgangen til regnskapsmaterialet skal sikres ved eventuell oppsigelse av avtalen.

Se punkt 7.2.6.6 om spesielle forhold ved bruk av skytjenester.

7.2.6.5 Mulighet for gjenfinning av regnskapsmaterialet

Gjenfinning av elektronisk regnskapsmateriale skal kunne skje på en enkel måte.

Oppbevaringspliktig regnskapsmateriale skal oppbevares ordnet. Dette gjelder også for elektronisk regnskapsmateriale.

Merking av oppbevaringsmedier er mest aktuelt for fysiske objekter som inneholder elektronisk regnskapsmateriale (~~CD, DVD~~ekstern harddisk, minnepinne mv.). Det bør være en ekstern merking av oppbevaringsmediet som indikerer hvilket regnskapsmateriale mediet inneholder, samt hvilket regnskapsår regnskapsmaterialet vedrører. Hvis elektronisk regnskapsmateriale oppbevares på PC, server eller ~~web-hotell~~i en skyløsning, bør det eksistere en logisk navngiving av kataloger (mapper~~).~~) eller på annen måte være enkelt å gjenfinne regnskapsmateriale for et konkret regnskapsår.

Uavhengig av hvilket elektronisk oppbevaringsmedium som velges, bør filer navngis på en måte som beskriver filens innhold - eventuelt gjennom bruk av tabeller som knytter filnavn til for eksempel identifikasjonskoder som er benyttet i bokføringen (bilagsnummer eller lignende).

Se punkt 7.2.6.6 om spesielle forhold ved bruk av skytjenester.

7.2.6.6 Bruk av skytjenester

Bruk av skytjenester hos eksterne leverandører kan medføre en lavere iboende risiko for urettmessig endring, sletting, tap eller ødeleggelse av regnskapsmateriale enn å ha egen server i egne lokaler eller å oppbevare regnskapsmateriale på andre elektroniske medier som harddisker.

Skyleverandøren har som oftest etablert gode sikkerhetspolicyer og -rutiner som den bokføringspliktige må benytte ved bruk av tjenesten. Kontroll av daglige driftsrutiner og oppfølging av avvik er også vanligvis godt ivaretatt hos eksterne leverandører av skytjenester.

En annen risikoreduserende faktor er at sikkerhetskopier normalt kun er tilgjengelig for skyleverandørens personale og ikke den bokføringspliktige, slik at risiko for at sikkerhetskopien ødelegges uforvarende er lavere.

[8] Den som påtar seg oppbevaringen har en selvstendig plikt til å gi offentlige kontrollmyndigheter nødvendig bistand til innsyn i regnskapssystemet og regnskapsmaterialet og stille til disposisjon utstyr og programvare for dette (jf. bokføringsloven § 14 annet ledd).

Leverandører av skytjenester har ofte etablert felles rutiner for sikkerhetskopiering og gjenoppretting for alle sine kunder. Den bokføringspliktige kan bygge på datasenterets erfaring med gjenoppretting, selv om gjenoppretting ikke er testet på den bokføringspliktiges eget regnskapsmateriale. Det bør innhentes en erklæring fra skyleverandøren selv om rutiner og testing av disse, eller at skyleverandøren viser til en ekstern bekreftelse på at rutinene fungerer (eksempelvis gjennom ISAE 3402 type 2 eller ISAE 3000-rapporter[9]).

Tilgangskontroller i skyløsninger, med unntak av dype administrasjonsrettigheter, er styrt av den bokføringspliktige selv. Dype administrasjonsrettigheter er normalt gitt til teknikere hos systemleverandører som har ansvar for å overvåke og vedlikeholde databaser. Den bokføringspliktige bør også i skyløsninger begrense tilgangen til oppbevaringspliktig regnskapsmateriale til de personene som har tjenstlig behov for tilgang, jf. punkt 7.2.6.3.

Flere nasjonale og internasjonale skyleverandører gir av sikkerhetsmessige årsaker ikke fysisk tilgang til datasenteret for deres kunder eller andre eksterne parter. Den bokføringspliktige må imidlertid gjennom avtaleregulering sørge for at den logiske tilgangen til regnskapsmaterialet ikke begrenses (se punkt 7.2.6.4 om regnskapsmaterialets tilgjengelighet og lesbarhet).

~~7.~~8. Tidsfrister for sikring

Oppbevaringspliktig regnskapsmateriale skal være løpende sikret mot endring, sletting, ødeleggelse og tap i hele oppbevaringsperioden.

