Oversikt over Kunnskapsdepartementets styringsmodell for informasjonssikkerhet

Dette notatet presenterer en oversikt over KDs styringsmodell for informasjonssikkerhet som bygger på ISO/IEC 27014-standarden. Omfanget av styringsmodellen er KD og Units styring av informasjonssikkerhet i virksomhetene under KDs avdeling for Eierskap i høyere utdanning og forskning.

KD og Units roller i sektorstyringen av informasjonssikkerhet

KD har eier og etatsstyringsansvaret for alle virksomhetene som omfattes av styringsmodellen for informasjonssikkerhet, og et sektoransvar for høyere utdannings og forskningssektoren.

Unit har ifølge vedtektene et overordnet forvaltningsansvar på vegne av Kunnskapsdepartementet for IKT-området, herunder informasjonssikkerhet og personvern, og har myndighet til å treffe beslutninger innenfor disse områdene.

Styringsmodellen for informasjonssikkerhet beskriver mer konkret hvordan disse rollene praktiseres.

ISO/IEC 27014:2013

ISO-standarden beskriver hvordan styring av informasjonssikkerhet må passe inn i andre styringsmodeller innenfor virksomheten og hvorfor innpassing i virksomhetsmålene derfor er spesielt viktig. Standarden bygger på de samme overordnede prinsippene for 'corporate governance' som KDs andre styringsprosesser (risikostyring, økonomistyring, internkontroll, IKT-styring mm.) og kan derfor integreres i årshjul og etablerte rutiner forholdsvis enkelt. Ettersom styringsmodellen bygger på en internasjonal standard som harmonerer med andre standarder for de nevnte styringsprosessene vil den også være kompatibel dersom KD senere ønsker å videreutvikle disse med utgangspunkt i internasjonal beste praksis.

De overordnede generiske målene for styring av informasjonssikkerhet er i følge i standarden å:

- Innpasse mål og strategi for informasjonssikkerhet i virksomhetsmål og -strategi ("strategic alignment")
    - Dette innebærer at informasjonssikkerheten skal bidra til å nå de målene, og underbygge de strategiene, som fastsettes på sektornivået og at målene for informasjonssikkerhet må passe sammen med sektormålene. Det innebærer dermed også at man må tenke innebygd informasjonssikkerhet i digitaliseringstiltak.
- Verdiskapning for styrende enhet og interessenter ("value delivery")
    - Dette innebærer å sikre forutsetningene for den gevinstrealisering man ønsker å oppnå ved at sikkerhetsrisikoen for disse gevinstene håndteres.
- Sikre at informasjonsrisiko blir møtt på riktig måte ("accountability")
    - Dette innebærer at man kan forsikre seg om at det er de riktige sikringstiltakene som iverksettes i tilstrekkelig grad for å håndtere risiko.

De ønskede resultatene fra effektiv styring av informasjonssikkerhet er ifølge standarden:

- Den styrende enheten er synlig eller åpen om sikkerhetstilstanden
    - Dette innebærer at interessenter og samarbeidspartnere kan ha tillit til sektoren ut fra egen åpenhet om sikkerhetstilstanden.
- En fremoverlent tilnærming til beslutninger om informasjonsrisiko
    - Dette innebærer å være i stand til å håndtere risiko effektivt
- Effektive investeringer i informasjonssikkerhet
    - Dette innebærer å gjøre riktige investeringer som tar utgangspunkt i risikostyring
- Etterlevelse av eksterne krav (lover, regler og kontrakter)
    - Dette innebærer internkontroll for å sikre etterlevelse

Standarden beskriver i mer detalj prosessene for styring av informasjonssikkerhet, og presenterer seks prinsipper som det anbefales å legge til grunn for styringen.

Prinsippene for KD og Units styring av informasjonssikkerhet

Beskrivelsen av prinsippene bygger på standarden og er tilpasset KD og Units anvendelse av denne på sektornivået.

