DIGITALISERINGSSTYRELSEN

Vejledning om den praktiske tilrettelæggelse af tilsynet med informationssikkerheden

Vejledningen og tilhørende bilag skal betragtes som inspiration og støtte til den overordnede vejledning "Departementets tilsyn med informationssikkerheden på ministerområdet" af 2015. Vejledningen giver eksempler på den praktiske tilrettelæggelse af tilsynet med informationssikkerheden og er udviklet i maj 2015 på baggrund af National strategi for cyber- og informationssikkerhed af december 2014.

Digitaliseringsstyrelsen er ansvarlig for vejledningens form og indhold, som er blevet til i et samarbejde med en referencegruppe bestående af Justitsministeriet, Forsvarsministeriet, Erhvervs- og Vækstministeriet og Skatteministeriet. Datatilsynet har deltaget som observatør.

Indledning

De overordnede rammer for departementets tilsynsansvar med styring af informationssikkerheden på ministerområdet er beskrevet i vejledningen "Departementets tilsyn med informationssikkerheden på ministerområdet". Ifølge vejledningen skal departementet som udgangspunkt planlægge, gennemføre og dokumentere tilsynet. Den praktiske udførelse af tilsynet kan dog uddelegeres, men det overordnede tilsyns- og styringsansvar påhviler departementet.

Denne vejledning og tilhørende bilagsmateriale skal betragtes som inspiration og støtte til departementets etablering af tilsynsprocesser. Vejledningen tager udgangspunkt i god praksis fra offentlige myndigheders tilrettelæggelse af tilsyn. Hensigten med vejledningen er derfor ikke at give detaljerede retningslinjer til hvordan tilsynet skal gennemføres, da ministerområderne ikke er ens, hverken hvad angår størrelse, organisering eller opgavernes karakter.

Tilsynsindsats

For at føre effektivt tilsyn med de områder af ministeriet, der er særligt kritiske, og for at der ikke bruges unødige ressourcer på områder, der fungerer tilfredsstillende, er det nødvendigt at fastlægge omfanget af tilsynsindsatsen. Derved sikres, at tilsynet er tilstrækkeligt i omfang og gennemføres med den nødvendige kvalitet.

Tilsynsindsatsen beror på de enkelte institutioners strategiske, økonomiske og forretningsmæssige betydning på ministerområdet. Eksempelvis vil institutioner, der driver national kritisk infrastruktur, indgå i en systematisk og tilbagevendende tilsynsfrekvens.

Tilsynsindsatsen besluttes bl.a. på baggrund af aktuelle forhold vedrørende informationssikkerheden og den løbende opfølgning på bemærkninger fra revisions- og tilsynsmyndigheder.

Tilsynet kan på baggrund af vurderingsgrundlaget gennemføres som "normalt tilsyn" eller "udvidet tilsyn". Udgangspunktet må oftest forventes at falde ind under "normalt tilsyn", hvorfor denne vejledning beskriver dette.

Normalt tilsyn
Tilsynet gennemføres med de basale undersøgelser, svarende til normal drift. Dette begrundes bl.a. med, at der ikke har været iagttaget kritiske sikkerhedshændelser eller bemærkninger, der kan føre til et udvidet tilsyn.

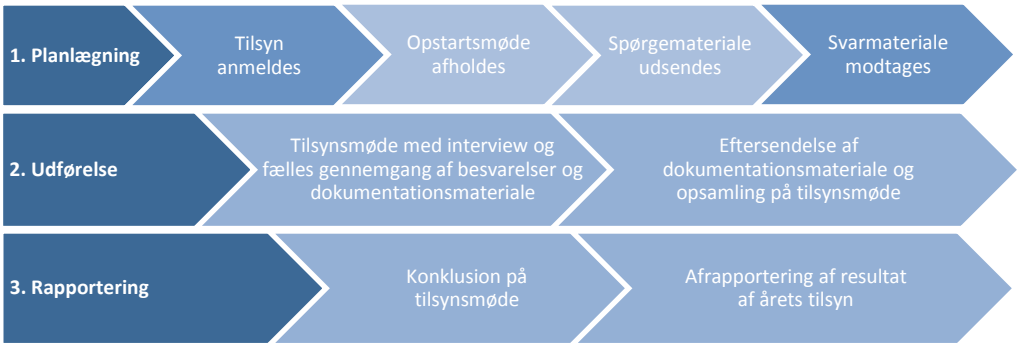
Udvidet tilsyn
Tilsynet gennemføres dybere og bredere, svarende til risikobetonet drift. Dette begrundes bl.a. med, at styring af informationssikkerhed er mindre tilfredsstillende og der eventuelt har været kritiske bemærkninger fra revisions- og tilsynsmyndigheder.