Oppbevaringspliktig regnskapsmateriale ~~bør~~skal holdes løpende sikret, noe som for eksempel innebærer at

- brukernavn og passord for tilgang til regnskapssystemet er etablert før bokføringen påbegynnes, og vedlikeholdes i hele oppbevaringsperioden,
- tilgangen til oppbevaringsstedet er avklart, og om nødvendig begrenset, før regnskapsmaterialet settes der, og følges opp gjennom hele oppbevaringsperioden,
- rutiner og utstyr for brannsikring av oppbevaringsstedet foreligger før regnskapsmaterialet settes der, og vedlikeholdes gjennom hele oppbevaringsperioden, og
- merking av oppbevaringsmediet gjennomføres på det tidspunkt regnskapsmaterialet overføres til mediet, og oppdateres om nødvendig gjennom hele oppbevaringsperioden.

Dette medfører at det ikke vil eksistere noen gitt tidsfrist for når regnskapsmaterialet senest skal være betryggende sikret mot urettmessig endring, sletting, tap eller ødeleggelse. Sikring skal skje løpende fra utstedelse, mottak eller utarbeidelse av regnskapsmaterialet, og frem til utløpet av oppbevaringsperioden.

I tillegg eksisterer det egne krav til sikringstiltak, med særskilte tidsfrister:

- ~~sikkerhetskopiering etter~~Sikkerhetskopiering så ofte som virksomhetens og transaksjonenes art og omfang tilsier og innen ajourholdsfristene i bokføringsloven § 7 annet ledd, jf. bokføringsforskriften § 7-2~~,~~ (se punkt ~~6~~7.2.6.4).

[9] ISAE 3402 og ISAE 3000 er internasjonale standarder som benyttes av revisorer på attestasjonsoppdrag om henholdsvis kontroller hos en serviceorganisasjon og andre attestasjonsoppdrag som ikke er revisjon eller forenklet revisorkontroll av historisk finansiell informasjon. En ISAE 3402 type 2-rapport uttaler seg om både beskrivelsen, utformingen og effektiviteten av kontroller hos en serviceorganisasjon.

- ~~lukking~~Lukking av regnskapsperioder ~~etter~~innen fristene som nevnt i bokføringsloven § 7 annet ledd, jf. bokføringsforskriften § 7-6~~,~~ (se punkt ~~8~~9).

~~8.~~9. Lukking av regnskapsperioder

~~8~~9.1 ~~Valgfrihet mellom produksjon av spesifikasjoner og~~ Krav om lukking av regnskapsperioder

Bokføringspliktige som oppbevarer bokførte opplysninger elektronisk som grunnlag for utarbeidelse av spesifikasjoner av pliktig regnskapsrapportering, skal lukke regnskapsperiodene.

Det følger av bokføringsforskriften § 7-6 tredje ledd at bestemmelsene om lukking av regnskapsperioder ikke gjelder for bokføringspliktige som oppbevarer ferdig utarbeidede spesifikasjoner av pliktig regnskapsrapportering. Det eksisterer altså en valgfrihet, jf. også bokføringsloven § 13 første ledd nr. 2:

- ~~Produksjon~~Periodisk produksjon og oppbevaring av ferdige spesifikasjoner av pliktig regnskapsrapportering, uten krav til lukking av regnskapsperioder.
- Elektronisk oppbevaring av bokførte opplysninger som muliggjør senere produksjon av spesifikasjoner av pliktig regnskapsrapportering på forespørsel, med krav til lukking av regnskapsperioder.

~~8~~9.2 Formål

Lukking av regnskapsperioder skal skje på en måte som sikrer integriteten og tilgjengeligheten til de bokførte opplysningene i hele oppbevaringsperioden.

Bokføringsloven § 9 bestemmer at bokførte opplysninger ikke skal endres eller slettes etter at ajourholdsfristene som nevnt i § 7 annet ledd er utløpt. Bokføringsforskriften § 7-6 første ledd krever derfor at regnskapsperioder skal lukkes innen ajourholdsfristen.

Lukkingen skal skje på en måte som gir betryggende sikring mot endring eller sletting av bokførte opplysninger i hele oppbevaringsperioden etter bokføringsloven § 13 annet ledd første punktum. ~~Dette er en bestemmelse som i første rekke skal sikre integriteten til de bokførte opplysningene.~~

Bestemmelsene i bokføringsforskriften § 7-6 kommer i tillegg til øvrige sikringsbestemmelser i bokføringsloven, bokføringsforskriften og denne standarden, jf. særlig punkt ~~6~~7.2 om elektronisk oppbevaring.