Prinsipp 1: Etabler informasjonssikkerhet som omfatter hele sektoren

Prinsippet skal sikre at informasjonssikkerhet er en integrert del av sektoren og omfatter hele denne. Det legger vekt på at informasjonssikkerhet skal etableres innenfor hele spekteret av sektorens aktiviteter, også utenfor de tradisjonelle organisatoriske rammene ettersom informasjon håndteres av eksterne parter.

Dette innebærer en form for styring av informasjonssikkerheten i alle underliggende virksomheter og selskaper i sektoren, herunder også underleverandører. Styringen må tilpasses tilknytningsformen.

Gjennomføringen av dette prinsippet skjer gjennom de ordinære styringslinjene:

- Unit: Direkte styring fra KD
- Diku, NOKUT, NFR, NUPI og FEK: Sektorstyring fra Unit, etatsstyring fra KD
- Statlige UH-inst.: Sektorstyring fra Unit, etatsstyring fra KD
- Private UH-inst.: Tilskuddsforvaltning og dialog fra KD
- Aksjeselskaper: Sektorstyring fra Unit i tråd med statens prinsipper for eierstyring, eierstyring fra KD og avtalestyring
- 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 styres gjennom *hele verdikjeden* ettersom risikoen for informasjonsverdiene ikke kjenner de organisatoriske grensene. For å håndtere dette må ansvar og ansvar for etterlevelse ("responsibility and accountability" i standarden) fastsettes klart og tydelig. KD og Unit må her ha en risikobasert tilnærming til hvordan man prioriterer oppmerksomheten innenfor alle delene av sektoren.

Hva innebærer dette?

For å etablere informasjonssikkerhet innenfor alle deler av høyere utdanning og forskning som er omfattet av KDs ansvar, må styringen av informasjonssikkerhet 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 deler av sektoren må omfattes i risiko- og sårbarhetsanalyser, og resultatene må ligge til grunn for styringen.

Prinsipp 2: Anta en risikobasert tilnærming

Dette prinsippet innebærer at beslutninger om styring av informasjonssikkerhet skal bygge på risikovurderinger og at sikkerhetsnivået skal bestemmes ut fra en organisasjons risikoaksept. Dette er fullt i tråd med de styringsprinsipper som gjelder i staten, men KDs risikoaksept vil måtte utvikles og defineres i takt med kvaliteten på de risikovurderingene som gjøres og i takt med utviklingen av egen styring. Det vil si at den risikobaserte tilnærmingen må utvikles i takt med innføringen av styringsmodellen. For at styringen på sektornivået skal være risikobasert må den ta utgangspunkt i risikovurdering på dette nivået.

For å oppnå resultater innenfor digitalisering må man ha et bevisst forhold til risikoaksept, og denne må nødvendigvis ligge høyere enn ingen risiko. For at ledelsen skal kunne akseptere en viss risiko må kvaliteten på beslutningsgrunnlaget være god, og de risikoreduserende tiltakene må være systematiske og etterprøvbare. Sektoren oppnår i dag resultater gjennom forskjellig grad av risikovillighet, men innenfor dagens styring og ledelse av informasjonssikkerhet ligger risikoaksepten ofte implisitt i beslutningene ved at den ikke er vurdert god nok eller i det hele tatt, og heller ikke på riktig ledelsesnivå.

Hva innebærer dette?

En gjennomføring av prinsippet vil innebære en systematisk behandling av risikovurderinger på sektornivå i KDs årshjul, og en gjennomføring av oppgavene og arbeidsdelingen i monitoreringsprosessen i standarden. Behandlingen av risikovurderingen vil innebære en definering av risikoaksept. For å kunne behandle risiko på riktig nivå må kvaliteten på risikovurderingene på alle nivåer i sektoren bli bedre, og Unit må vurdere måter for sektoren å aggregere risiko opp fra systemnivået til institusjonsnivået på en hensiktsmessig måte for at toppledere i sektoren skal ha et reelt beslutningsgrunnlag. Tilsvarende vil Unit og KD måtte forbedre sin metodikk for risikovurderinger på sektornivået årlig gjennom de faste oppgavene i styringsmodellen.