På baggrund af en vurdering af den aktuelle situation kan der eventuelt være behov for et udvidet eller et såkaldt ad-hoc tilsyn. Dette kan eksempelvis betyde, at der foretages særskilte undersøgelser af sikkerhedshændelser eller der følges op på særligt kritiske revisions- og tilsynsbemærkninger.

Tilrettelæggelse

Tilrettelæggelse af et tilsynsforløb kan eksempelvis opdeles i tre trin og en række aktiviteter, som illustreret i nedenstående diagram. De tre trin sikrer, at tilsynet sker i dialog med institutionerne og samtidig er systematisk og tilstrækkeligt. Aktiviteterne under de enkelte trin skal ses som inspiration og bør tilpasses i forhold til den enkelte tilsynsopgave.

Procesdiagram for tilrettelæggelse af tilsyn:



1. *Planlægning*
   Første trin i et tilsynsforløb er planlægning, der omfatter de aktiviteter, der går forud for afholdelse af det formelle tilsynsmøde i trin 2. I planlægningsdelen varsles tilsynet, og der afholdes eventuelt et opstartsmøde, hvorpå formen for det praktiske tilsynsforløb og rammespørgsmål drøftes. Herefter fremsendes spørgeskema til institutionen, der besvarer og returnerer skemaet med tilhørende dokumentationsmateriale.

2. *Udførelse*
   Andet trin er afholdelse af et formelt tilsynsmøde med interview og fælles gennemgang af udfyldte svar i spørgeskemaet samt dokumentation herfor. Som opsamling eftersendes eventuelt uddybende svar og dokumentationsmateriale.

3. *Rapportering*
   Tredje trin omhandler konklusion på tilsynsmøde og opsamling på årets tilsyn. Efter afslutning på et tilsynsmøde udarbejdes fx en konklusion i notatform, der er baseret på besvarelse af spørgeskema, uddybende spørgsmål og dokumentationsmateriale. Hertil afgiver institutionen høringssvar. Årets tilsyn afsluttes med en samlet afrapportering.

Vurderingsgrundlag
Der føres tilsyn i overensstemmelse med vejledningen "Departementets tilsyn med informationssikkerheden på ministerområdet" med henblik på at vurdere modenhedsniveauet for ledelsens styring af informationssikkerheden.

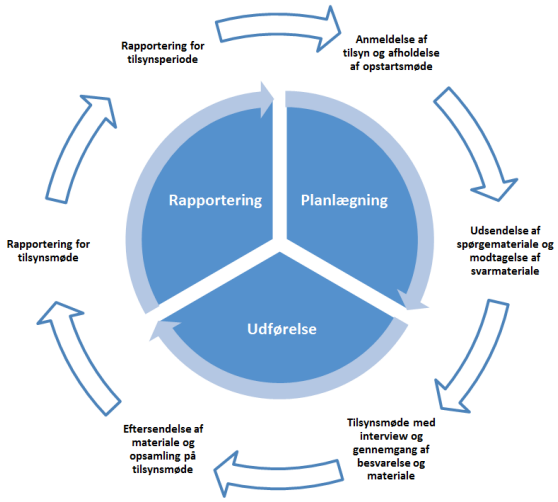
I vurderingsgrundlaget opstilles kriterier til udformning af en spørgeramme, som primært har fokus på at vurdere styringen af de organisatoriske og administrative forretningsgange og ikke de tekniske detaljer.

