Beskrivelse av Kunnskapsdepartementets styringsmodell for informasjonssikkerhet og personvern i høyere utdanning og forskning

Innledning

Denne beskrivelsen gir en oversikt over Kunnskapsdepartementets styringsmodell for informasjonssikkerhet og personvern som bygger på standarden NS-ISO/IEC 27014:2020[1]. Se vedlegg A for omtale av forholdet til standarden.

Formålet med beskrivelsen er å fastsette roller, ansvar og oppgaver i det løpende samarbeidet mellom KD og HK-dir om sektorstyringen av informasjonssikkerhet og personvern, samt formålene med sektorstyringen på dette området.

Modellen er utarbeidet av Kunnskapsdepartementet (KD) og Direktoratet for høyere utdanning og kompetanse (HK-dir). Styringsmodellens virkeområde er todelt. Først omfatter den KD og HK-dirs styring av informasjonssikkerhet og personvern hos de enkelte virksomhetene direkte under departementet i høyere utdannings- og forskningssektoren. Dernest omfatter den styringen av det generelle nivået på informasjonssikkerheten og personvernet i denne delen av høyere utdannings- og forskningssektoren.

Styringsmodellen er opprettet for å ivareta det overordnede ansvaret departementet har for informasjonssikkerheten og personvernet i de underliggende virksomhetene. Departementet har også et overordnet sektoransvar for hele høyere utdannings- og forskningssektoren som ivaretas utenfor prosessene i styringsmodellen. I denne beskrivelsen viser begrepet «sektoren» til virksomhetene som er omfattet av styringsmodellen.

Målgruppen for beskrivelsen er KD og HK-dir, virksomhetene i høyere utdannings- og forskningssektoren samt andre aktører (interessenter) som er opptatt av arbeidet med informasjonssikkerhet og personvern i sektoren. Beskrivelsen er offentlig og departementet ønsker å legge til rette for at organiseringen av styringen er transparent, forutsigbar og etterprøvbar.

KD og HK-dirs roller i sektorstyringen av informasjonssikkerhet og personvern

- Instruks for departementenes arbeid med samfunnssikkerhet (samfunnssikkerhetsinstruksen) fastsetter krav til departementenes arbeid med samfunnssikkerhet og beredskap. IKT-sikkerhet er en integrert del av arbeidet med samfunnssikkerhet og omfattes av kravene i instruksen. Kravene i instruksen tar utgangspunkt i at arbeidet med samfunnssikkerhet skal være basert på systematisk risikostyring.

[1] NS-ISO/IEC 27014:2020 Informasjonssikkerhet, cybersikkerhet og personvern — Styring av informasjonssikkerhet

- Det enkelte departement har ansvar for samfunnssikkerhet i egen sektor. Dette innebærer et ansvar for arbeid med forebygging, beredskap og krisehåndtering.
- KD har eier- og etatsstyringsansvaret for alle virksomhetene som omfattes av styringsmodellen for informasjonssikkerhet og personvern, og et sektoransvar for de øvrige virksomhetene i høyere utdannings- og forskningssektoren.
- Virksomhets- og økonominstruks for HK-dir beskriver direktoratets faste myndighets- og forvaltningsoppgaver. Den gir HK-dir ansvar for sektorstyring av informasjonssikkerhet og personvern som beskrevet i Kunnskapsdepartementets styringsmodell for informasjonssikkerhet og personvern.
- Styringsmodellen for informasjonssikkerhet og personvern beskriver rolle- og ansvarsfordelingen mellom KD og HK-dir i det forebyggende arbeidet med informasjonssikkerhet og personvern.

Andre sentrale etater og rammeverk

- Rammeverk for håndtering av IKT-sikkerhetshendelser i høyere utdanning og forskning beskriver rollene og ansvarsfordelingen for beredskap for IKT-sikkerhetshendelser.
- Sikt har en viktig rolle i å levere relevante tjenester innenfor informasjonssikkerhet og personvern til sektoren og har ansvaret for sektorvist responsmiljø (SRM) iht. rammeverket ovenfor.
- NOKUT har ansvar for å føre selvstendig kontroll med informasjonssikkerhet og personvern hos virksomhetene i sektoren.

