Direktoratet for høyere utdanning og kompetanse

Temarapport 2021
– informasjonssikkerhet og personvern i høyere utdanning og forskning

Ledelsens styring og kontroll av arbeidet med informasjons-sikkerhet

Innhold

Sammendrag

Den øverste ledelsen i virksomheten har ansvaret for overordnet styring og kontroll av arbeidet med informasjonssikkerhet. Det skal skje som en del av virksomhetens ledelsessystem for informasjonssikkerhet.

Ledelsens gjennomgang er den viktigste arenaen toppledelsen har for å utøve sin styring og kontroll. I dette status- og planleggingsmøtet er det meningen at toppledelsen skal bestemme rammene for, holde seg informert om og følge opp virksomhetens arbeid med informasjonssikkerhet.

I denne temarapporten drøftes i hvilken grad og på hvilke måter ledelsens gjennomgang gjennomføres i de 30 virksomhetene i universitets- og høgskolesektoren som omfattes av Kunnskapsdepartementets policy for informasjonssikkerhet og personvern.

Datagrunnlaget for rapporten er Unit/HK-dir sin kartlegging av disse virksomhetenes arbeid med informasjonssikkerhet og personvern, gjennomført i 2020 (direktorater og selskaper) og 2021 (universiteter og høgskoler).

De viktigste funnene

- 20 av de 30 virksomheter opplyste om at ledelsens gjennomgang ble gjennomført i løpet av det siste året. 15 av de 20 virksomhetene var universiteter og høgskoler. De siste fem var direktorater og selskaper.
- Fire av de 20 virksomhetene som gjennomførte ledelsens gjennomgang, opplyste om at gjennomgangen ble avholdt to eller flere ganger det siste året. 16 virksomheter opplyste om at ledelsens gjennomgang ble gjennomført én gang.
- Sju av de 10 virksomhetene som oppga at ledelsens gjennomgang ikke ble gjennomført det siste året, oppga at de enten hadde rutiner for ledelsens gjennomgang og at den hadde vært avholdt tidligere, eller at de involverte ledelsen på andre måter.
- Samtlige 20 virksomheter som gjennomførte ledelsens gjennomgang i det siste året, opplyste om at toppledelsen faktisk deltok på gjennomgangen.
- De vanligste temaene som ble behandlet på ledelsens gjennomgang var virksomhetenes risikostyringsprosess, gjennomførte risikovurderinger, brudd på informasjonssikkerheten i virksomhetene, iverksetting av ulike typer sikringstiltak og avvik fra egne sikkerhetsrutiner.
- 10 av de 15 universitetene og høgskolene som gjennomførte ledelsens gjennomgang det siste året, opplyste om at de rapporterte videre til universitets- eller høgskolestyret om status for og prioriteringer i arbeidet med informasjonssikkerhet.

Disse funnene kan indikere at i deler av sektoren er arbeidet med informasjonssikkerhet forankret på toppledernivå og i ferd med å bli en del av den øvrige virksomhetsstyringen.

Samtidig ser vi at antallet virksomheter som opplyser om at ledelsens gjennomgang gjennomføres er en del høyere enn antallet virksomheter som i vesentlig grad har styrket arbeidet med informasjonssikkerhet de siste par årene. Vi mener derfor at det i enkelte deler av sektoren kan være behov for å forbedre styringskraften i ledelsens gjennomgang ytterligere.

Forslag til gjennomføring

For å styrke styringskraften i ledelsens gjennomgang, mener vi at det kan være behov for å tilpasse gjennomgangen enda bedre til den rollen toppledelsen er ment å spille i arbeidet med informasjonssikkerhet. Det betyr, slik vi ser det, at gjennomgangen bør gi toppledelsen en oversikt over status for arbeidet og et grunnlag for å gjøre overordnede prioriteringer med hensyn til den videre innsatsen.

Med dette som utgangspunkt, foreslår vi at ledelsens gjennomgang struktureres rundt følgende seks agendapunkter:

1. Kunnskapsdepartementets policy for informasjonssikkerhet og personvern i høyere utdanning og forskning.
2. Anbefalinger og tilbakemeldinger fra Kunnskapsdepartementet og HK-dir.
3. Brudd på informasjonssikkerheten og avvik fra egne sikkerhetsrutiner.
4. Risikostyring – vurderinger av risiko og etablering av tiltak.
5. Håndtering av alvorlige hendelser, beredskap og kontinuitet.
6. Ressursers- og kompetansebehov.

Under hvert agendapunkt har vi utarbeidet noen hjelpespørsmål. Hjelpespørsmålene er ment å konkretisere innholdet i de ulike agendapunktene.

Om tema-rapportene

HK-dir sine temarapporter retter søkelyset mot viktige områder i arbeidet med informasjonssikkerhet og personvern i UH-sektoren. De publiseres vanligvis hver høst.

Målgruppene for temarapportene er alle i sektoren som jobber med, har lederansvar for eller er interessert i spørsmål om informasjonssikkerhet og personvern.

I tillegg til å gi informasjon om utvalgte temaområder, kan virksomhetene benytte rapportene til å vurdere inn-retningen og kvaliteten på eget arbeid, eller eget ståsted sett opp mot den generelle tilstanden i sektoren.

Innledning

Det er den øverste ledelsen, for eksempel rektor eller direktør, som har det overordnede ansvaret for informasjonssikkerheten i virksomheten.

Ansvaret innebærer at digitale verdier – infrastruktur, applikasjoner, tjenester, IT-utstyr, personopplysninger og andre typer informasjon – er tilfredsstillende sikret. Verdiene skal blant annet sikres mot uautorisert tilgang og tyveri, skade eller ødeleggelse, og misbruk, for eksempel at datamaskiner benyttes til utvinning av kryptovaluta eller til å gjennomføre angrep mot andre virksomheter.

Ledelsen må også sørge for at digitale verdier er tilgjengelige for bruk, og at ulike typer nettsvindel forebygges, for eksempel direktør- eller fakturasvindel.

Den øverste ledelsens ansvar for informasjonssikkerheten øker i takt med at digitale verdier blir stadig viktigere innenfor UH-sektorens kjerneområder (utdanning, forskning, administrasjon og formidling). Avhengigheten av disse verdiene er nå såpass stort at det dreier seg om sektorkritisk infrastruktur og tjenester.[1] Det er derfor særlig viktig at ledelsen sørger for at virksomhetens digitale verdier er tilfredsstillende sikret mot «negativ påvirkning».

Den viktigste arenaen toppledelsen har for å utøve sitt ansvar, er ledelsens gjennomgang. Dette er et status- og planleggingsmøte hvor ledelsen holder seg orientert om, stiller krav til og følger opp arbeidet med informasjonssikkerhet i virksomheten, inkludert sikringen av personopplysninger.

I denne temarapporten drøfter vi i hvilken grad og på hvilke måter ledelsens gjennomgang gjennomføres hos virksomheter i UH-sektoren. Vi ser blant annet på om og hvor ofte ledelsens gjennomgang gjennomføres, hvem fra toppledelsen som deltar og hva som diskuteres på disse møtene. Hos universitetene og høgskolene ser vi i tillegg på hvordan styrene er informert om og involvert i arbeidet med informasjonssikkerhet.