Kriterierne for spørgerammen konkretiseres i en række spørgsmål, der eksempelvis omfatter krav til styring og efterlevelse af persondataloven, gældende standard for informationssikkerhed, regeringens sikkerhedsinitiativer og eventuelle bemærkninger fra revisions- og tilsynsmyndigheder.

Spørgerammen tilpasses den enkelte institutions størrelse, organisering og opgavernes karakter og bør fastlægges i dialog med institutionen.

Det samlede grundlag for tilsynets vurdering er bl.a. baseret på institutionens besvarelse af spørgeskemaet og tilhørende dokumentation.

Plan for tilsynsaktiviteter
Tilrettelæggelsen af tilsynsaktiviteterne bør fremgå af en plan, der giver et samlet overblik over tilsynsindsatsen, og hvilke aktiviteter der skal udføres hvornår. Hovedaktiviteterne i planen kan eventuelt illustreres ved et årshjul, for at vise, at der arbejdes kontinuerligt og systematisk med tilsynet.



Mål og rapportering
Tilsynsaktiviteterne afrapporteres regelmæssigt til departementet på baggrund af de opstillede mål. Særlige risici, som er identificeret på ministerområdet, gennem kritiske revisionsbemærkninger og mangelfuld styring med informationssikkerheden kan beskrives i statusrapporteringer.

Årets tilsynsaktiviteter afsluttes med en rapportering til departementschefen, hvori der samles op på resultater fra tilsynsperioden i en overordnet konklusion for ministerområdet.

Bilagsmateriale

I bilagsmaterialet kan der hentes hjælp til udformning af en spørgeramme for tilsynet og henvisning til vejledninger, information og hjælpemateriale.

Bilagsmaterialet skal opfattes som inspiration og støtte ved udarbejdelse af en spørgeramme for tilsynet. Det er derfor frivilligt i hvilket omfang og form emner og spørgsmål indgår i en spørgeramme.

Det udvalgte materiale har fokus på ledelsens overordnede styring og tager udgangspunkt i en række generelle krav til styring af informationssikkerheden, som går på tværs af ministerområderne.

Bilagsmaterialet er således ikke en fyldestgørende liste over emner og spørgsmål, hvorfor spørgerammen skal suppleres og tilpasses i forhold til tilsynsopgavens karakter. Ligeså er listen af emner og spørgsmål ikke opstillet i en prioriteret rækkefølge, men må afhænge af tilsynets karakter og fokusområder.

Bilagsmateriale:

Bilag 1: Love og bestemmelser vedrørende informationssikkerhed

Bilag 2: Initiativer fra cyber- og informationssikkerhedsstrategi

Bilag 3: Guide til implementering af ISO27001

Bilag 4: Opfølgning på revisions- og tilsynsbemærkninger

Bilag 5: Henvisninger til information, vejledninger og hjælp

Bilag 1: Love og bestemmelser vedrørende informationssikkerhed

Lovgivningen om informationssikkerhed handler blandt andet om beskyttelse af den enkelte borger og informationer, der er vigtige for landets sikkerhed og samfundets værdier, samt informationer, der er interessante for eftertiden og for offentligheden.

Både persondataloven og særregler i anden lovgivning sætter grænser for, hvilke oplysninger der må indgå, og hvad de må bruges til, herunder f.eks. hvornår oplysninger må videregives.

Lovgivningen understreger dermed behovet for informationssikkerhed og har indvirkning på, hvorledes politik, strategi og sikkerhed udformes i den enkelte institution.

Uanset hvilken form for løsning oplysningerne håndteres i, skal man være opmærksom på bestemmelserne i lovgivningen om behandling af personoplysninger. Et eksempel herpå er brug af databehandlere, som er beskrevet nedenfor.

I bilag 5 findes henvisninger til en liste over relevante love og regler, cloud computing og de juridiske rammer.

Brug af databehandlere
Den dataansvarlige er ansvarlig for, at loven overholdes – også for de oplysninger, som behandles hos databehandleren. Den dataansvarlige afgør derfor til hvilket formål og med hvilke hjælpemidler, der må foretages behandling af personoplysninger, mens databehandleren behandler personoplysninger på vegne af den dataansvarlige.