Forholdet til styringen av andre ansvarsområder

ISO-standarden, som styringsmodellen baserer seg på, bygger på de samme overordnede prinsippene for virksomhetsstyring[2] som KDs andre styringsprosesser (risikostyring, økonomistyring, internkontroll mm.) og kan derfor integreres/tilpasses i årshjul og etablerte rutiner på disse områdene. Styringsmodellen bygger på en internasjonal standard som harmonerer med andre standarder for de nevnte styringsprosessene. Dette er med på å ivareta langsiktig, helhetlig styring og kontroll av informasjonssikkerhet og personvern.

Formålene med KD og HK-dirs styring av informasjonssikkerhet og personvern

Standarden beskriver de overordnende formålene[3] med å styre informasjonssikkerhet. Beskrivelsen av disse formålene i styringsmodellen bygger på standarden og er tilpasset KD og HK-dirs anvendelse av denne på sektornivået.

Formål 1: Etablere informasjonssikkerhet og personvern som en integrert del av sektorstyringen

Informasjonssikkerhet og personvern er en integrert del av styringen av sektoren og skal etableres innenfor hele bredden av sektorens aktiviteter. Dette innebærer styring av informasjonssikkerheten og personvernet i alle underliggende virksomheter og selskaper i sektoren. Krav til informasjonssikkerhet og personvern må også ivaretas hos

[2] 'Corporate governance' oversettes ofte til *eierstyring og selskapsledelse* av bransjeorganisasjoner og selskaper eller til *virksomhetsstyring* av Digitaliseringsdirektoratet
[3] Standardens seks «objectives» er oversatt til formål i styringsmodellen for å ikke forveksles med virksomhetsmålene i mål- og resultatstyringen som standarden beskriver

underleverandører. Styringen må tilpasses tilknytningsformen. Dette formålet skal ivaretas innenfor de ordinære styringslinjene:

- HK-dir: Etatsstyring fra KD
- Sikt, NOKUT, NFR, NUPI og FEK: Sektorstyring fra HK-dir, etatsstyring fra KD
- Statlige universiteter og høyskoler: Sektorstyring fra HK-dir, etatsstyring fra KD
- Aksjeselskaper: Sektorstyring fra HK-dir i tråd med statens prinsipper for eierstyring, eierstyring fra KD og avtalestyring/oppdragsstyring
- Underleverandører og tredjeparter: Avtalestyring

I alle disse delene av sektoren eier statsråden og KD risikoen og har en klar styringsinteresse i å håndtere denne effektivt. Det innebærer at departementet må forsikre seg om at informasjonssikkerheten og personvernet styres gjennom *hele verdikjeden* ettersom risikoen for informasjonsverdiene ikke kjenner de organisatoriske grensene. For å håndtere dette må ansvar fastsettes klart og tydelig hos alle aktører.

Hva innebærer dette?

For å etablere informasjonssikkerhet og personvern innenfor alle virksomhetene som omfattes av styringsmodellen, må styringen av informasjonssikkerhet og personvern integreres i de ordinære styringsprosessene. Noen eksempler på dette er:

- Tildelingsbrev: Fastsette krav, ansvar og rapporteringskrav
- Etatsstyringsmøter og styringsdialog: Følge opp risiko, måloppnåelse og etterlevelse
- Generalforsamlinger/selskapsstyring: Fastsette krav, ansvar og rapporteringskrav
- Dialogmøter: Fremheve forventninger og tydeliggjøre ansvar
- Kommunikasjon med interessenter: Kommunisere sikkerhetstilstand og etterlevelse til f.eks. Riksrevisjonen og JD
- Risikostyring: Alle aktører i sektoren bør omfattes i risiko- og sårbarhetsanalyser, og resultatene må ligge til grunn for styringen.

Formål 2: Fatte beslutninger basert på risiko

Styring av informasjonssikkerhet bør ifølge standarden ta utgangspunkt i krav og regelverk samt i sektorspesifikke, risikobaserte beslutninger. Beslutninger om informasjonssikkerhet og personvern bør dermed bygge på risikovurderinger, og sikkerhetsnivået bør bestemmes ut fra risikoaksept.

Hva innebærer dette?

Dette formålet innebærer at risiko bør beskrives på samme nivå som styringen, og at det bør være en systematisk behandling av risikovurderinger på sektornivå i KDs årshjul. Behandling av risikovurderinger innebærer en beslutning om risikoaksept. Dette er i tråd med de styringsprinsipper som gjelder i staten.

KDs risikoaksept og beskrivelsen av denne bør videreutvikles og defineres i takt med kvaliteten på de risikovurderingene som gjøres, og i takt med utviklingen av egen risikostyring.