Prinsipp 3: Gi retning til investeringsbeslutninger

Dette prinsippet innebærer at det etableres en investeringsstrategi for informasjonssikkerhet med utgangspunkt i de målbilder som er satt. Formålet er at finansieringen skal henge sammen med den generelle styringen av informasjonssikkerhet.

Hva innebærer dette?

For KD vil dette innebære å vurdere risikovurderingen og planen som skal håndtere denne, nye forslag og evalueringene av måloppnåelse opp mot finansieringsbehovet. Her vil det alltid være større behov enn finansiering, så risikovurderingen vil være sentral for å kunne vurdere hva som skal nedprioriteres på kort sikt. En investeringsstrategi vil bidra til å planlegge tidshorisonten for investeringene bedre, innenfor rammene av statlig budsjettarbeid.

Investeringsstrategien for informasjonssikkerhet inngår som et område i KDs digitaliseringsstrategi, og handlingsplanen for informasjonssikkerhet er en del av handlingsplanen for digitalisering i sektoren som revideres årlig.

Prinsipp 4: Sikre etterlevelse av interne og eksterne krav

Dette innebærer å sikre at informasjonssikkerhetspolicy og -praksis er i tråd med gjeldende lover, regler og andre forpliktelser. For å ivareta prinsippet anbefales det at KD bestiller uavhengige sikkerhetsrevisjoner for å forvisse seg om at sektoren møter interne og eksterne krav.

Dette prinsippet er i tråd med KDs praksis for å gjennomføre evalueringer av egen forvaltning og av UH-sektorens forvaltning, men vil avhenge av finansieringen av disse, og dermed av prinsipp 3. Økonomireglementet pålegger statlige virksomheter å bruke evalueringer som virkemidler for informasjonsinnhenting til mål- og resultatstyringen. Bestemmelser om økonomistyring i staten er mer konkret: "Virksomheten skal sørge for at det gjennomføres evalueringer for å få informasjon om effektivitet, måloppnåelse og resultater innenfor hele eller deler av virksomhetens ansvarsområde og aktiviteter. (…) Evalueringer kan utføres av interne eller eksterne fagmiljøer". Departementets egne retningslinjer fastsetter imidlertid at evalueringer som hovedregel skal gjennomføres av eksterne.

En evaluering har ikke i utgangspunktet like klart definerte rammer som en sikkerhetsrevisjon, men dersom man legger til grunn at den skal avdekke effektivitet, måloppnåelse og resultater, og man følger metodeanbefalinger fra Finansdepartementet vil evalueringer langt på vei kunne nå målet med prinsippet. I tillegg til dette kommer Riksrevisjonens forvaltningsrevisjoner som kontrollerer departementenes etterlevelse, også på sektornivå, men disse følger Riksrevisjonens egne prioriteringer og gir ikke KD systematisk forsikring med utgangspunkt i egne risikovurderinger. Frekvens og omfang av evalueringer skal bestemmes ut fra virksomhetens egenart, risiko og vesentlighet ifølge Finansdepartementet.

Hva innebærer dette?

En gjennomføring av prinsippet innebærer å etablere en langtidsplan for evalueringer og uavhengig revisjon som oppdateres årlig i tråd med endringer i risikovurderingene.

Prinsipp 5: Skape et miljø som er positivt til sikkerhet

Dette prinsippet handler om å koordinere de forskjellige aktørene og interessentene, og å skape et miljø som legger til rette for måloppnåelse. Prinsippet virker å handle mindre om holdningsskapende arbeid og sikkerhetskultur og mer om ledelse og organisasjonskultur. Resultatet av å gjennomføre dette prinsippet vil måtte være at informasjonssikkerhet blir en naturlig del av organisasjonskulturen og virksomhetsstyringen på samme måte som andre styringsprosesser slik som f.eks. budsjettering, økonomistyring og internkontroll.