Eksempelvis kan der være tale om en kunde (dataansvarlig), der overdrager den praktiske behandling af personoplysninger til en ekstern driftsleverandør (databehandler).

Når den praktiske behandling af personoplysninger overdrages til en ekstern part, skal der ifølge persondatalovens §41 og §42 indgås en skriftlig aftale herom (databehandleraftale). Myndigheden skal desuden påse, at der er truffet de nødvendige sikkerhedsforanstaltninger hos databehandleren, herunder at myndighedens behandlinger lever op til sikkerhedskravene i persondataloven og sikkerhedsbekendtgørelsen. Endvidere skal datahandlere (og underdatabehandlere), fremgå af myndighedens eventuelle anmeldelse(r) til Datatilsynet.

Eksempler på spørgsmål vedrørende brug af databehandlere
A. Indeholder eventuelle anmeldelser til Datatilsynet information om de databehandlere, der aktuelt anvendes?
B. Er der indgået databehandleraftaler med relevante leverandører og underleverandører?
C. Følges der op på de aftalte sikkerhedsforanstaltninger i forbindelse med behandlinger af personoplysninger, der er overladt til databehandlere?
D. Er der udarbejdet interne procedurer i forbindelse med overholdelse af anmeldelsespligt til Datatilsynet og indgåelse af databehandleraftale?

Bilag 2: Initiativer fra cyber- og informationssikkerhedsstrategi

Regeringen lancerede i december 2014 National strategi for cyber- og informationssikkerhed. Strategien indeholder 27 initiativer, der skal bidrage til at øge informationssikkerheden og styrke beskyttelsen mod cyberangreb. En række af disse initiativer indeholder anbefalinger eller krav, der kan være relevante for tilsynets rammespørgsmål. Initiativerne fremgår nedenfor.

Beskrivelse af udvalgte initiativer fra den nationale strategi for cyber- og informationssikkerhed
Initiativ nr. 1: Styrket arbejde med informationssikkerhed i staten • ISO27001 skal være implementeret af statslige myndigheder primo 2016 • Alle ministerier skal anvende et statsligt tilsynskoncept, medmindre ministeriet følger eget koncept, som er på samme niveau eller højere.
Initiativ nr. 2: Sikkerhedsmæssig risikovurdering i offentlige it-projekter • Privatlivsrelateret og sikkerhedsmæssig risikovurdering i it-projekter og programmer, skal følge hhv. statens it-projektmodel og den fællesstatslige programmodel.
Initiativ nr. 7: Sikkerhedsmæssige krav i udbud og ved indgåelse af kontrakter på it-området • Liste over sikkerhedsmæssige krav, som myndighederne kan bruge som inspiration ved indgåelse af it-kontrakter.
Initiativ nr. 8: Løbende opfølgning på den sikkerhedsmæssige leverandørstyring • Efterlevelse og indarbejdelse af anbefalingerne i rapporten "Anbefalinger til styrkelse af sikkerheden i statens outsourcede it-drift."
Initiativ nr. 9: Cybertrusler skal indgå i grundlaget for myndighedernes risikoledelse fra 2015 • Statslige myndigheder skal sikre, at cybertrusler indgår i myndighedernes risikovurderinger og risikoledelse fra 2015.
Forud for udarbejdelse af startegien i foråret 2014 besluttede regeringen, at iværksætte en række tiltag på cybersikkerhedsområdet. Tiltagene er kort nævnt i strategien, men en nærmere beskrivelse kan findes på www.digst.dk eller www.fe-ddis.dk. **Regeringens sikkerhedstiltag af maj 2014:** **Tilslutning til netsikkerhedstjeneste og underretning ved større sikkerhedshændelser** • Bekendtgørelse om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste for bl.a. regioner, kommuner eller virksomheder, der er beskæftiget med samfundsvigtige funktioner. • Statslige myndigheders forpligtelse til at underrette Center for Cybersikkerhed ved større it-sikkerhedsmæssige hændelser, f.eks. hacker- og overbelastningsangreb fra 1. september 2014. **Fire konkrete sikkerhedstiltag** • Statslige myndigheder skal i 2014 implementere fire konkrete sikkerhedstiltag i deres it-miljøer. De fire sikkerhedstiltag er formuleret i vejledningen "Cyberforsvar der virker".