Formål 3: Gi retning til investeringsbeslutninger

De sannsynlige konsekvensene av risiko bør adresseres på en adekvat måte og vil ofte forutsette nødvendige ressursprioriteringer. Dette formålet innebærer at det planlegges for finansiering av informasjonssikkerhet og personvern med utgangspunkt i de mål som er satt, slik at finansieringen av nye sikkerhetstiltak henger sammen med den generelle styringen av informasjonssikkerhet og personvern.

Hva innebærer dette?

For KD innebærer dette å vurdere risiko- og tilstandsrapporten, planen som skal håndtere denne samt nye forslag og evalueringer av måloppnåelse opp mot finansieringsbehovet. Det kan oppstå situasjoner med f.eks. skjerpet digital risiko hvor behovet kan være større enn tilgjengelig finansiering, og risikovurderingen vil være sentral for å kunne vurdere hva som skal prioriteres innenfor gitte rammer. Prioriteringer av nye informasjonssikkerhets- og personverntiltak besluttes i den ordinære budsjettprosessen. Forslag fremmes av HK-dir og Sikt, og planlegges i forbindelse med risikostyringen og mål- og resultatstyringen.

Formål 4: Sikre etterlevelse av interne og eksterne krav

Styring av informasjonssikkerhet og personvern skal sørge for etterlevelse av *Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning* (fastsatt i rundskriv fra KD). Kravene i policyen følger av lovpålagte krav til arbeidet med informasjonssikkerhet og personvern, og øvrige nasjonale føringer for disse områdene. Policyen oppdateres ved vesentlige endringer i interne og eksterne krav.

Etterlevelse av kravene bør kontrolleres.

Hva innebærer dette?

I forbindelse med monitoreringsprosessen omtalt nedenfor, kartlegger HK-dir etterlevelse av krav med utgangspunkt i selvrapportering fra virksomhetene. Kartleggingen har som formål å gi oversikt over tilstanden og risiko for uønskede hendelser, og er ikke en formell kontroll. Oversikten gir KD og HK-dir et informasjonsgrunnlag for styringen. I tillegg bør det gjennomføres kontroller av oversiktens gyldighet ved den enkelte institusjon. Vedlegg C beskriver roller og ansvar for kontroll.

Riksrevisjonen gjennomfører egne undersøkelser av informasjonssikkerheten og personvernet i sektoren samt departementets styring. Informasjon fra undersøkelsene er viktig for å avdekke manglende etterlevelse og skal følges opp.

Formål 5: Skape et miljø som er positivt til sikkerhet

Formålet er at informasjonssikkerhet og personvern blir en naturlig del av organisasjonskulturen og virksomhetsstyringen på samme måte som andre styringsprosesser slik som f.eks. virksomhetsstyring, budsjettering, økonomistyring og internkontroll. Styringsaktivitetene bør fungere på tvers av fagområdene, og på tvers av andre prosesser og aktiviteter i virksomheten.

Hva innebærer dette?

Å arbeide med dette formålet innebærer å forstå hva som må til for å skape et miljø som legger til rette for måloppnåelse innenfor informasjonssikkerhet og personvern, og som integrerer dette i den øvrige mål- resultat- og risikostyringen.

KD og HK-dirs samarbeid om å integrere styringen av informasjonssikkerhet og personvern i etatsstyringen er viktig for gjennomføringen av dette formålet.

HK-dirs temarapporter og deltakelse på sektorens forskjellige fora for informasjonssikkerhet, personvern og administrasjon er viktig for å bygge en god sikkerhetskultur.

Formål 6: Sørge for måloppnåelse

Styring av informasjonssikkerhet og personvern har som formål å støtte opp om målene for sektoren og å sørge for at sikkerheten er på det nivået regelverket og departementet forutsetter.

Sikkerhetsnivået bør overvåkes og opprettholdes på et nivå som svarer til disse sikkerhetskravene.

Graden av måloppnåelse og sikkerhetsnivå bør vurderes med utgangspunkt i konsekvenser på sektornivå (se evaluering av konsekvenser på side 6 nedenfor).

Hva innebærer dette?

Dette innebærer å definere hva som er de nødvendige sikkerhetsnivåene for sektoren og overvåke hvordan informasjonssikkerhets- og personvernarbeidet påvirker disse. Å definere sentrale informasjonsverdier som skal sikres vil være en viktig del av dette.