Hva innebærer dette?

Å kunne arbeide med dette prinsippet vil måtte innebære å forstå hva som må til for å skape et miljø som legger til rette for måloppnåelse innenfor informasjonssikkerhet, og dette prinsippet bør beskrives nærmere i løpet av innføringen av de andre prosessene og prinsippene slik at man kan identifisere kritiske suksessfaktorer og evaluere hva som er effektivt. Med utgangspunkt i nasjonale risikovurderinger og undersøkelser kan man si at informasjonssikkerhetsnivået ennå ikke er helt modent, og at man ikke skal undervurdere hva det vil si å ta på alvor gjennomføringen av et slikt prinsipp. KD og Units regelmessige behandling av styringsmodellen på ledelsesnivå er et viktig tiltak for gjennomføringen av dette prinsippet.

Prinsipp 6: Vurdere gjennomføringsevne opp mot målbilder

Dette prinsippet handler om at KD skal vurdere resultatene av informasjonssikkerhetsarbeidet opp mot "business impact", altså gjennomføre konsekvensanalyser av arbeidet.

Hva innebærer dette?

Å gjennomføre dette prinsippet innebærer å definere hva som er de nødvendige sikkerhetsnivåene for sektoren og hvordan informasjonssikkerhetsarbeidet påvirker disse. Å definere sentrale informasjonsverdier vil være en viktig del av dette. For å kunne vurdere resultater er det nødvendig med klare mål. Det første skrittet i gjennomføringen av prinsippet vil dermed være Handlingsplan for digitalisering og Units plan for håndtering av avdekket risiko.

Styringsprosessene

Alle prosessene i styringsmodellen inngår i den helhetlige sektorstyringen av informasjonssikkerhet, er styringsoppgaver, og må forstås i sammenheng med hverandre og prinsippene i standarden. Prosessene i standarden bør inngå i en årlig syklus for kontinuerlig forbedring der de evalueres jevnlig.

Prosessen styre

Prosessen omfatter de styringsaktivitetene som gir retning til informasjonssikkerhetsarbeidet.

Kunnskapsdepartementet

- Beslutter risikoaksept på sektornivå
- Godkjenner plan for håndtering av avdekket risiko og -policy på sektornivå på bakgrunn av forslag fra Unit.
- Vurderer ressursbehov i de årlige statsbudsjettene på bakgrunn av innspill fra Unit.
- Gir styringssignaler til institusjonene i etatsstyringen og i øvrig styringsdialog med utgangspunkt i Units risiko- og tilstandsvurdering av informasjonssikkerhet og personvern

Unit

- Utvikler og implementerer revidert Handlingsplan for digitalisering i høyere utdanning og forskning herunder tiltaksplan for informasjonssikkerhetsområdet og -policy på sektornivå (se nedenfor)
- Foreslår en plan for håndtering av risiko som er avdekket i den årlige risikovurderingen
- Innpasser informasjonssikkerhetsmålene i sektormålene
    - Bygger på aktiviteten evaluere
    - Gir styringssignaler til virksomhetene for å sikre tilpasning/'alignment' til digitaliserings- og sektormål

    - Gir styringssignaler til virksomhetene for å redusere identifisert risiko som er høyere enn akseptabelt nivå
- Har på vegne av KD en ledende rolle og sikrer god brukermedvirkning i informasjonssikkerhets- og personvernarbeidet i sektoren med sikte på måloppnåelse
- Fremmer en positiv informasjonssikkerhetskultur (bl.a. årlig sikkerhetsforum)
- Kan foreta «stikkprøver» ved mistanke om avvik innenfor informasjonssikkerhet (for eksempel evaluering av enkeltområder i ledelsessystemet).