Bilag 3: Guide til implementering af ISO27001

Nedenstående skema indeholder et bud på spørgsmål, der kan indgå i en spørgeramme. Spørgemålene er udformet på baggrund af guide til implementering af ISO27001. Guiden gennemgår på et overordnet niveau centrale punkter, der skal gennemløbes, etableres og dokumenteres i arbejdet med at implementere ISO27001. Ydermere findes der hjælp til bl.a. vejledninger, værktøjer og henvisninger i ISO-standarden. Guiden kan hentes på www.digst.dk.

Eksempler på spørgsmål i relation til implementering af ISO27001
1. Ledelsens styring af informationssikkerhed Er den organisatoriske styring af informationssikkerheden herunder placering af roller, ansvar og beføjelser beskrevet? Er beskrivelsen af den organisatoriske styring og tilhørende planer for ledelsens sikkerhedsaktiviteter godkendt i det forløbne år?
2. Politik for informationssikkerhed Er der formuleret en overordnet politik for informationssikkerheden, der er rammesættende for organisationens behandling af informationer og informationssystemer? Er politikken ledelsesgodkendt i det forløbne år?
3. Risikovurdering Foreligger der en overordnet risikovurdering af de kritiske forretningsområder i relation til informationssikkerhed og den understøttende it? Er risikovurderingen ledelsesgodkendt i det forløbne år?
4. Til- og fravalg Er der udarbejdet et beslutningsdokument (SoA-dokument), som dokumenterer til- og fravalg af sikkerhedskontrollerne i ISO27001 anneks A (ISO27002)? Er dokumentet ledelsesgodkendt i det forløbne år?
5. Leverandørstyring Er de opstillede anbefalinger i rapporten "Styrkelse af sikkerheden i statens outsourcede it-drift" indarbejdet i leverandørstyringen?
6. Hændelseshåndtering Er der formuleret procedurer for hændelseshåndtering? Har der i det forløbne år været væsentlige hændelser, der har givet anledning til sikkerhedsmæssige initiativer?
7. Beredskabsplanlægning Er der udarbejdet beredskabsplan(er) til retablering af kritiske forretningsområder herunder kommunikation og it-drift i forhold til leverandører? Er planen testet og ledelsesgodkendt i det forløbne år?
8. Uddannelse og oplysning Er der gennemført aktiviteter i det forløbne år, der eksempelvis fremmer medarbejdernes forståelse for informationssikkerheden?
9. Evaluering og opfølgning Evaluering og opfølgning skal sikre, at ledelsens mål for informationssikkerheden i organisationen bliver opfyldt efter hensigten. Foreligger der dokumentation for ledelsens beslutning om korrigerende handlinger på baggrund af de indsamlede resultater og erfaringer?
10. Planer for sikkerhedsaktiviteter Er der plan(er) for sikkerhedsaktiviteter og evt. årshjul for tilbagevendende aktiviteter, fx opfølgning, evaluering og forbedring af kontroller, risikovurdering, politikker og procedurer? Er planer for sikkerhedsaktiviteter ledelsesgodkendt?

Bilag 4: Opfølgning på revisions- og tilsynsbemærkninger

En del af departementets styrings- og tilsynsansvar omfatter løbende opfølgning på bl.a. rapporter, undersøgelser og beretninger fra revisions- og tilsynsmyndigheder i relation til bemærkninger og anbefalinger vedrørende informationssikkerheden.

Eksempler på overordnede spørgsmål ved opfølgning på revisionsbemærkninger
A. Er der udarbejdet interne procedurer til systematisk opfølgning på bl.a. rapporter, undersøgelser og beretninger fra revisions- og tilsynsmyndigheder?
B. Har der været kritiske bemærkninger, udfordringer eller lignende fra revisions- og tilsynsmyndigheder i det forløbende år?
C. Er der etableret konkrete handlinger på baggrund af bemærkninger og anbefalinger fra myndighederne?