Kravene i Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning definerer minstenivået på informasjonssikkerhet og personvern.

Styringsprosessene

Styringsprosessene i ISO-standarden som ligger til grunn for styringsmodellen er konkrete oppgaver som gjennomføres i et samspill mellom to nivåer. I styringsmodellen er disse nivåene KD og HK-dir. Oppgavene inngår i en syklus for kontinuerlig forbedring[4] og gjennomføres for å oppnå formålene med styringen. Dette er styringsoppgaver som må forstås i sammenheng med hverandre og i sammenheng med formålene i standarden. For å oppnå kontinuerlig forbedring bør prosessene evalueres jevnlig og tilpasses KD og HK-dirs behov.

Prosessen «styre»

Prosessen omfatter de styringsaktivitetene som gir retning til arbeidet med informasjonssikkerhet og personvern.

[4] Denne typen sykluser innenfor IT-styring kategoriseres i styringstrinnene «evaluate-direct-monitor» i styringsstanarder som f.eks. NS-ISO/IEC 38500 og COBIT 2019 i tillegg til NS-ISO/IEC 27014 som styringsmodellen tar utgangspunkt i.

KD

- Beslutter mål for informasjonssikkerhet og personvern på sektornivå
- Beslutter risikoaksept på sektornivå
- Godkjenner plan for håndtering av avdekket risiko og manglende etterlevelse
- Godkjenner endringer i policy for informasjonssikkerhet og personvern i høyere utdanning og forskning og formidler denne i rundskriv
- Vurderer ressursbehov i de årlige statsbudsjettene på bakgrunn av innspill fra HK-dir
- Gir overordnede styringssignaler til institusjonene i etatsstyringen og i øvrig styringsdialog med utgangspunkt i HK-dirs risiko- og tilstandsvurdering av informasjonssikkerhet og personvern, samt direktoratets anbefalinger og forslag

HK-dir

- Foreslår endringer i policy for informasjonssikkerhet og personvern i høyere utdanning og forskning
- Foreslår en plan for håndtering av risiko og manglende etterlevelse som er avdekket i den årlige risiko- og tilstandsvurderingen
    - Planen tar utgangspunkt i departementets risikoaksept
- Innpasser informasjonssikkerhets- og personvernmålene i sektormålene
    - Dette bygger på prosessen evaluere som beskrives nedenfor
    - Gir styringssignaler til virksomhetene for å sikre tilpasning til digitaliserings- og sektormål
- Gir styringssignaler og anbefalinger til virksomhetene for å redusere identifisert risiko og for å lukke avvik
- Gir KD anbefalinger om styring og leverer forslag til:
    - Føringer og krav i tildelingsbrev til virksomheter i sektoren
    - Tilbakemeldinger til den enkelte virksomhet i etatsstyringen

Prosessen «monitorere og rapportere»

Prosessen gjør det mulig for KD og HK-dir å vurdere måloppnåelse og risiko.

KD

- Mottar og vurderer HK-dirs årlige rapport om risiko og tilstand for informasjonssikkerhet og personvern
    - Rapporten omfatter både sektor- og institusjonsnivået
- Kommuniserer behandlingen av rapporten og departementets prioriteringer til HK-dir
- Vurderer informasjon om informasjonssikkerhets- og personvernforhold fra interessenter som f.eks.:
    - Justis- og beredskapsdepartementet, herunder departementenes nettverk for IKT-sikkerhet
    - Kommunal og distriktsdepartementet
    - Etterretnings- og sikkerhetstjenestene (EOS-tjenestene)
    - Direktoratet for samfunnssikkerhet og beredskap
- Gjør selvstendige vurderinger av årlige rapporter og risikovurderinger fra EOS-tjenestene