89.3 Hva som skal lukkes

Lukking av regnskapsperioder skal omfatte alle bokførte opplysninger som er nødvendige for å kunne utarbeide spesifikasjoner av pliktig regnskapsrapportering og pliktig regnskapsrapportering.

Det fremgår av bokføringsforskriften at det er regnskapsperiodene som skal lukkes. Det er ikke tilstrekkelig å lukke hver enkelt bokført opplysning, da noe av formålet med bestemmelsen er å sikre at bokføringen for hver enkelt regnskapsperiode i sin helhet ikke endres etter utløp av ajourholdsfristen. Å lukke hver enkelt bokført opplysning i stedet for perioden, vil ikke gi sikkerhet for at det ikke bokføres ytterligere transaksjoner eller andre regnskapsmessige disposisjoner i regnskapssystemet etter utløpet av ajourholdsfristen.

Det følger av bokføringsloven § 13 første ledd nr. 2 at innholdet i lukkede regnskapsperioder skal omfatte alle bokførte opplysninger som er nødvendige for å utarbeide spesifikasjoner av pliktig regnskapsrapportering og pliktig regnskapsrapportering, jf. bokføringsloven § 7 første ledd. I praksis betyr dette at innholdet i lukkede regnskapsperioder defineres av kravene til innhold i spesifikasjoner av pliktig regnskapsrapportering etter bokføringsforskriften § 3-1, samt bransjebestemmelser i bokføringsforskriften kapittel 8[10].

89.4 Grad av sikring i lukkingsfunksjonen

Lukking av regnskapsperioder skal redusere risikoen for urettmessig endring eller sletting av bokførte opplysninger til et akseptabelt nivå.

Som drøftet i punkt 5 er formålet med sikring av oppbevaringspliktig regnskapsmateriale å gi rimelig – men ikke absolutt – sikring mot urettmessig endring, sletting, ødeleggelse og tap. Det vil være nærmest umulig å konstruere lukkings-, låsings- ellers sperringsmekanismer som ikke lar seg manipulere eller omgå ved ønske om å begå misligheter. Lukkingsmekanismen bør likevel være av en slik kvalitet at urettmessig endring eller sletting av bokførte opplysninger ikke kan skje uaktsomt, men krever en bevisst handling. Dette vil normalt gi et akseptabelt risikonivå for urettmessig endring eller sletting av bokførte opplysninger.

Et argument for ikke å kreve høyere grad av sikring i lukkingsmekanismen, er at bokførte opplysninger kan avstemmes mot pliktig regnskapsrapportering for perioden (for eksempel ~~omsetningsoppgaver~~skattemeldinger for merverdiavgift, ~~terminoppgaver~~a-meldinger, skattemeldinger for ~~skattetrekk~~inntekts- og ~~arbeidsgiveravgift, ligningsoppgaver~~formuesskatt eller årsregnskap). Avstemmingen vil avdekke om bokførte opplysninger er endret, men vil ikke alene være et fullgodt sikringstiltak, da muligheten for gjenoppretting med integriteten i behold ikke sikres.

Lukking vil normalt være et forhindrende sikringstiltak, som gjør at bokførte opplysninger ikke kan endres eller slettes etter utløp av ajourholdsfristen. I punkt ~~4~~5 drøftes i tillegg korrigerende sikringstiltak, hvor blant annet sporing og/eller logging kan benyttes til å

[10] Dette gjelder blant annet prosjektregnskaper i bygge- og anleggsvirksomhet og verftsindustri, jf. bokføringsforskriften § 8-1-3.

avdekke endringer mv, og også til å gjenskape den opprinnelige informasjonen. Korrigerende sikringstiltak, i form av sporing av endringer etter utløp av ajourholdsfristen, kan også tilfredsstille kravene til lukking av regnskapsperioder. Etter ajourholdsfristens utløp lukkes regnskapsperioden på en slik måte at alle etterfølgende endringer markeres særskilt, og kan spesifiseres i en egen rapport. Rapporten må vise både opprinnelig informasjon og endringene. På den måten vil det være full mulighet til å etterprøve endringer som er gjennomført etter utløpet av ajourholdsfristen, og gjenskape opprinnelige bokførte opplysninger. Dette tilsvarer det som kreves ved gjenåpning av regnskapsperioder, jf. punkt ~~8~~9.7.