Til slutt gir vi noen forslag om hvilke agendapunkter (temaer) som det kan være hensiktsmessig for toppledelsen å be om status på, diskutere og ta stilling til på ledelsens gjennomgang.

1 Se spesielt «Risiko- og tilstandsvurdering 2021», kapittel 1 (https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning).

Informasjonssikkerhet, person-opplysninger og personvern

Personvern handler om mer enn informasjonssikkerhet. At person-opplysninger beskyttes mot brudd på sikkerheten, for eksempel at uvedkommende får tilgang til slike opplysninger, er en nødvendig, men ikke tilstrekkelig betingelse for å ivareta personvernet. Eksempler på andre nødvendige betingelser er at opplysningene brukes til spesifikke og avgrensede formål, at behandlingen har et lovlig grunnlag, at det ikke samles inn flere opplysninger enn nødvendig, at opplysningene er korrekte og oppdaterte, og at opplysningene slettes når det ikke lenger er bruk for dem.

Samtidig handler informasjonssikkerhet om mer enn personopplysninger og personvern. Det handler i tillegg om beskyttelse av andre typer data eller opplysninger, blant annet vær- og klimadata, geologiske data og maritime data, og om ivaretakelse av andre hensyn, for eksempel nasjonal sikkerhet og kommersielle interesser. Det handler også om data innenfor fagområder hvor det utvikles flerbruksteknologi, det vil si tekniske løsninger som kan ha både sivile og militære anvendelsesområder (nanoteknologi, maskinlæring og nevrale nettverk, kryptologi, undervannsteknologi, osv.).

I tillegg til å beskytte data/opplysninger, er beskyttelse av miljøet som opplysningene befinner seg i en viktig del av informasjonssikkerheten. Dette miljøet består blant annet tekniske elementer (datamaskiner, programvare, datanettverk, osv.), menneskelige elementer (sluttbrukere, administratorer, osv.) og organisatoriske elementer (kjennetegn ved virksomheter som behandler opplysninger og som anvender eller drifter IT-løsninger).[2]

Mye av innsatsen på informasjonssikkerhetsområdet i UH-sektoren gjelder beskyttelse av personopplysninger. Dette har medført at en del virksomheter har slått sammen arbeidet med informasjonssikkerhet og arbeidet med personvern (GDPR). Det innebærer enten at ledelsessystemet for informasjonssikkerhet og internkontrollen for GDPR er integrert i et felles internkontrollsystem, eller at internkontrollen for GDPR inngår i ledelsessystemet for informasjonssikkerhet.

Datagrunnlaget

Drøftelsene og forslagene i denne temarapporten baserer seg på funn fra Unit/HK-dir sin kartlegging av informasjonssikkerhet og personvern i UH-sektoren for 2020/2021. Kartleggingen omfatter de 30 universitetene, høgskolene, direktoratene og selskapene som «Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning» gjelder for.[3]

Datagrunnlag og metodikk gjøres nærmere rede for i «Risiko- og tilstandsvurdering 2021», vedlegg 1-3.[4]

2 For mer om informasjonssikkerhet og personvern (GDPR), se for eksempel Audun Jøsang (2021): *Informasjonssikkerhet – teori og praksis.* Oslo: Universitetsforlaget; Dag Wiese Schartum (2020): *Personvernforordningen. En lærebok*. Bergen: Fagbokforlaget; Jon Wessel-Aas og Magnus Ødegaard (2018): *Personvern. Publisering og behandling av personopplysninger.* Oslo: Gyldendal.

3 Policyen er tilgjengelig på https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning.

4 «Risiko- og tilstandsvurdering 2021» er tilgjengelig på https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning.

Policy, ledelsessystem og ledelsens gjennomgang

I Kunnskapsdepartementets «Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning» presiseres toppledelsens ansvar for informasjonssikkerheten. Dette gjøres i policyens punkt 1.

Som for de øvrige punktene i policyen, oppsummerer punkt 1 lovpålagte krav til ledelsens styring av og kontroll med virksomhetens arbeid med informasjonssikkerhet. I tillegg bygger dette punktet på veiledninger fra Datatilsynet,[5] Nasjonal sikkerhetsmyndighet[6] og Digitaliseringsdirektoratet[7] om sikkerhetsstyring, internkontroll og informasjonssikkerhet.

Punkt 1 – policy for informasjonssikkerhet og personvern

Det er virksomhetens øverste ledelse som har ansvaret for at informasjonssikkerheten er tilfredsstillende. Virksomhetens øverste ledelse må derfor se til at arbeidet med informasjonssikkerhet skjer på en systematisk og planmessig måte. Dette gjøres ved at (i) det innføres et ledelsessystem for informasjonssikkerhet og (ii) informasjonssikkerhet inngår i den generelle virksomhetsstyringen.

a) Virksomheten innfører, vedlikeholder og forbedrer et ledelsessystem for informasjonssikkerhet tilpasset virksomhetens størrelse og behov. Ledelsessystemet bør basere seg på anerkjente internasjonale standarder, for eksempel ISO/IEC 27001.
b) Virksomhetens øverste ledelse stiller tydelige krav til arbeidet med informasjonssikkerhet. Virksomhetens øverste ledelse fastsetter sikkerhetsmål, sikkerhetsstrategi og kriterier for akseptabel risiko.
c) Virksomhetens øverste ledelse kan delegere sikkerhetsoppgaver og myndighet til andre ansatte i virksomheten. Dette beskrives i virksomhetens sikkerhetsorganisering.
d) Virksomhetens øverste ledelse ser til at arbeidet med informasjonssikkerhet tilføres tilstrekkelige ressurser.
e) Virksomhetens øverste ledelse forsikrer seg om at tilfredsstillende organisatoriske og tekniske sikringstiltak er etablert og holder seg orientert om sikkerhetstilstanden i virksomheten, for eksempel med utgangspunkt i NSMs grunnprinsipper for IKT-sikkerhet.
f) Virksomhetens øverste ledelse sørger for periodisk revisjon av arbeidet med informasjonssikkerhet og oppdatering av ledelsessystemet (ved behov).

Virksomhetens øverste styrende organ fører kontroll med arbeidet med informasjonssikkerhet.

5 Se Datatilsynets veileder om internkontroll og informasjonssikkerhet (https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/).

6 Se Nasjonal sikkerhetsmyndighets veileder om sikkerhetsstyring (https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/veileder-i-sikkerhetsstyring/om-denne-veilederen/).

7 Se Digitaliseringsdirektoratets veileder om internkontroll på informasjonssikkerhetsområdet (https://internkontroll-infosikkerhet.difi.no/).

Av policyen fremgår det at topp-ledelsen, vanligvis rektor eller direktør, har ansvaret for at det blir etablert og innført et ledelsessystem for informasjonssikkerhet. Ledelsessystemet (også omtalt som styringssystem eller internkontroll) er ledelsens redskap for å styre, kontrollere og forbedre arbeidet med informasjonssikkerhet. Det skal være en del av den ordinære virksomhetsstyringen.