HK-dir

- Gjør overordnede risikovurderinger på sektornivå, og tilstandsvurderinger på institusjonsnivå, med utgangspunkt i årlige kartlegginger
- Gjør systematiske vurderinger av årlige nasjonale risikovurderinger fra EOS-tjenestene og fra DSB, herunder:
    - NSMs Risiko
    - NSMs "Nasjonalt digitalt risikobilde"
    - PSTs "Nasjonal trusselvurdering"
    - Etterretningstjenestens "Fokus"
- Vurderer risikovurderinger fra andre relevante aktører
- Følger med på endringer i strategiske, organisatoriske og regulatoriske rammebetingelser og hvordan disse påvirker risiko
- Henter inn informasjon om risiko og etterlevelse fra virksomheter som er omfattet av styringsmodellen.
- Vurderer informasjonssikkerheten og personvernet hos virksomhetene som er omfattet av policy for informasjonssikkerhet og personvern i høyere utdanning og forskning.
    - Denne utgjør minstekravene til informasjonssikkerhet og personvern som sektoren skal etterleve[5] og vurderingsgrunnlaget.
- Vurderer informasjon om hendelser, trusler og sårbarheter, herunder informasjon fra tekniske sikkerhetstester og informasjon fra sektorvist responsmiljø (SRM) i Sikt og har en fast dialog med SRM om dette
- Bestemmer måleparametre/styringsparametere[6] og intervaller for disse
- Utarbeider en årlig risiko- og tilstandsvurdering til KD av informasjonssikkerhet og personvern på virksomhets- og sektornivå u.off. (rapporten *Risiko- og tilstandsvurdering – informasjonssikkerhet og personvern i høyere utdanning og forskning*)
- Utarbeider en åpen årlig risiko- og tilstandsvurdering av informasjonssikkerhet og personvern på sektornivå som distribueres til sektoren
    - Informerer interessenter om denne
- Informerer KD om endringer i risikobildet

For å vurdere risiko og måloppnåelse bør dette evalueres med utgangspunkt i de konsekvensene det har på virksomhets- og sektornivået. Dette innebærer at konkrete konsekvenser av risiko bør vurderes for den enkelte informasjonsverdi som er identifisert av HK-dir. Konsekvenser bør i størst mulig grad tallfestes. Risiko og måloppnåelse bør knyttes til andre styringsparametere som benyttes i sektorstyringen for å være relevant, og det er et mål at risiko og måloppnåelse kan uttrykkes kvantitativt.

Konsekvenser kan beskrives konkret gjennom for eksempel antall, omfang og varighet. Mer abstrakte konsekvenser som for eksempel tap av tillit, omdømme og trygghet, kan vurderes i form av grad av tap. For å sammenligne konsekvenser av ulike hendelser, bør samme type og kategorier av konsekvenser benyttes[7].

[5] Et 'baseline'-nivå eller en grunnsikring
[6] 'metrics'
[7] Beskrivelse er basert på NS 5814:2020 Krav til risikovurderinger

Konsekvensvurderingene vil igjen være grunnlaget for de kost-nytte-vurderingene som gjøres av nye sikkerhetstiltak[8].

Prosessen «evaluere og forbedre»

Prosessen innebærer å vurdere nåværende og langsiktig måloppnåelse med utgangspunkt i dagens tilstand og planlagte endringer, og bestemme hvor det er behov for justeringer.

KD

- Sikrer at KDs planer og tiltak tar høyde for informasjonssikkerhetsrisiko og -muligheter
    - Eksempler på dette er nye satsinger på digitalisering i sektoren som kan øke risiko eller som kan ha gevinster som bidrar positivt til sikkerheten
- Responderer på sektorens oppnådde resultater innenfor informasjonssikkerhet og personvern slik disse er rapportert fra HK-dir og prioriterer tiltak

HK-dir

- Sikrer at informasjonssikkerhets- og personvernarbeidet understøtter sektorens målsettinger
- Foreslår nye effektive tiltak til KD gjennom en plan for håndtering av risiko (dokumentet *Risikohåndteringsplan*) og gjennom andre strategiske satsinger
- Gir råd til KD om forhold som krever departementets oppmerksomhet og eventuelle beslutninger

Prosessen «kommunisere»

Prosessen omfatter toveiskommunikasjonen mellom KD og departementets eksterne interessenter og mellom HK-dir og direktoratets eksterne interessenter. Standarden beskriver hvordan man kan benytte informasjonssikkerhetserklæringer til interessentene som en måte å kommunisere informasjonssikkerhet på.