~~8~~9.5 Risikovurdering og sikringstiltak

Den bokføringspliktige skal vurdere risikoen for urettmessig endring eller sletting av bokførte opplysninger, og om lukking av regnskapsperioder reduserer risikoen til et akseptabelt nivå.

Det er den bokføringspliktiges ansvar å sørge for at regnskapssystemet har en lukkingsfunksjon som gir betryggende sikring mot urettmessig endring eller sletting av bokførte opplysninger.

Et eksempel på sikringstiltak kan være at regnskapssystemet kun gir brukere med administrator-rettigheter tilgang til å gjenåpne lukkede regnskapsperioder, mens øvrige brukere kun har lesetilgang. En annen løsning kan være bruk av en egen brukerkonto med tilhørende passord for å gjenåpne lukkede regnskapsperioder. Denne brukerkontoen bør om mulig administreres av noen utenfor økonomi- og regnskapsfunksjonen. Arbeidsdeling bør skje på lik linje med nivået for arbeidsdeling på andre områder hos den bokføringspliktige, jf. punkt ~~6~~7.2.6.3. Dette vil være forhindrende sikringstiltak, som i rimelig grad sikrer at urettmessige endringer ikke forekommer.

~~8~~9.6 Perioder og tidsfrister

Lukking av regnskapsperioder skal skje innenfor ajourholdsfristene i bokføringsloven § 7 annet ledd ~~og bokføringsforskriften § 4-1.~~. For bokføringspliktige med krav til ajourhold ikke sjeldnere enn hver fjerde måned, skal lukking av regnskapsperioder uten pliktig regnskapsrapportering skje innen to måneder etter utløpet av perioden.

Lukking av regnskapsperioder skal etter bokføringsforskriften § 7-6 første ledd skje innen fristene for pliktig regnskapsrapportering, og uansett ikke sjeldnere enn hver fjerde måned. For bokføringspliktige med færre enn 600 bilag i året skal lukking av regnskapsperioder skje senest innen fristene for pliktig regnskapsrapportering, jf. bokføringsforskriften § 4-1 annet ledd.

For bokføringspliktige som har pliktig regnskapsrapportering sjeldnere enn hver fjerde måned, og som ikke faller inn under unntaket for bokføringspliktige med færre enn 600 bilag i året, krever bokføringsforskriften at regnskapsperiodene ikke lukkes ~~ikke~~ sjeldnere enn hver

fjerde måned. To måneder regnes som en romslig frist i denne sammenheng.[11] ~~.~~ Dette innebærer lukking minimum for følgende perioder og innen følgende frister:

- Regnskapsperioden fra januar til april lukkes innen 30. juni.
- Regnskapsperioden fra mai til august lukkes innen 31. oktober.
- Regnskapsperioden fra september til desember lukkes innen fristene for pliktig regnskapsrapportering, se ~~under~~nedenfor.

Pliktig regnskapsrapportering ~~etter merverdiavgiftsloven (omsetningsoppgaver) anses å medføre~~i form av skattemeldinger for merverdiavgift, medfører plikt til lukking av hele regnskapsperioden, slik at ingen transaksjoner eller andre regnskapsmessige disposisjoner kan bokføres, endres eller slettes i regnskapssystemet etter fristen for rapportering. Dette gjelder også transaksjoner som vedrører lønn mv, se ~~under~~nedenfor.

Månedlig regnskapsrapportering av lønnsopplysningspliktige ytelser, arbeidsgiveravgift og skattetrekk mv. i form av a-meldinger, medfører i seg selv ikke plikt til å ajourføre bokføringen, jf. bokføringsforskriften § 4-1 første ledd. Begrunnelsen for dette er at denne rapporteringen kan skje fra et ajourført lønnssystem uten at det er behov for å bokføre opplysningene. Det er dermed ikke nødvendig å sørge for særskilt lukking av regnskapsperioden hva gjelder opplysninger som inngår i a-meldingene, før regnskapsperioden som en helhet lukkes etter de generelle reglene.

Det bemerkes at dersom foretaket i tillegg har to-månedlig rapportering av merverdiavgift, skal også transaksjoner knyttet til lønn, arbeidsgiveravgift og skattetrekk mv. bokføres hver annen måned, og opplysningene inkluderes i den lukkingen som gjennomføres for regnskapsperioden.