Ledelsen har et særlig ansvar for å bestemme målene for arbeidet med informasjonssikkerhet (sikkerhetsmål og akseptkriterier), hvordan målene skal oppnås (sikkerhetsstrategi) og hvem som skal gjøre det praktiske arbeidet (sikkerhetsorganisering). Ledelsen har også ansvar for at arbeidet er riktig dimensjonert og at det har den nødvendige kvaliteten (ressursprioritering). I tillegg skal ledelsen se til at informasjonssikkerheten evalueres for å avdekke og utbedre svakheter (sikkerhetsrevisjoner/-tester).

Til sist stilles det krav om at det øverste styrende organet, for eksempel universitets- eller høgskolestyret, ser til at virksomhetsledelsen ivaretar sitt ansvar, spesielt at ledelsessystemet fungerer etter hensikten og at informasjonssikkerheten er tilfredsstillende.

Ledelsessystem for informasjonssikkerhet

Ledelsessystemer strukturerer arbeidet med risikostyring av informasjonssikkerheten. Formålet er at virksomhetene skal oppnå og vedlikeholde et tilfredsstillende sikkerhetsnivå.

Følgende hovedaktiviteter inngår i ledelsessystemer for informasjonssikkerhet:

(i) identifisere hva som skal sikres (data, personopplysninger, programvare, datamaskiner, osv.),
(ii) vurdere risikoen for brudd på informasjonssikkerheten og etablere forebyggende tiltak,
(iii) oppdage og håndtere brudd på informasjonssikkerheten og avvik fra egne sikkerhetsrutiner,
(iv) opprettholde kritiske oppgaver/funksjoner ved alvorlige informasjonssikkerhetshendelser,
(v) gjenopprette sikker drift etter alvorlige informasjonssikkerhetshendelser.

Ledelsessystemene er bygd opp på samme måte som andre typer internkontrollsystemer (styrende, gjennomførende og kontrollerende deler). Toppledelsen spiller en særlig viktig rolle i forvaltningen av den styrende delen av ledelsessystemet (sikkerhetsmål og -strategi, akseptkriterier, sikkerhetsorganisering og ressursplanlegging).

Digitaliseringsdirektoratet, Datatilsynet, Nasjonal sikkerhetsmyndighet og Direktoratet for økonomiforvaltning anbefaler at ledelsessystemet for informasjonssikkerhet baserer seg på internasjonalt anerkjente standarder, for eksempel ISO/IEC 27001, og at det er integrert i virksomhetens øvrige internkontrollarbeid (helhetlig internkontroll).[8]

8 Se for eksempel veileder om helhetlig styring og kontroll av informasjonssikkerhet på https://www.digdir.no/informasjonssikkerhet/helhetlig-styring-og-kontroll-av-informasjonssikkerhet/2284.

Ledelsens gjennomgang er ikke eksplisitt nevnt i departementets policy for informasjonssikkerhet og personvern. Den er likevel en avgjørende del av ledelsessystemet for informasjonssikkerhet. Uten at slike status- og planleggingsmøter gjennomføres, er det vanskelig å snakke om at virksomheten har et fungerende ledelsessystem hvor at toppledelsen setter premissene for, holder seg informert om og følger opp arbeidet med informasjonssikkerhet.

I veiledninger fra nasjonale myndigheter[9] er det, så langt vi kan se, noe ulike oppfatninger om hvordan ledelsens gjennomgang bør gjennomføres og hva som bør diskuteres. Det er derfor i stor grad opp til den enkelte virksomhet og toppledelse å bestemme praktiske forhold som hyppighet, form og innhold. De viktigste ufravikelige kravene er at ledelsens gjennomgang skjer regelmessig (minimum én gang i året) og på måter som er egnet til å ivareta formålet med gjennomgangen (ledelsens styring og kontroll).

I praksis delegerer toppledelsen det daglige ansvaret for informasjonssikkerhetsarbeidet til informasjonssikkerhetsleder/-rådgiver (CISO) eller sikkerhetsleder (CSO), eventuelt personvernombudet. Det er vanligvis lederen for det daglige arbeidet som forbereder ledelsens gjennomgang og følger opp prioriteringer bestemt i ledelsens gjennomgang.

Mange virksomheter har også opprettet et eget forum for informasjonssikkerhet (og personvern) eller et nettverk av personvernkontakter på enhetsnivå. Forumet/nettverket består av ressurspersoner fra ulike deler av virksomheten, ledes av CISO, CSO eller personvernombudet og koordinerer arbeidet med informasjonssikkerhet (eventuelt personvern) i virksomheten. Disse koordineringsorganene bistår ofte lederen for det daglige arbeidet i forberedelsene til og oppfølgingen av ledelsens gjennomgang.

Ettersom ledelsens gjennomgang er en særlig viktig aktivitet i ledelsessystemet for informasjonssikkerhet, har vi, som nevnt ovenfor, kartlagt om den gjennomføres og hvor ofte. Vi har også kartlagt måten den gjennomføres på og hva som diskuteres på disse status- og planleggingsmøtene. Resultatene fra kartleggingen gir en viktig indikasjon på

i. om toppledelsen ivaretar sitt lovpålagte ansvar for informasjonssikkerheten på tilfredsstillende måter, og
ii. om, eventuelt hvordan, ledelsens styring og kontroll på informasjonssikkerhetsområdet kan styrkes/forbedres.

På de neste sidene presenterer vi resultatene fra kartleggingen av ledelsens gjennomgang hos de 30 virksomhetene – statlige universiteter og høgskoler, direktorater og selskaper – som omfattes av Kunnskapsdepartementets policy for informasjonssikkerhet og personvern.

9 Datatilsynet, Nasjonal sikkerhetsmyndighet og Digitaliseringsdirektoratet (se fotnote 3-5).

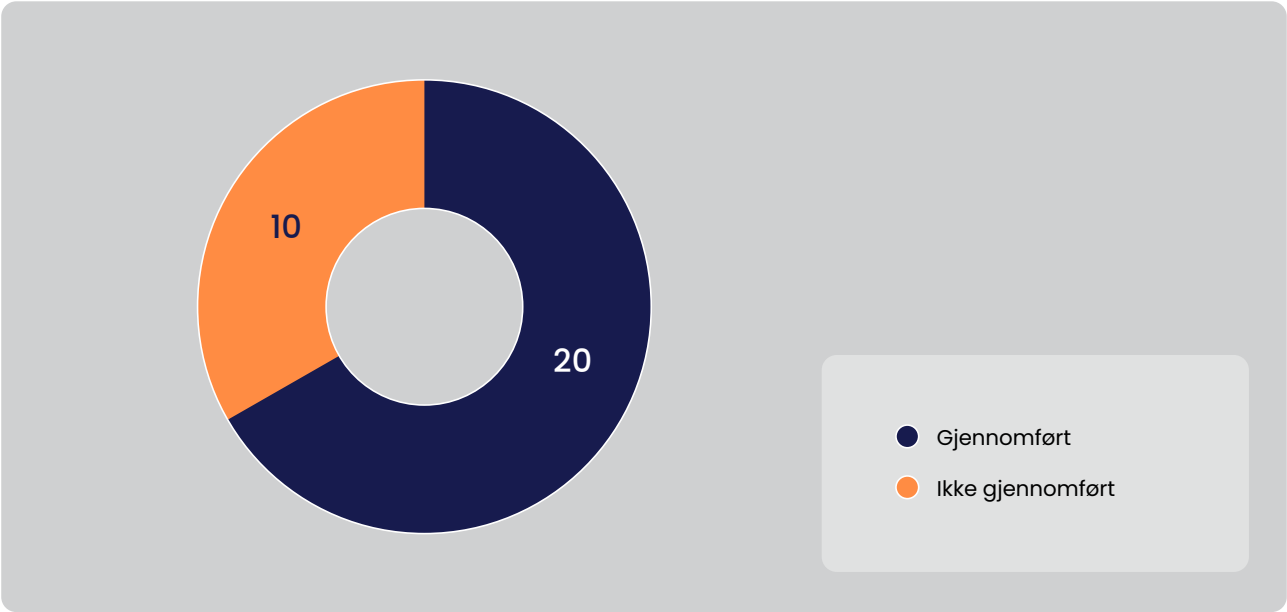
Om og hvor ofte?