KD

- Informerer departementets eksterne interessenter om hvordan sektorens informasjonssikkerhet og personvern samsvarer med nasjonale krav, definerte målsettinger og sektorens egenart.
    - Vedlikeholder oppdatert standardinformasjon om tilstand i sektoren for å kunne svare på spørsmål fra blant annet Stortinget og media.
    - Sender en årlig erklæring med utgangspunkt i HK-dirs rapportering til:
        - Justis- og beredskapsdepartementet som har samordningsansvaret for digital sikkerhet for sivil side av samfunnet
        - Kommunal og distriktsdepartementet som har ansvar for koordinering av arbeidet med informasjonssikkerhet i forvaltningen
        - Riksrevisjonen som er Stortingets revisjons- og kontrollorgan. De kan kontrollere om departementet, og virksomheter under

[8] Et overordnet eksempel på slik evaluering kan være: Hvilke konkrete skader kan et utpressingsangrep innebære for en viktig sektortjeneste? Hvilke følgekonsekvenser har dette for andre verdier og mål? Hvor mange rammes av skadene, hvor lenge varer skaden, og hvilke kostnader medfører dette? Hvordan er nytten av å redusere risikoen til et akseptabelt nivå sett i forhold til kostnaden? Hvordan er forholdet kost/nytte sett i forhold til andre risikoer?

departementet, ivaretar sitt ansvar for informasjonssikkerhet og personvern i tråd med Stortingets vedtak og føringer.

HK-dir

- Informerer direktoratets/sektorens eksterne interessenter om hvordan sektorens informasjonssikkerhet og personvern samsvarer med nasjonale krav, definerte målsettinger og sektorens egenart
- Sender en kort årlig erklæring til:
    - NSM som har ansvar for ivaretakelse av digital sikkerhet på nasjonalt nivå
    - Digdir som er samordner og pådriver i offentlig sektors arbeid med forebyggende informasjonssikkerhet
- Utvikler rammeverk og anbefaler beste praksis for informasjonssikkerhet og personvern i høyere utdannings- og forskningssektoren
- Informerer sektoren om tiltak som skal iverksettes for å støtte opp om føringer og beslutninger
- I tillegg til en årlig offentlig rapport om sikkerhetstilstanden i sektoren utarbeider HK-dir rapporter om aktuelle tema som har særlig betydning for sektoren.

Vedlegg

A. Om ISO/IEC 27014:2020

Kunnskapsdepartementets styringsmodell for informasjonssikkerhet ble etablert i 2019 med utgangspunkt i standarden ISO/IEC 27014:2013. I 2020 ble standarden oppdatert. Beskrivelsen av styringsmodellen har som følge av dette blitt endret på noen punkter, mens andre har blitt tilpasset høyere utdannings- og forskningssektorens egenart. Dette vedlegget forklarer noen av punktene som avviker fra standarden.

- Beskrivelsen av styringsmodellen følger så langt det passer ISO-standarden med de tilpasningene som er nødvendig for denne sektoren og for styring på sektornivået. Standarden NS/ISO-IEC 27014:2020 er generell og er ment å passe på flere typer virksomheter og konstellasjoner av slike. Der standarden omtaler «enheten» (entity) viser styringsmodellen til høyere utdannings- og forskningssektoren[9]. Standarden omtaler styring av informasjonssikkerhet. I styringsmodellen omfatter dette også styring av personvern og der beskrivelsen av styringsmodellen omtaler informasjonssikkerhet omfatter dette også personvernet. Personvern i styringsmodellen er primært avgrenset til krav i personopplysningsloven og personvernforordningen (GDPR), men inkluderer også sentrale krav i andre lovverk.

- I 2020-versjonen av standarden er ikke lenger revisjon en egen prosess og dette er tatt ut av styringsmodellen. Departementet vurderer selv behovet for å gjennomføre eksterne evalueringer av styringen av informasjonssikkerhet og

[9] Departementet har i 2018 vurdert at rammeverket i ISO/IEC 27014:2013 kan anvendes på den overordnede styringen av informasjonssikkerheten til underliggende virksomheter i høyere utdannings- og forskningssektoren.

personvern. Riksrevisjonens undersøkelser vil i noen tilfeller dekke departementets behov for uavhengig undersøkelse. Styringsmodellen skal ha en prosess for kontinuerlig forbedring, og behov for endringer skal vurderes årlig.

- Den nye versjonen av standarden legger vekt på sammenhengen mellom styringsaktivitetene og ledelsessystem for informasjonssikkerhet (ISMS) basert på ISO/IEC 27001. Kunnskapsdepartementets styringsmodell benyttes på sektornivået og har ikke samme tilknytning til de enkelte virksomhetenes ISMS. Styringsmodellen beskriver forholdet mellom KD som «styrende enhet» (governing body) i standarden og HK-dir som «toppledelse» (top management). Høyere utdannings- og forskningssektoren utgjør standardens «enhet» (entity). ISMS benyttes ikke på sektornivå og det er det enkelte styre/toppledelse ved hver virksomhet som har ansvar for ISMS på virksomhetsnivå. Standardens omtale av ISMS benyttes derfor ikke i styringsmodellen.