Om strategi og policy

Strategi og policy er toppdokumentene i to separate hierarkier med styrende dokumenter som utfyller hverandre. Tabellen nedenfor forklarer forholdet mellom dokumentene uten å være uttømmende eller definere begrepene. Strategien er en konkret plan for hvordan man skal nå definerte målsettinger for informasjonssikkerhet som støtter opp om digitaliseringsstrategien og dermed sektormålene og som tar utgangspunkt i identifisert risiko. Strategien er avgrenset i tid og fornyes jevnlig og gjerne fullstendig. Policyen er stående føringer, prinsipper og anbefalinger for hvordan informasjonssikkerheten skal ivaretas for å opprettholde en definert sikkerhetstilstand, herunder minstekravene til informasjonssikkerhet og personvern. Policyen setter et "baselinenivå", er ikke tidsavgrenset og endres inkrementelt og sjelden. Når man opererer med begge sett med styrende dokumenter bør strategien rendyrke målstyring mot prioriterte mål mens formuleringer om at "informasjonssikkerheten i sektoren skal være…" holdes i policyen.

Mål- og resultatstyring	**Regelstyring**
(Regjeringens prioriteringer)	(Regelverk)
(Sektormål)	(Krav og føringer)
Digitaliseringsstrategi	Informasjonssikkerhetspolicy for sektoren
Handlingsplan for digitalisering, område Informasjonssikkerhet og personvern	Standarder (f.eks. veileder i ledelsessystem)
Risikohånderingsplan	Rutiner (f.eks. vedleggene til veilederen i ledelsessystem)

Prosessen monitorere og rapportere

Prosessen gjør det mulig for KD og Unit å vurdere måloppnåelse og risiko.

Kunnskapsdepartementet

- Vurdere Units rapporter og risikovurdering
- Vurdere informasjon om informasjonssikkerhetsforhold fra interessenter som f.eks.:
    - JD
    - Departementenes nettverk for IKT-sikkerhet
    - KMD
    - NSM, PST, Etterretningstjenesten og DSB
- Gjøre selvstendige vurderinger av åpne risikovurderinger

Unit

- Systematisk vurdere årlige nasjonale risikovurderinger fra sikkerhetstjenestene
    - NSMs Risiko
    - NSMs "Helhetlig risikobilde"
    - PSTs "Åpen trusselvurdering"
    - Etterretningstjenestens "Fokus"
    - DSBs rapporter
- Vurdere risikovurderinger fra andre relevante aktører som f.eks.
    - NSRs "Mørketallsundersøkelsen"
    - Mnemonic "Security report"
    - Enisa "Threat Landscape"
    - Internasjonale sikkerhetsrapporter fra FireEye, Kaspersky, Microsoft m.fl.
- Gjøre overordnede risikovurderinger for institusjonene på sektornivå og tilstandsvurderinger på institusjonsnivå med utgangspunkt i årlige kartlegginger
- Vurdere hvordan informasjonssikkerheten i sektoren ligger i forhold til et 'baseline'-nivå eller fastsatt minstenivå som er de nasjonale kravene til informasjonssikkerhet, herunder personvernreglene.
- Vurdere informasjon om hendelser, trusler og sårbarheter fra sektorvist responsmiljø
- Vurdere informasjon fra penetrasjonstesting
- Utarbeide en årlig risiko- og tilstandsvurdering til KD av informasjonssikkerhet og personvern på virksomhets- og sektornivå
- Rapportere til KD om endringer i risikobildet

Prosessen evaluere og forbedre

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

Kunnskapsdepartementet

- Sikrer at KDs planer og tiltak tar høyde for informasjonssikkerhetsproblemstillinger
    - Eksempler på dette er nye satsinger på digitalisering i sektoren
- Responderer på sektorens oppnådde resultater innenfor informasjonssikkerhet og personvern rapportert fra UNIT, prioriterer og initierer tiltak

Unit

- Sikrer at informasjonssikkerheten understøtter sektorens målsettinger
    - Dette innebærer at informasjonssikkerheten støtter og opprettholder digitaliseringsstrategien for UH-sektoren
        - Evaluere hvordan arbeidet støtter opp under digitaliseringsstrategien (det legges til grunn at Unit og KD løpende evaluerer hvordan digitaliseringsstrategien støtter opp under sektormålene).