Figur 1 viser hvor mange av de 30 virksomhetene som sa at ledelsens gjennomgang hadde blitt gjennomført det siste året.

Her ser vi at 20 av 30 virksomheter opplyste om at ledelsens gjennomgang ble gjennomført det siste året. 15 av de 20 virksomhetene var universiteter og høgskoler, mens direktorater og selskaper utgjorde de resterende fem. 10 virksomheter svarte at ledelsens gjennomgang ikke hadde blitt avholdt.

Tallene indikerer at ledelsessystemet for informasjonssikkerhet synes å være forankret på toppledernivå hos majoriteten av virksomhetene i UH-sektoren. Dette kan også indikere at arbeidet med informasjonssikkerhet er i ferd med å bli en integrert del av den ordinære virksomhetsstyringen hos disse virksomhetene. I hvilken grad dette faktisk er tilfelle, avhenger blant annet av hvem som deltar på møtene, hva som diskuteres og bestemmes, og hvordan eventuelle beslutninger iverksettes i organisasjonen. Dette er spørsmål vi vil se litt nærmere på nedenfor.

Figur 1: Gjennomføring av ledelsens gjennomgang



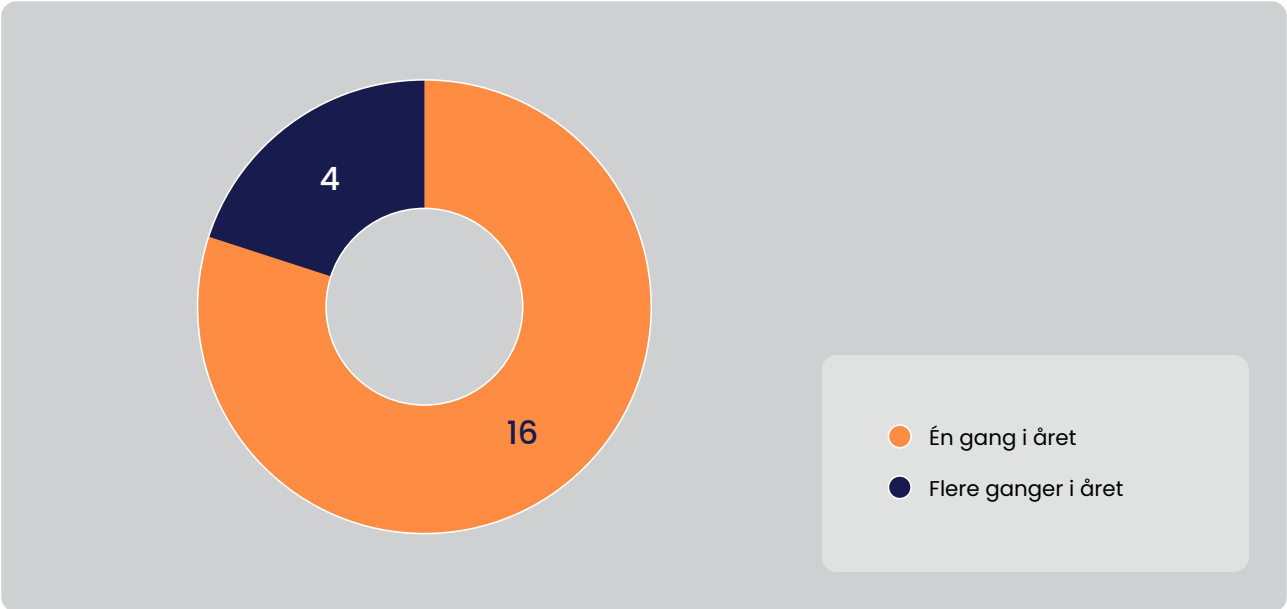
Figur 2 viser hvor ofte ledelsens gjennomgang ble gjennomført hos de 20 virksomhetene som oppga at dette status- og planleggingsmøtet ble avholdt.

Av figuren ser vi at fire av de 20 virksomhetene svarte at ledelsens gjennomgang ble gjennomført to eller flere ganger i løpet av det siste året. 16 virksomheter opplyste om at ledelsens gjennomgang ble gjennomført én gang.

Hvordan ledelsens gjennomgang ble gjennomført varierte noe. Den kunne for eksempel bli avholdt som ett eller flere møter som i sin helhet var dedikert til arbeidet med informasjonssikkerhet. Men den kunne også foregå ved at informasjonssikkerhet var et eget tema i møter hvor andre internkontrollområder ble diskutert (personvern/GDPR, samfunnssikkerhet og beredskap, helse, miljø og sikkerhet, osv.). Det vanligste var likevel at informasjonssikkerhet enten var det eneste temaet på agendaen eller at både informasjonssikkerhet og personvern (GDPR) ble drøftet på det samme møtet. Det siste var særlig vanlig hos virksomheter som hadde integrert ledelsessystemet for informasjonssikkerhet og internkontrollen for GDPR.

At 20 virksomheter hadde gjennomført ledelsens gjennomgang det siste året, indikerer at arbeidet med informasjonssikkerhet er tilfredsstillende forankret på toppledernivå. Samtidig antyder dette at informasjonssikkerhet er i ferd med å bli en integrert del av virksomhetsstyringen i viktige deler av sektoren.