- I siste versjon av standarden har prinsippene for styring av informasjonssikkerhet fått benevnelsen målsettinger eller formål («objectives»). I styringsmodellen brukes begrepet formål.

- De generelle innledende klausulene i standarden er ikke gjengitt i styringsmodellen.

B. Årshjul

Styringsprosessene og samarbeidet mellom KD og HK-dir gjentas årlig i et årshjul. Hovedelementene i dette er:

Kvartal	KD	HK-dir
1		kartlegger risiko og etterlevelse hos virksomhetene;
2	behandler rapport og beslutter risikoaksept; godkjenner risikohåndteringsplan; gir tilbakemeldinger til virksomhetene i etatsstyringen;	leverer risiko- og tilstandsvurdering samt risikohåndteringsplan til KD i tråd med risikoaksept; leverer anbefalinger til virksomhetene; leverer anbefalinger om KDs styringssignaler innenfor informasjonssikkerhet og personvern; publiserer offentlig rapport;
3	godkjenner eventuelle endringer i policy;	foreslår eventuelle endringer i policy;
4	gir føringer i tildelingsbrev.	leverer anbefalinger til KD om hvilke føringer som skal gis i tildelingsbrev

		gjeldende virksomhetenes arbeid med informasjonssikkerhet og personvern; publiserer temarapporter; leverer budsjettinnspill; kartlegger risiko og etterlevelse hos virksomhetene.

Samarbeidet følges opp i halvårlige møter kalt ledelsens gjennomgang.

C. Kontroll

I forbindelse med monitoreringsprosessen kartlegger HK-dir etterlevelse av krav med utgangspunkt i selvrapportering fra virksomhetene samt møter der virksomhetene svarer på spørsmål. Kartleggingen har som formål å gi oversikt over risiko og tilstand, og er ikke en formell kontroll av etterlevelsen av krav.

En formell kontroll innebærer å gjennomføre kontrollhandlinger som bekrefter at etterlevelsen av krav er slik virksomheten rapporterer.

KD har gitt denne kontrolloppgaven som oppdrag til NOKUT for at den skal være uavhengig av styringsoppgaven til HK-dir. En viktig oppgave for kontrollen er å bekrefte eller finne avvik i den situasjonsforståelsen som styringsmodellen gir.

NOKUT er imidlertid som virksomhet omfattet av HK-dirs styring av informasjonssikkerhet og personvern, men HK-dir har ikke myndighet over kontrolloppdraget og skal ikke kunne påvirke dette. Kontrollen har omtrent tilsvarende uavhengighet som en internrevisor ved at den er uavhengig fra de områdene og prosessene som skal kontrolleres[10], men er ikke definert som internrevisjon. Det er viktig for departementet å skille rollene styring og kontroll, samt å ivareta kontrollens uavhengighet så langt det lar seg gjøre innenfor samme sektor.

NOKUT bestemmer selv omfanget på kontrollene og metode, men kontrollene skal kunne gi departementet en bekreftelse på etterlevelse av krav i policy. NOKUTs kontroller bør gi et representativt bilde over tid.

Virksomhetene som er omfattet av styringsmodellen rapporterer til HK-dir og har ingen fast rapportering til NOKUT. NOKUT innhenter den virksomhetsinterne dokumentasjonen som er nødvendig hos de virksomhetene som kontrolleres i tillegg til å gjennomføre stedlig kontroll i henhold til egen risikovurdering.

I arbeidet med å sikre etterlevelse av krav kan arbeidsdelingen oppsummeres med:

- HK-dir kartlegger graden av etterlevelse i hele sektoren gjennom tillitsbasert dialog.

[10] Jf. Finansdepartementets rundskriv r-117 om internrevisjon i statlige virksomheter

- NOKUT gjennomfører uavhengige kontroller av etterlevelsen ved enkelte virksomheter gjennom utvalgte kontrollhandlinger.
- HK-dir gir departementet oversikt over etterlevelse.
- NOKUT gjennomfører kontroller av etterlevelse ved den enkelte institusjon og leverer rapporter om dette til departementet.

KD kan vurdere den samlede belastningen som styring og kontroll innebærer for virksomhetene og tilpasse kontrollbehovet deretter.