Bilag 5: Henvisninger til information, vejledninger og hjælp

For det videre arbejde med tilrettelæggelse og udførelse af tilsynet henvises til nedenstående hjemmesider med information, vejledninger og hjælpemateriale.

- Udvalgte love med krav til informationssikkerhed
  Digitaliseringsstyrelsen har udarbejdet ikke-udtømmende liste over love, der indeholder regler for informationssikkerhed. Listen kan findes på www.digst.dk

- Datatilsynets vejledning til sikkerhedsbekendtgørelsen
  Offentlige myndigheder skal etablere sikkerhedsforanstaltninger som beskrevet i Justitsministeriets bekendtgørelse nr. 528 af 15. juni 2000. Kravene er nærmere beskrevet i Datatilsynets sikkerhedsvejledning af 2. april 2001 samt andre tekster der kan hentes på www.datatilsynet.dk.

- Cloud computing og de juridiske rammer
  Digitaliseringsstyrelsen har udarbejdet en vejledning, der stiller skarpt på hvilke love og regler, virksomheder skal være opmærksomme på, når der implementeres en cloudløsning. Vejledningen kan hentes på www.digst.dk.

- Hjælpeværktøj og skabeloner til implementering af ISO27001
  Digitaliseringsstyrelsen har udarbejdet vejledninger og værktøjer til hjælp for sikkerhedsstyringen. Vejledningerne kan hentes på www.digst.dk

- Standard for informationssikkerhed ISO27000-serien
  Digitaliseringsstyrelsen har købt brugsretten til ISO27000, ISO27001 og ISO27002 til anvendelse i staten. Nærmere oplysninger om rekvirering af standarden findes på www.digst.dk

- Guide til implementering af ISO27001
  Guiden beskriver en forenklet model med ti punkter, der bør være opfyldt ved implementering af ISO27001. Guiden kan hentes på www.digst.dk

- National strategi for cyber- og informationssikkerhed
  Regeringen lancerede i december 2014 National strategi for cyber- og informationssikkerhed. Strategien indeholder 27 initiativer, der skal bidrage til at øge informationssikkerheden og styrke beskyttelsen mod cyberangreb. Strategien kan bl.a. hentes på www.digst.dk og www.fmn.dk.

- "Anbefalinger til styrkelse af sikkerheden i statens outsourcede it-drift"
  Digitaliseringsstyrelsen har i samarbejde med Center for Cybersikkerhed udarbejdet en rapport med 11 konkrete anbefalinger til, hvordan sikkerheden i den outsourcede it-drift kan forbedres. Rapporten kan hentes på www.digst.dk og www.fe-ddis.dk.

- Den fællesstatslige it-projektmodel og programmodel
  Statslige myndigheder skal følge en række krav, når de gennemfører it-projekter herunder bl.a. privatlivsrelateret og sikkerhedsmæssig risikovurdering i it-projekter. Kravene fremgår af vejledningerne til hhv. statens it-projektmodel og den fællesstatslige programmodel, og kan hentes på www.digst.dk.

- Beredskabsplanlægning for statslige myndigheder
  Beredskabslovens § 24, ændret ved lov nr. 514 af 26. maj 2014. Ifølge loven skal de enkelte ministerier udarbejde en beredskabsplan, der skal revideres mindst én gang hvert fjerde år. Vejledning til ministerier og styrelser udmøntning af planlægningsforpligtelsen kan hentes på www.brs.dk.

- Tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste
  Tilslutning til netsikkerhedstjenesten sker bl.a. for regioner, kommuner eller virksomheder, der er beskæftiget med samfundsvigtige funktioner. Information og bekendtgørelse vedrørende netsikkerhedstjeneste kan hentes på www.fe-ddis.dk.

- Vejledning "Cyberforsvar, der virker"
  Danske offentlige myndigheder og private virksomheder er dagligt udsat for forstyrrende eller skadelige aktiviteter fra forskellige aktører. Derfor har Center for cybersikkerhed og Digitaliseringsstyrelsen udgivet en vejledning i, hvordan risikoen for cyberangreb kan mindskes. Vejledningen kan bl.a. hentes på www.digst.dk og www.fe-ddis.dk.