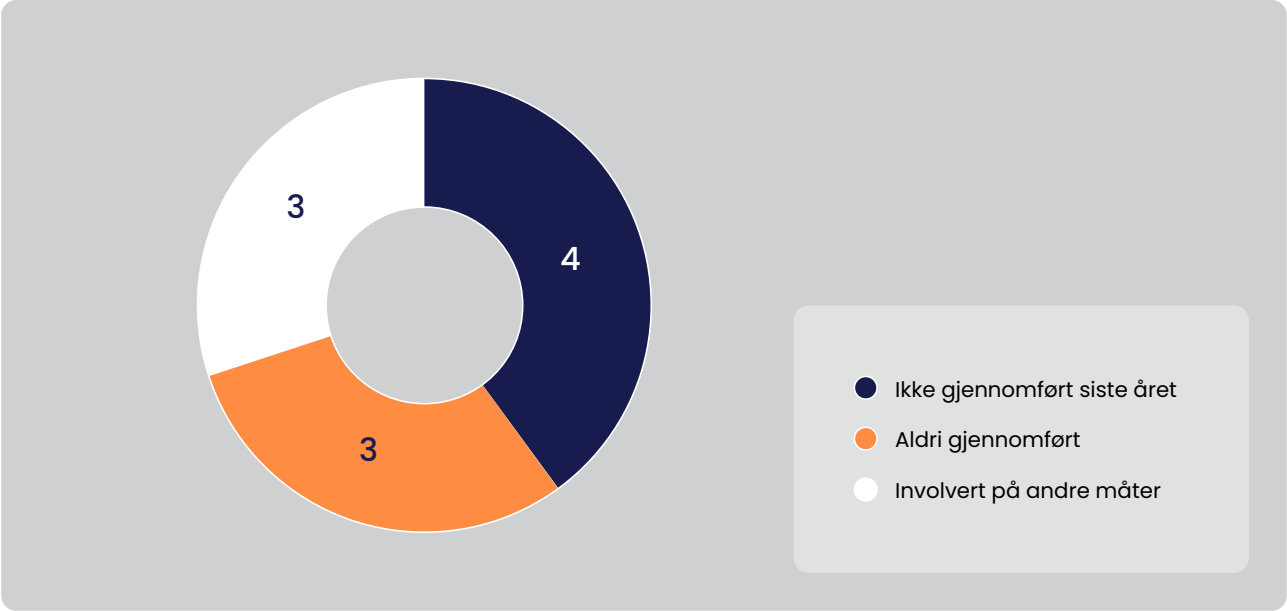
Figur 2: Ledelsens gjennomgang – hyppighet



De siste 10

Figur 1 viser at et relativt stort mindretall av virksomhetene i UH-sektoren – 10 av 30 – ikke hadde gjennomført ledelsens gjennomgang det siste året. Men selv om dette ikke ble gjort, betyr det likevel ikke at ledelsens gjennomgang aldri hadde vært gjennomført eller at toppledelsen ikke var involvert i arbeidet med informasjonssikkerhet på andre måter.

Figur 3: Status for ledelsens gjennomgang hos de 10 siste virksomhetene



Figur 3 viser hvor mange av de 10 siste virksomhetene som aldri hadde gjennomført ledelsens gjennomgang. Den viser også hvor mange som hadde avholdt ledelsens gjennomgang tidligere (men ikke det siste året), og som oppga at toppledelsen deltok i arbeidet med informasjonssikkerhet på andre måter.

Tre av virksomhetene opplyste om at ledelsens gjennomgang aldri hadde blitt gjennomført. To av disse hadde likevel vedtatt rutiner for ledelsens gjennomgang, og opplyste om at den ville bli gjennomført i inneværende år.

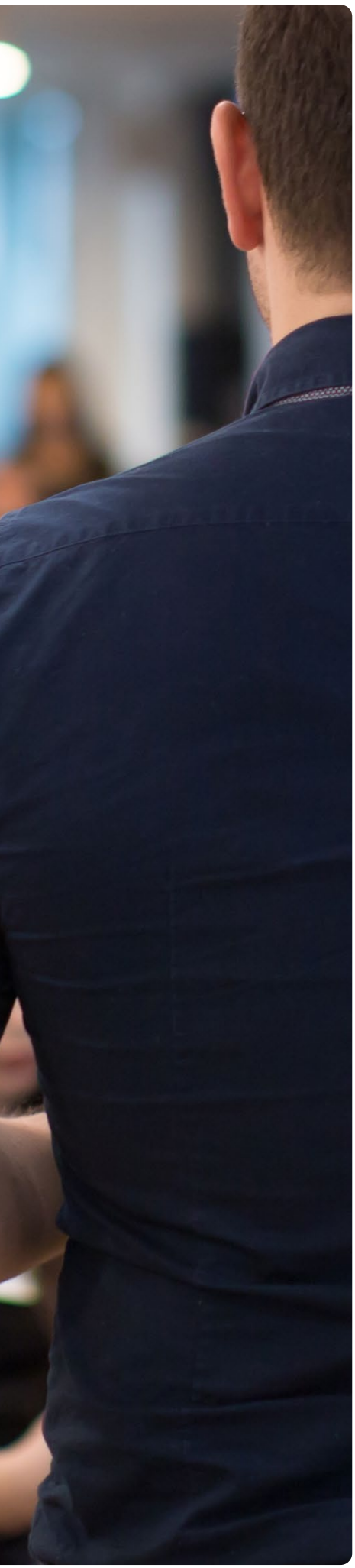
Tre andre virksomheter hadde heller ikke gjennomført ledelsens gjennomgang, men rapporterte om at ledelsen ble involvert i arbeidet med informasjonssikkerhet på andre måter. Her ble det vist til at toppledelsen ble holdt løpende orientert om arbeidet med informasjonssikkerhet (og personvern) eller at ledelsen fikk innblikk i arbeidet gjennom utarbeidelse av årsrapporten.

Fire av virksomhetene oppga at ledelsens gjennomgang ikke ble gjennomført siste året, men at den

hadde blitt gjennomført tidligere. De hadde også rutiner for ledelsens gjennomgang. Manglende gjennomføring var derfor et avvik fra de lokale rutinene.

Avvikene fra egne rutiner for ledelsens gjennomgang ble forklart på litt ulike måter. Enkelte oppga for eksempel at internkontrollarbeidet og ledelsessystemet for informasjonssikkerhet var under revisjon. De mente derfor at det var hensiktsmessig å utsette gjennomgangen til etter at revisjonsarbeidet var sluttført. Andre virksomheter oppga at ledelsens gjennomgang hadde blitt avlyst fordi lokale ressurser måtte omdisponeres til håndtering av korona-situasjonen. Det ble opplyst om at ledelsens gjennomgang ville bli avholdt i løpet av inneværende år.

Resultatene viser at hos flertallet av de siste 10 virksomhetene er ledelsens gjennomgang en aktivitet som det enten finnes rutiner for og som er avholdt tidligere, eller som involverer toppledelsen på andre måter enn gjennom et eget, formelt møte. Samlet sett indikerer dette likevel at ledelsens gjennomgang trolig er noe svakere institusjonalisert enn hos de øvrige 20 virksomhetene i sektoren.



Hvem deltok fra toppledelsen?

Ledelsens gjennomgang vil ikke tjene sin hensikt uten at toppledelsen deltar. At det avholdes et status- og planleggingsmøte én eller flere ganger i året som har tittelen «ledelsens gjennomgang», er derfor ikke nok. Det er også en forutsetning at toppledelsen faktisk er til stede.

Av de 20 universitetene, høgskolene, direktoratene og selskapene som gjennomførte ledelsens gjennomgang, rapporterte alle at toppledelsen faktisk var til stede.

Toppledelsen ble hos de fleste av disse 20 virksomhetene definert som rektor, universitets- eller høgskoledirektør, administrerende eller assisterende direktør.

Hos en del virksomheter ble det opplyst om bred deltakelse fra ledelsen. Her ble ledelsens gjennomgang enten gjennomført i utvidet ledermøte eller i ledergruppen. Hos én virksomhet ble ledelsens gjennomgang avholdt sammen med universitetsstyret.

Oppsummert kan vi si at hos disse virksomhetene ble én av de viktigste forutsetningene for toppledelsens styring og kontroll ivaretatt – den øverste ledelsen var representert. Men toppledelsens deltakelse er ikke den eneste forutsetningen – det er også andre forhold som må være til stede for at ledelsens styring og kontroll skal kunne utføres på en tilfredsstillende måte.