Når bokføringspliktige har flere pliktige regnskapsrapporteringer med ulike frister, for eksempel ved regnskapsårets utløp, styrer som hovedregel fristen for siste pliktige regnskapsrapportering tidspunktet for lukking av regnskapsperioden. ~~Det er to unntak fra dette:~~

- ~~Det~~ ~~Rapportering etter skattebetalingsloven og folketrygdloven (a-meldinger).~~
- ~~Rapportering etter merverdiavgiftsloven (omsetningsoppgave for 6. termin, eventuelt årsterminoppgave eller årsoppgave).~~

er imidlertid et unntak fra dette. De deler av regnskapsperioden som inneholder bokførte opplysninger som inngår i ~~spesifikasjons~~spesifikasjonen av merverdiavgift, må lukkes innen ~~fristene~~fristen for pliktig regnskapsrapportering av merverdiavgift. ~~Dette~~ (skattemeldingen for merverdiavgift). For mange bokføringspliktige løses dette ved å for eksempel ha en regnskapsperiode 12 som kan lukkes når skattemeldingen for merverdiavgift for den siste perioden sendes inn (november og desember), og deretter en «periode 13» som benyttes til årsoppgjørsdisposisjoner mv. og som lukkes innen fristen for den siste pliktige regnskapsrapportering for perioden (normalt innen fristen for fastsettelse av årsregnskapet).

Kravet kan imidlertid skape utfordringer for bokføringspliktige som har et regnskapssystem hvor det ikke er praktisk gjennomførbart å skille ut de bokførte ~~opplysninger~~opplysningene

[11] Jf. NOU 2002: 20 *Ny bokføringslov* punkt 8.3.2.

som inngår i spesifikasjon av merverdiavgift. Utfordringen kan løses for eksempel ved at ~~spesifikasjon~~spesifikasjoner som nevnt i bokføringsloven § 5 første ledd og spesifikasjonen av merverdiavgift etter annet ledd nr. 1 for siste ~~termin~~skattleggingsperiode for merverdiavgift produseres, og de ferdige spesifikasjonene oppbevares utenfor regnskapssystemet som underlag for skattemeldingen for merverdiavgift. Lukking av regnskapsperioden som en helhet gjennomføres deretter innen fristen for siste pliktige regnskapsrapportering ~~(normalt innen fristen for fastsettelse av årsregnskapet).~~for perioden.

~~8~~9.7 Gjenåpning av regnskapsperioder

Gjenåpning av lukkede regnskapsperioder kan skje dersom ~~dette~~det er nødvendig for etterlevelse av bestemmelser gitt i eller i medhold av lov. Regnskapsperioden skal lukkes på nytt snarest mulig etter gjennomført bokføring. Gjenåpning og gjennomført bokføring skal dokumenteres særskilt.

Som nevnt i punkt ~~8~~9.2 er det i utgangspunktet ikke tillatt å endre bokførte opplysninger i en lukket regnskapsperiode, herunder å bokføre nye transaksjoner eller disposisjoner i perioden.

I enkelte tilfeller kan det likevel bli nødvendig å gjenåpne en lukket regnskapsperiode, for å etterleve andre bestemmelser. Et eksempel på dette kan være at det etter lukking av en ~~merverdiavgiftstermin~~skattleggingsperiode for merverdiavgift mottas ~~kjøpsdokument~~kjøpsdokumenter med dokumentasjonsdato i den lukkede perioden. Regnskapssystemet kan i noen tilfeller håndtere dette uten å gjenåpne regnskapsperioden, ved regnskapsmessig å registrere transaksjonen i en ny periode, men likevel tillate produksjon av ~~korreksjonsoppgave~~en ny skattemelding for merverdiavgift for den lukkede ~~terminen~~perioden (med en tilleggs-spesifikasjon av merverdiavgift). I regnskapssystemer uten slik funksjonalitet vil det i eksempelet være nødvendig å åpne den lukkede regnskapsperioden for å sikre korrekt periodisering av inngående merverdiavgift.

I punkt ~~8~~9.5 er det drøftet hvordan tilgang til gjenåpning av regnskapsperioder bør begrenses, og at arbeidsdeling om mulig bør implementeres. Videre vil det være sentralt å dokumentere bakgrunnen for gjenåpning, samt de endringer som gjennomføres i regnskapsperioden, slik at det er enkelt å spore de transaksjoner og disposisjoner som er bokført etter gjenåpning. Den bokføringspliktige velger selv hvordan denne dokumentasjonen utformes. Et eksempel kan være at regnskapssystemet har en funksjonalitet for å hente ut rapporter som viser alle gjenåpninger av lukkede regnskapsperioder, samt hvilke endringer som er gjort i forbindelse med gjenåpningen (sporing, jf. også omtale i punkt ~~8~~9.4).