- Systematisk gjennomføre tiltak som støtter opp under måloppnåelsen i digitaliseringsstrategien gjennom årlig revisjon av handlingsplan og tiltak på informasjonssikkerhetsområdet
- Foreslår nye effektive informasjonssikkerhetstiltak til KD gjennom plan for håndtering av avdekket risiko

Prosessen kommunisere

Prosessen omfatter toveiskommunikasjonen mellom de styrende enhetene og interessentene. Standarden beskriver og gir to eksempler på informasjonssikkerhetserklæringer til interessentene som en måte å kommunisere informasjonssikkerhet.

Kunnskapsdepartementet

- Informerer eksterne interessenter om at sektoren praktiserer et informasjonssikkerhetsnivå i samsvar med nasjonale krav, definerte målsettinger og sektorens egenart.
    - Vedlikeholde standardinformasjon (flak) til:
        - Stortinget
        - Regjeringen
        - Riksrevisjonen
        - JD og NSM som har ansvar for ivaretakelse av informasjonssikkerhet på nasjonalt nivå
        - KMD og Difi som har ansvar for informasjonssikkerhet i statsforvaltningen
- Behandler resultater fra eksterne gjennomganger som har identifisert informasjonssikkerhetsutfordringer og vurderer behov for korrigerende tiltak
    - Riksrevisjonens gjennomganger
    - JDs evalueringer
    - KMDs evalueringer
- Er kjent med krav i regelverk, interessenters forventninger og sektorens behov med hensyn til informasjonssikkerhet

Unit

- Kommuniserer gjennom en kort årlig erklæring til eksterne interessenter at sektoren praktiserer et informasjonssikkerhetsnivå i samsvar med nasjonale krav, definerte målsettinger og sektorens egenart
- Varsler KD og sektoren om resultater fra eksterne gjennomganger som har identifisert informasjonssikkerhetsutfordringer og ber om korrigerende tiltak
- Utvikler rammeverk og foreslår beste praksis for informasjonssikkerhet og personvern
- Informerer KD, og gir råd og praktisk støtte til sektoren om krav i regelverk, annen regelverksinformasjon, interessenters forventninger og virksomhetens behov med hensyn til informasjonssikkerhet
- Gir råd til KD om forhold som krever departementets oppmerksomhet og eventuelle beslutninger

- Informerer, gir råd og praktisk støtte til sektoren om tiltak som skal iverksettes for å støtte opp om føringer og beslutninger
- I tillegg til årlig offentlig rapport om sikkerhetstilstanden i sektoren vurderer Unit behovet for ad-hoc rapporter som behandler aktuelle tema av interesse for sektoren

Prosessen forsikre

Prosessen "Forsikre" er ikke utarbeidet for KD og Unit, men handler om å bestille ekstern revisjon. Den overlapper i stor grad med prinsipp 4 som handler om å etterleve eksterne krav. Denne prosessen bør utarbeides og innføres til slutt i innføringsplanen da en har som mål å evaluere måloppnåelsen som styringsmodellen skal sikre.

Prosessen har som formål å etterprøve om de målene og tiltakene som inngår i KD og Units sektorstyring og forvaltning er tilstrekkelige for å oppnå det ønskede sikkerhetsnivået. Med utgangspunkt i standarden kan oppgavene i denne styringsprosessen være:

Kunnskapsdepartementet

- Bestiller revisjon eller uavhengig evaluering av hvordan KD ivaretar sitt ansvar for å oppnå ønsket sikkerhetsnivå.

Unit

- Støtter de revisjonene og evalueringene som KD bestiller.