Hva ble diskutert?

I veiledningene fra nasjonale myndigheter referert til ovenfor, er det noe ulike oppfatninger om hva det kan være mest hensiktsmessig å ta opp på ledelsens gjennomgang. Det viktige er imidlertid at agendaen for møtene – hva som diskuteres – er egnet for den rollen toppledelsen er ment å spille: sette premissene for, holde seg informert om og følge opp arbeidet med informasjonssikkerhet, inkludert personopplysningssikkerheten.

Spørsmålet er derfor hva ledelsens gjennomgang hos virksomhetene i UH-sektoren ble brukt til? I hvilken grad ble forhold som ivaretar hensikten med gjennomgangen (overordnet styring og kontroll) faktisk tatt opp og diskutert?

Som nevnt ovenfor, er det vanligvis informasjonssikkerhetsleder/-rådgiver eller sikkerhetsleder, gjerne i samarbeid med personvernombudet, som har ansvaret for å forberede agendaen og saksunderlaget til ledelsens gjennomgang. Hos enkelte virksomheter ble oppgaven utført av personvernombudet.

Figuren nedenfor gir en oversikt hvilke agendapunkter/tema disse aktørene hadde valgt å fokusere på i ledelsens gjennomgang. Hver av de 20 virksomhetene som hadde gjennomført ledelsens gjennomgang oppga flere ulike tema.

Figur 4: Vanligste tema diskutert på siste ledelsens gjennomgang

Av figur 4 fremgår det at spørsmål knyttet til risikostyring av informasjonssikkerheten ble diskutert av flest virksomheter. Det handlet enten om (i) hvordan risikostyringsprosessen i virksomhetene var organisert og fungerte, eller (ii) redegjørelser for selve risikovurderingsaktiviteten (konkrete risikovurderinger som hadde blitt gjennomført det siste året eller som var planlagt for det kommende/inneværende året).

Det siste (risikovurderingsaktiviteten) omfattet enten vurderinger av informasjonssikkerheten på system-, tjeneste- og prosessnivå eller overordnede vurderinger av informasjonssikkerheten på virksomhetsnivå, eventuelt begge deler. De overordnede vurderingene kunne også omfatte andre risikoområder enn informasjonssikkerhet, for eksempel helse, miljø og sikkerhet.

Brudd på informasjonssikkerheten som virksomhetene hadde vært utsatt for det siste året (sikkerhetshendelser) var et annet vanlig tema i ledelsens gjennomgang. Her ble det blant annet gjort rede for hvor mange og hvilke typer sikkerhetsbrudd det dreide seg om, hvilke skadevirkninger (om noen) sikkerhetsbruddene hadde medført og tiltak som var iverksatt for å forebygge gjentakelser.

Det ble også gjort rede for eventuelle varslinger som var sendt til Datatilsynet eller til de registrerte (brudd på personopplysningssikkerheten som førte til risiko eller høy risiko for de registrertes personvern, rettigheter og friheter).

Gjennomføring av eller behovet for konkrete sikkerhetstiltak, spesielt tekniske og pedagogiske (informasjon, opplæring, osv.), ble også ofte tatt opp. Dette kunne for eksempel dreie seg om segmentering av datanettverk, innføring av totrinnsinnlogging, kursvirksomhet, informasjon på hjemmesider, osv.

Til slutt var det en del virksomheter som opplyste om at registrerte avvik fra lokale rutiner for sikker behandling av personopplysninger eller annen viktig informasjon ble behandlet på ledelsens gjennomgang. I denne forbindelse kunne det også bli diskutert behov for revisjon av rutinene eller utarbeidelse av nye.

I tillegg til dette ble enkelte andre tema diskutert hos flere av virksomhetene. Det gjaldt for eksempel revisjoner av ledelsessystemet for informasjonssikkerhet eller internkontrollen for GDPR (eventuelt ledelsessystemet for informasjonssikkerhet og personvern i virksomheter hvor dette var integrert i et felles styringssystem/internkontroll).

Oppsummert kan vi si at svarene fra de 20 virksomhetene som gjennomførte ledelsens gjennomgang, gir et noe sprikende bilde av innholdet i gjennomgangene: virksomhetene virker å ha litt ulike oppfatninger om hva ledelsens gjennomgang bør brukes til. Slik vi ser det, behandlet alle virksomhetene tema som er relevante for toppledelsen å bli informert om og ta stilling til. Men oversikten i figur 4 viser også, etter vår mening, at enkelte tema som det kan være hensiktsmessig å diskutere i liten grad ble behandlet. Vi kommer tilbake til hva dette er i siste del av temarapporten.

Linjen til universitets- eller høgskolestyret

I «Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning» (punkt 1 bokstav g) forventes det at virksomhetens øverste organ fører kontroll med informasjonssikkerheten. Hos universitetene og høgskolene vil dette være universitets- eller høgskolestyret.

Policyen spesifiserer ikke hvordan universitets- eller høgskolestyret skal utøve sin kontrollrolle. Den forutsetter imidlertid at (i) styret blir orientert om prioriteringer i ledelsens gjennomgang og (ii) kan stille forventninger eller krav til arbeidet med informasjonssikkerhet i virksomheten.

Figur 5 viser om og på hvilke måter styrene utøvde sin kontrollrolle hos de 15 universitetene og høgskolene som gjennomførte ledelsens gjennomgang det siste året.

Av figuren ser vi at 10 av de 15 universitetene og høgskolene som gjennomførte ledelsens gjennomgang, rapporterte videre til styret om status for og prioriteringer i arbeidet med informasjonssikkerhet.

Hos ett av universitetene ble det opplyst om at årsrapport for arbeidet med informasjonssikkerhet og personvern ble behandlet både i universitetsstyret og i fakultetsstyrene.

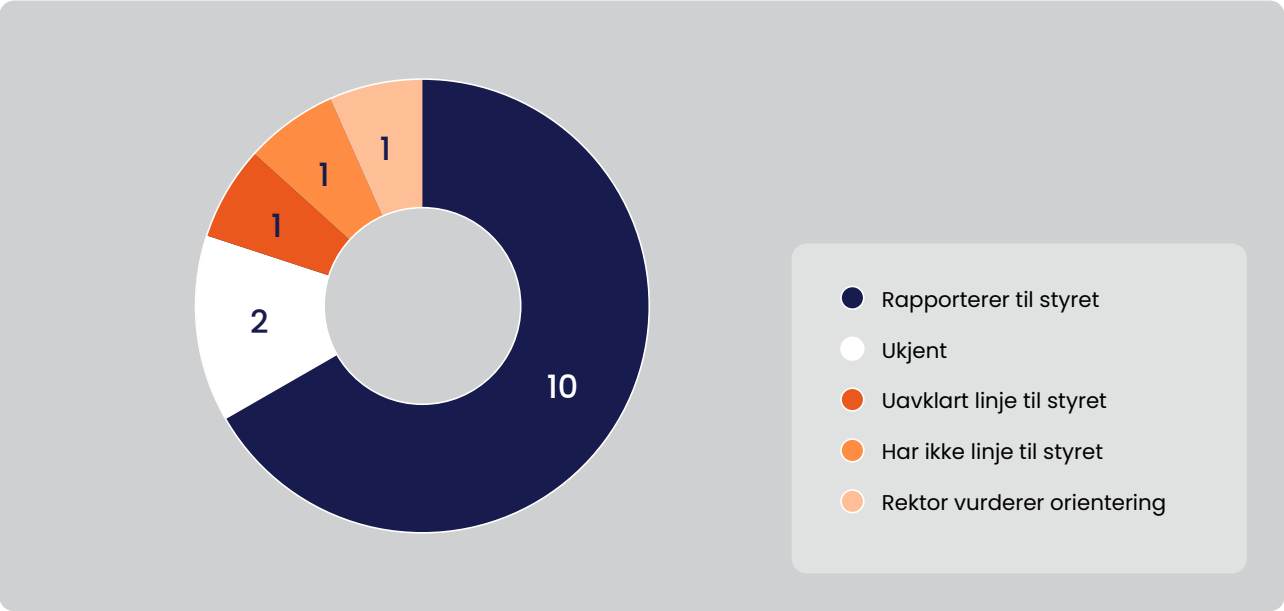
Én virksomhet oppga at styret ikke ble involvert («har ikke linje til styret»). Hos én av de andre var det meningen å involvere styret, men hvordan dette skulle skje var ikke bestemt enda («uavklart linje til styret»).