Ny lukking bør gjennomføres så snart som mulig etter at nødvendig bokføring er gjennomført.

~~8~~9.8 Dokumentasjon

Den bokføringspliktige skal dokumentere regnskapssystemets funksjonalitet for lukking av regnskapsperioder, herunder hvordan lukkingen reduserer risikoen for urettmessig endring eller sletting av bokførte opplysninger til et akseptabelt nivå. Dokumentasjonen skal oppbevares så lenge bokføringsforskriften § 7-6 annet ledd krever.

Etter bokføringsforskriften § 7-6 annet ledd skal det foreligge en beskrivelse av regnskapssystemets funksjonalitet for lukking av regnskapsperioder, herunder hvordan lukkingen gir betryggende sikring mot endring eller sletting av bokførte opplysninger.

For å vise at betryggende lukking gjennomføres, skal det utarbeides og oppbevares en beskrivelse av hvordan lukkingen skjer, og hvordan den gir betryggende sikring mot endring eller sletting av bokførte opplysninger. Beskrivelsen bør i tillegg omfatte for eksempel

- hva som defineres som den oppbevaringspliktige utgaven av bokførte opplysninger,
- hvor bokførte opplysninger oppbevares og kan gjenfinnes, og
- hvilken maskin- og programvare som er nødvendig for å lese og skrive ut de bokførte opplysningene.

I mange tilfeller er dokumentasjon fra leverandøren av regnskapssystemet en naturlig del av beskrivelsen av regnskapssystemets funksjonalitet for lukking av regnskapsperioder. Slik systemdokumentasjon vil kunne vise hvordan regnskapssystemets lukkingsfunksjon er bygget opp for å forhindre endring eller sletting av bokførte opplysninger i avsluttede regnskapsperioder.

Dokumentasjon av lukkingsfunksjonen bør oppbevares på samme måte som øvrig oppbevaringspliktig regnskapsmateriale. Det er naturlig å inkludere dokumentasjon av lukkingsfunksjonen som en integrert del av dokumentasjonen av risikovurdering og sikringstiltak, se punkt ~~6~~7.2.5.

~~9.~~10. Ikrafttredelse

Standarden får virkning for oppbevaringspliktig regnskapsmateriale for regnskapsår som begynner 1. januar ~~2014~~2026 eller senere, men det oppfordres til tidligere anvendelse.

Vedlegg 1: Forhåndsdefinerte risikoer og eksempler på sikringstiltak for bokføringspliktige med oppbevaring på papir ~~eller papirlignende medier~~

Dette eksemplet er ment som en veiledning i forbindelse med kravet om sikker oppbevaring av regnskapsmateriale for bokføringspliktige med oppbevaring på papir ~~eller papirlignende medier.~~. Det er ikke forventet at den bokføringspliktige har alle eksempler på tiltak implementert, men at den bokføringspliktige har et rimelig sett av tiltak i forhold til virksomheten, oppbevaringsstedets beskaffenhet, lagringsmetode og tilgang til regnskapsmaterialet. Eksemplene er ikke uttømmende, den bokføringspliktige kan iverksette alternative sikringstiltak som oppfyller sikringsformålene på en tilfredsstillende måte.

Eksemplene gjelder for de som har oppbevaring på papir ~~eller papirlignende medier.~~. For bokføringspliktige med elektroniske oppbevaringsløsninger må det gjennomføres egne risikovurderinger, se eksempel i vedlegg 2.

Risiko	Sikringstiltak - eksempler
Generelt	
Brannskade	• Brannvarsler, eventuelt koblet mot vekter, brannvesen eller annen sentral • Brannslukkingsutstyr • Kontroll av elektriske anlegg • Atskillelse fra brannfarlige eiendeler eller andre risikofaktorer • Ryddige lokaler med adgangsbegrensninger
Vann- og fuktskader (flom, lekkasjer, brannslukking mv)	• Lufting ~~i forhold til~~for å redusere risiko for fuktskader • Oppbevaring i høyere etasjer eller sikre rom når oppbevaringsstedet er særlig utsatt for vannskade (flom mv). • Oppbevaring i skap eller lignende med tanke på lekkasjer fra tak, brannslukking med sprinkleranlegg mv
Fjerning av regnskapsmateriale (tyveri mv)	• Låste dører • Systemer for adgangskontroll • Alarmanlegg, eventuelt koblet mot vekter • Lokaler med adgangsbegrensninger
Vanskelig gjenfinning av regnskapsmaterialet - mangelfull orden i oppbevaringen (merking mv)	• Dedikerte oppbevaringssteder • Ryddige lokaler for oppbevaring • Tydelig merking av oppbevaringsmedier (regnskapsår, perioder, type materiale, intervall for bilagsnumre etc)
Manglende lesbarhet (trykk- og papirkvalitet mv)	• Oppbevaring utenfor sterkt sollys som kan gjøre regnskapsmaterialet uleselig