Det var også én virksomhet som opplyste om at det var opp til rektor å vurdere om styret skulle orienteres om arbeidet med informasjonssikkerhet («rektor vurderer orientering»).

Fra to virksomheter mangler vi informasjon om styret ble involvert og hvordan dette i så fall foregikk («ukjent»).

Den vanligste måten å involvere styret på, var at rapport/oppsummering fra ledelsens gjennomgang ble fremmet som orienteringssak. Enkelte virksomheter oppga imidlertid at det ble gitt egne presentasjoner av

Figur 5: Involvering av universitets- eller høgskolestyret



arbeidet med informasjonssikkerhet for styret.

Hos flere av universitetene og høgskolene ble også årsrapport fra personvernombudet lagt frem sammen med orienteringen fra ledelsens gjennomgang.

Vårt inntrykk er at der hvor arbeidet med informasjonssikkerhet (og personvern) ble fremmet som orienteringssak, kunne grundigheten i styrebehandlingen variere noe. Men det ble også opplyst om styrer som ivaretok sin kontrollrolle på en særlig aktiv måte. Disse styrene forventet å bli holdt løpende orientert om arbeidet, etterspurte statusoppdateringer på viktige tiltak/initiativ eller ba om at kontrollaktiviteter ble utført, for eksempel at det ble gjennomført eksterne revisjoner av virksomhetens arbeid med informasjonssikkerhet (eventuelt personvern).

Hos én av de seks universitetene og høgskolene som ikke hadde gjennomført ledelsens gjennomgang det siste året, ble det opplyst om at det fantes rutiner for hvordan styret skulle involveres i etterkant av gjennomgangen (orienteringssak). Én av de andre virksomhetene svarte at styret ble holdt orientert gjennom prosessen med utarbeidelse av årsrapport. Hos én tredje var iverksettingen av ledelsessystemet ikke kommet langt nok til at spørsmålet om styrets involvering var avklart.

Ledelsens gjennomgang – hva så?

Vi har sett at 2/3 av virksomhetene i UH-sektoren opplyste om at ledelsens gjennomgang ble gjennomført én eller flere ganger det siste året. Samtidig oppga 10 av universitetene og høgskolene at styrene ble involvert i arbeidet med informasjonssikkerhet (og personvern).

Spørsmålet er hvilken styringskraft dette gir – har «tonen på toppen» bidratt til å styrke arbeidet og forbedre informasjonssikkerheten?

I hvor stor grad «tonen på toppen» påvirker virksomhetenes daglige arbeid med informasjonssikkerhet, er vanskelig å avgjøre. Dette fordi det finnes en rekke andre interne og eksterne forhold som har stor betydning for omfanget av og kvaliteten på arbeidet. Det kan for eksempel dreie seg om kompleks og desentralisert organisasjonsstruktur, skepsis mot toppstyring, liten erfaring med kvalitetsstyring og internkontroll, vanskelig tilgang på kvalifisert sikkerhetspersonell, et utfordrende regelverk og lite brukervennlige sikringstiltak. Likevel mener vi at resultatene i denne temarapporten indikerer at styringseffekten av ledelsens gjennomgang kan forbedres ytterligere i deler av sektoren.

Dette illustreres i Unit/HK-dir sin risiko- og tilstandsvurdering for 2021. Her konkluderes med at fire av 30 virksomheter kan sies å ha etablert et bærekraftig og systematisk informasjonssikkerhetsarbeid som omfatter alle deler av virksomheten.[10] Flere andre virksomheter hadde gjort viktige forbedringer i arbeidet med informasjonssikkerhet i løpet av de siste par årene. Samlet sett er dette likevel færre enn antallet virksomheter som opplyste om at ledelsens gjennomgang blir gjennomført. Forskjellen mellom antallet virksomheter som tydelig har forbedret sitt arbeid og antallet virksomheter som oppgir at de gjennomfører ledelsens gjennomgang, antyder at det kan være rom for å styrke ledelsens gjennomgang som toppledelsens viktigste forbedringsredskap.

10 Se «Risiko- og tilstandsvurdering 2021», side 22 og 52. Rapporten er tilgjengelig på https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning.


2
1
3
4
5
6

Forslag til gjennomføring

Det kan finnes flere måter å forbedre styringseffekten av ledelsens gjennomgang på. Én av disse er å sørge for at innholdet i gjennomgangen holdes på et strategisk, overordnet nivå.

Det betyr at ledelsens gjennomgang ikke bør være for detaljert eller for ambisiøs på ledelsens vegne, for eksempel at sakene legges frem på en måte som forutsetter særskilt ekspertise og faglig innsikt. Gjennomgangen bør isteden tilpasses så godt som mulig til ledelsens rolle og kompetanse.

Slik vi ser det, betyr dette at ledelsen bør få et overblikk over status for arbeidet og et grunnlag for å gjøre overordnede prioriteringer med hensyn til den videre innsatsen.

Agendapunkter for ledelsens gjennomgang

Med dette som utgangspunkt, foreslår vi at ledelsens gjennomgang struktureres rundt seks agendapunkter. Under hvert agendapunkt har vi foreslått noen hjelpespørsmål.[11] Formålet med hjelpespørsmålene er å konkretisere innholdet i de ulike agendapunktene.

Virksomhetene bør selv vurdere om det er hensiktsmessig å drøfte alle hjelpespørsmålene i ledelsens gjennomgang. Dette gjelder spesielt for de mindre virksomhetene i sektoren.

1

Kunnskapsdepartementets policy for informasjonssikkerhet og personvern i høyere utdanning og forskning

- Hva er status for vår etterlevelse av hovedpunktene i policyen?
- Hvor ligger vi godt an og hva bør vi forbedre?
- Hvilke forbedringspunkter bør vi prioritere særlig høyt i det videre arbeidet?
- Hvilke endringer (om noen) er det behov for i vårt ledelsessystem for informasjonssikkerhet, spesielt med hensyn til sikkerhetsmål, sikkerhetsstrategi, akseptkriterier og sikkerhetsorganisering?
- Hvilke forbedringer ble anbefalt i eventuelle eksterne revisjoner av vårt ledelsessystem, og hvilke av disse bør vi særlig prioritere å gjøre noe med?
- Når bør neste eksterne revisjon av vårt ledelsessystem gjennomføres, og hva bør revisjonen i særlig grad fokusere på?

2

Anbefalinger og tilbakemeldinger fra Kunnskapsdepartementet og HK-dir

- Har vi mottatt anbefalinger i det årlige anbefalingsbrevet fra HK-dir som vi bør bite oss merke i og ha spesiell oppmerksomhet på fremover?
- Hvilke forventninger stilles til arbeidet med informasjonssikkerhet og sikring av personopplysninger i tildelingsbrevet fra departementet, og hva bør vi gjøre for å imøtekomme forventningene?
- Hvilke tilbakemeldinger har vi fått i styringsdialogen med departementet som det er særlig viktig at vi har oppmerksomhet på fremover?

3

Brudd på informasjonssikkerheten og avvik fra egne sikkerhetsrutiner

- Hvor mange og hvilke typer brudd på informasjonssikkerheten er registrert det siste året, og hvor alvorlige er disse hendelsene?
- Hvor mange og hvilke typer avvik fra egne sikkerhetsrutiner er registrert det siste året, og hvor alvorlige er disse avvikene?
- Har vi registrert flere eller færre hendelser og avvik i år enn tidligere?
- Hva bør vi gjøre fremover for å styrke vår evne til å forebygge, oppdage og håndtere disse og liknende typer hendelser og avvik?

11 Digitaliseringsdirektoratet har utarbeidet en mer detaljert og omfattende liste med hjelpespørsmål til ledelsens gjennomgang (https://internkontroll-infosikkerhet.difi.no/maler-og-eksempler). Det britiske cybersikkerhetssenteret har utarbeidet en liknende spørsmålsliste myntet på styremedlemmer (https://www.ncsc.gov.uk/files/Board-toolkit-QAs.pdf).

Status innenfor disse seks områdene og planer for det videre arbeidet bør rapporteres til og gjennomgås av virksomhetens øverste styrende organ (styret).

4

Risikostyring – vurderinger av risiko og etablering av tiltak

- Innenfor hvilke områder (undervisning, forskning, formidling og administrasjon) ble det gjennomført risikovurderinger av informasjonssikkerheten i år?
- I hvilken grad ble vurderingene fulgt opp med nødvendige tiltak, og når vil manglende tiltak bli gjennomført?
- Hva forteller risikovurderingene oss om hvilke hovedtyper trusler og sårbarheter vi bør rette oppmerksomheten og innsatsen mot fremover?
- Hvilke nye digitaliseringsinitiativ har vi gjennomført som påvirker risikoen for brudd på informasjonssikkerheten, og hva er gjort/bør vi gjøre for å håndtere denne risikoen?
- Hva bør vi legge særlig merke til i nasjonale vurderinger av risiko og trusler i høyere utdanning og forskning (for eksempel fra NSM, PST, Datatilsynet eller HK-dir)?
- Hvilke sårbarheter/sikkerhetshull ble avdekket i eventuelle tekniske sikkerhetstester (sårbarhets- eller inntrengingstester), og hvilke av disse må vi prioritere å lukke?
- Hvilke investeringer i nye sikkerhetsløsninger (om noen) er det særlig behov for slik at vi kan redusere risikoen for brudd på informasjonssikkerheten?

5

Håndtering av alvorlige hendelser, beredskap og kontinuitet

- Er vår evne til å oppdage og håndtere digitale sikkerhetshendelser, for eksempel datatyveri eller dataødeleggelse, tilfredsstillende, og hva kan vi gjøre for å forbedre oss?
- I hvilken grad er vi i stand til å videreføre viktige oppgaver/funksjoner dersom vi utsettes for et større dataangrep, og hva kan vi gjøre for å forbedre oss?
- Hvor raskt vil vi være i stand til å gjenopprette normal driftstilstand dersom vi utsettes for et større dataangrep, og hva kan vi gjøre for å forbedre oss?
- Hvilke øvelser på håndtering av alvorlige dataangrep er gjennomført, hvilke læringspunkter sitter vi igjen med og har vi behov for å revidere våre beredskaps- og kontinuitetsplaner?

6

Ressurs- og kompetansebehov

- Har vi de ressursene vi trenger, og bruker vi dem på riktig måte?
- Hvilke opplærings- og kompetansebehov har vi, og hvordan kan vi imøtekomme disse?
- Hvilke planlagte sikkerhetsoppgaver og tiltak trenger vi ekstern assistanse, for eksempel fra Cybersikkerhetssenteret for forskning og utdanning, for å gjennomføre?

Iverksetting av beslutninger

Det er lederen for det daglige arbeid med informasjonssikkerhet (CISO, CSO eller tilsvarende) som har ansvaret for å se til at beslutninger fattet i ledelsens gjennomgang blir iverksatt.

Hos mange virksomheter i UH-sektoren kan den daglige lederen for arbeidet støtte seg på lokale eksperter, for eksempel medlemmene i forum for informasjonssikkerhet og personvern, når toppledelsens beslutninger skal iverksettes. Andre aktører med roller i sikkerhetsorganisasjonen, for eksempel system-, tjeneste- eller prosesseiere, vil også kunne være sentrale i dette arbeidet.

Status for iverksetting rapporteres på neste ledelsens gjennomgang og til virksomhetens øverste styrende organ (styret).

Praktisk råd og veiledning

Cybersikkerhetssenteret for forskning og utdanning er sektorens tjenesteleverandør innenfor informasjonssikkerhet og personvern. Senteret er et samarbeid mellom fagmiljøer hos Kunnskapssektorens tjenesteleverandør (Sikt), NTNU og Universitetet i Oslo.

Cybersikkerhetssenteret vil kunne gi praktisk råd og veiledning om hvordan ledelsens gjennomgang best kan gjennomføres og følges opp. Senteret vil også kunne bistå virksomhetene på en rekke andre områder, for eksempel revisjon av ledelsessystemet for informasjonssikkerhet eller av internkontrollen for GDPR.

Oversikt over cybersikkerhetssenteret sine tjenester finnes i fotnoten nedenfor. [12]

Hva med internkontrollen for personvern (GDPR)?

I virksomheter som har integrert ledelsessystemet for informasjonssikkerhet og internkontrollen for personvern (GDPR), kan det være behov for å diskutere flere spørsmål i ledelsens gjennomgang enn de som er nevnt ovenfor. Eksempler på slike punkter kan være om rutinene for ivaretakelse av de registrerte personvernrettigheter bør revideres, om personopplysninger slettes/anonymiseres og arkiveres slik som forutsatt, om behandlingsgrunnlaget for ulike typer behandlinger er vurdert og fastsatt, om behandlingsprotokollen er oppdatert og fullstendig, eller om kontrollen med og rutinene for overføringer av personopplysninger til tredjeland er tilfredsstillende.

Legg likevel merke til at spesielt agendapunkt 1 og 2 ovenfor dekker viktige deler av arbeidet med personvern (internkontrollen for GDPR).

12 https://www.uninett.no/cybersikkerhetssenteret.