	• Ekstra kopier av regnskapsmateriale som i utgangspunktet har dårlig papir- eller trykkvalitet
~~**Risiko**~~	~~**Sikringstiltak – eksempler**~~
~~*Tillegg ved oppbevaring på papirlignende medier*~~	
~~Endring, sletting eller tap av elektronisk regnskapsmateriale~~	~~• Sikkerhetskopiering etter bokføringsforskriften § 7-2[12].~~ ~~• Sikkerhetskopien skal oppbevares atskilt fra originalen (fysisk)~~ ~~• Sikkerhetskopien skal testes for lesbarhet~~ ~~• Sikkerhetskopien skal være fullstendig (alt oppbevaringspliktig regnskapsmateriale).~~ ~~• Sikkerhetskopiering skal skje innenfor ajourholdsfristene for bokføringen.~~ ~~• Det skal foreligge en fortegnelse over regnskapsmateriale som er sikkerhetskopiert, hvor ofte sikkerhetskopiering skjer og hvor original og sikkerhetskopi oppbevares.~~ ~~• Bruk av oppbevaringsmedium med minst like lang holdbarhet som oppbevaringsperioden for regnskapsmaterialet (eventuelt jevnlig kopiering til nytt medium).~~
~~Manglende lesbarhet av elektronisk regnskapsmateriale~~	~~• Oppbevaring av programvare som er nødvendig for å lese regnskapsmaterialet i hele oppbevaringsperioden (for eksempel Adobe Reader for lesing av pdf-filer) – eventuelt med nødvendige lisenser for bruk.~~ ~~• Oppbevaring av maskinvare som er nødvendig for å lese og skrive ut regnskapsmaterialet på papir i hele oppbevaringsperioden.~~ ~~• Oppbevaring av dokumentasjon (for eksempel brukerhåndbøker) som er nødvendige for å kunne gjenfinne, lese og skrive ut regnskapsmaterialet i hele oppbevaringsperioden.~~

~~[12] Sikkerhetskopiering etter bokføringsforskriften § 7-2 er pliktig for alle bokføringspliktige med elektronisk oppbevaring av regnskapsmateriale.~~

Vedlegg 2: Eksempel på risikovurdering for bokføringspliktige med elektronisk oppbevaring

Følgende er kun ment som et eksempel på en risikovurdering, og kan ikke legges til grunn som en ferdig vurdering for en bokføringspliktig virksomhet. Ikke alle hendelser i eksemplet vil være relevante for alle bokføringspliktige, men eksemplet er heller ikke uttømmende. Eksemplet viser en nettovurdering (altså hvor risiko er vurdert etter å ta ha tatt hensyn til implementerte sikringstiltak). Risikovurderingen kan også være en bruttovurdering, hvor risiko vurderes før det tas hensyn til implementerte sikringstiltak, som deretter beskrives.

ID	Hendelse	Sannsynlighet	Konsekvens	Risiko
1	Uautorisert endring av regnskaps-materiale	Kun brukere med bruker-ID har tilgang til regnskapssystemet (tilgangskontroll). Regnskapsperiodene lukkes etter utløp av ajourholdsfristen. Kun regnskapssjef kan gjenåpne perioder. Det er ikke implementert arbeidsdelingsstruktur i økonomisystemet. Antar derfor at det er mulig å gjøre feil bevisst eller ubevisst. Sannsynlighet = middels	Uautoriserte endringer vil svekke integriteten i regnskapsmaterialet, og kan være vanskelig å oppdage. Dette vil medføre feil i bokførte opplysninger og pliktig regnskaps-rapportering. Mulighet for å forbigå lukking av regnskapsperioder. Konsekvens = høy	Risiko = høy Dette er over akseptabelt risikonivå og det er etablert et prosjekt for å implementere en arbeidsdelingsmatrise i økonomisystemet. Forbedret rutine for lukking av regnskapsperioder kommer i neste versjon av økonomisystemet.
2	Konvertering	Bokførte opplysninger ble konvertert ~~i 2008~~et par år siden fra gammelt regnskapssystem. Det ble ikke foretatt en formell godkjenning av de konverterte dataene. Historiske data kan derfor inneholde feil. Det er oppdaget 2 forekomster av saldofeil så langt. Sannsynlighet = høy	Feil i konverterte data kan gi feil i data som hentes ut for ledelsesformål, revisjon eller kontroll fra offentlige myndigheter Konsekvens = middels	Risiko = høy Det bør igangsettes et prosjekt for å kvalitetssikre de bokførte opplysningene i regnskapssystemet, gjennom å sammenligne disse mot produserte spesifikasjoner av pliktig regnskapsrapportering. Ved eventuelle fremtidige konverteringer vil det bli gjennomført en formell godkjennelse

				av konverterte data for å forhindre feil.
3	Disk-krasj	Harddisker ryker i gjennomsnitt hvert 5 år. Det kjøres speiling med flere harddisker. At flere disker ryker samtidig, er lite sannsynlig. Sannsynlighet = lav	En ødelagt disk vil ikke gi nedetid, da server er satt opp med RAID 1 (speiling) Konsekvens = lav	Risiko = lav
4	Hendelse	Sannsynlighet =	Konsekvens =	Risiko =
5	Hendelse	Sannsynlighet =	Konsekvens =	Risiko =
6	Hendelse	Sannsynlighet =	Konsekvens =	Risiko =

Vedlegg 3: Eksempler på fysisk sikring av regnskapsmateriale – tilgang til oppbevaringsstedet

Eksempel 1
En sushi-bar kan ha et lokale for kunder, og et bakrom/lager ment kun for de ansatte. Det er å anta at kunder i lokalet ikke har allmenn tilgang til bakrommet, men det er heller ikke spesielt sikret eller låst. Oppbevaring av regnskapsmateriale i bakrommet må kunne anses som tilfredsstillende så lenge det er begrenset hvem som har tilgang til bakrommet. Begrensningen skjer gjennom ansattes generelle overvåkning av aktiviteter i lokalet i åpningstiden.

Spørsmålet blir om det er tilstrekkelig å oppbevare det elektroniske regnskapsmaterialet hvor som helst i bakrommet, eller om kreves ytterligere sikringstiltak. Her vil løsningen avhenge av medietypen som det elektroniske regnskapsmaterialet oppbevares på (for eksempel papir, server, ~~DVD,~~ minnepinne eller annet).

Eksempel 2
Den bokføringspliktige leier fysisk plass hos en profesjonell arkivtilbyder. Allmennheten har tilgang til fellesområder, men hver leietaker har sin «bod». Tilgang til den del av arkivlokalet som er den enkelte bokføringspliktiges område er begrenset til den bokføringspliktige selv, samt eventuelt autoriserte personer hos utleier. Dette anses å utgjøre tilstrekkelig fysisk sikring av tilgangen til oppbevaringsstedet. Oppbevaring i fellesområder anses ikke å utgjøre tilstrekkelig sikring.

Eksempel 3
Den bokføringspliktige oppbevarer papirdokumentasjon og elektroniske medier i en låve sammen med andre bokføringspliktige. Først bør låvens beskaffenhet vurderes i forhold til for eksempel brann, fuktskader og støvskader på elektroniske medier. Om disse forholdene anses å være tilfredsstillende, skal materialet oppbevares innelåst i et eget rom i låven, slik at andre ikke har allmenn tilgang til materialet (herunder de andre bokføringspliktige som leier oppbevaringsplass på låven).

Eksempel 4
Et stort foretak har betydelige mengder med elektronisk regnskapsmateriale. Det er mange personer som jobber i foretakets lokaler. Til forskjell fra butikken med bakrommet i eksempel 1, vil risikoen for uautorisert tilgang være større, og det må derfor stilles større krav til fysisk sikring av mediene enn hva som er tilfellet for butikken. Det forventes at oppbevaringslokalene er låst, og at det er kontroll med hvem som har tilgang til de deler av lokalet hvor mediene oppbevares.

Eksempel 5
En bokføringspliktig oppbevarer regnskapsmateriale i et anerkjent regnskapssystem som er en skytjeneste. Den bokføringspliktige innhenter en erklæring fra leverandøren av skytjenesten om rutiner for sikkerhetskopiering og gjenoppretting. Tilgangskontroller knyttet til oppbevaringspliktig regnskapsmateriale er basert på tjenstlig behov. Det blir logget hvem som har vært inne på området med oppbevaringspliktig materiale og loggen viser også om det er utført endringer i regnskapsmaterialet.