FINANSMINISTERIET

Vejledning om tilsynet med Statens It

Juni 2025

Vejledning om tilsynet med Statens it
Juni 2025

Denne publikation er udarbejdet af
Finansministeriet
Center for Tilsyn og Jura
Christiansborg Slotsplads 1
1218 København K
Telefon 33 92 33 33

Elektronisk publikation:
ISBN: 978-87-94088-96-1

Publikationen kan hentes på
Finansministeriets hjemmeside
fm.dk

Indhold

1. Ansvar for tilsynet

Vejledningen giver en uddybning til Statens It's (SIT) kunder og samarbejdspartnere i forhold til at forstå det statslige setup, herunder det politiske og driftsmæssige ansvar samt kundernes dataansvar og samspillet mellem disse.

1.1 Ressortoverdragelse

De fleste af SIT's kunder har fået deres basale it-drift ressortoverført fra den pågældendes institutions ressortminister til finansministeren ved kongelig resolution. Finansministeren har overtaget ansvaret for opgaverne, fordi SIT er en styrelse under Finansministeriet. Det er Statsministeriet, som har vurderet, at den korrekte måde at overføre it-drift til SIT er ved kongelig resolution (ressortoverdragelse). Det fremgår af et notat af 6. februar 2017 udarbejdet af Statsministeriet.

Det tydeliggøres bl.a. i notatet, at alene én minister kan være ansvarlig for den opgavevaretagelse, som overdrages. Ressortoverdragelsen indebærer, at det politiske ansvar for den basale it-drift er overført fra ressortministeren til finansministeren.

Det fremgår endvidere af notatet, at pligten til at føre tilsyn med de opgaver, der er overført, også overføres.

For de institutioner, hvor deres basale it-drift er blevet overført til finansministeren, gælder således, at ansvaret for at føre tilsyn med opgaverne relateret til basal it-drift, er overført til Finansministeriet.

> "Det skal være muligt entydigt at fastlægge, hvilken minister, der har ministeransvaret (og tilsynspligten) med et givent område, og der kan i den forbindelse ikke inden for grundlovens rammer være "konkurrerende kompetence" mellem flere ministre."
>
> "Den minister, som overgiver kompetence har ikke nogen kompetence til at udstede nærmere dekreter vedrørende opgavernes udførelse…"
>
> …Ved en ressortoverdragelse indebærer dette, "at også ansvaret for ressortområdet, herunder også tilsynet for de opgaver, der er overdraget, vil være overført".
>
> "Såfremt det relevante ressortområde – i dette tilfælde it-sikkerhed – er overført, vil det ikke længere kunne kræves, at den afgivende myndighed fører tilsyn med opgavens udførelse (men eventuelt med tilgrænsende opgaver, som ressortansvaret ikke er overført for.)"
>
> *Statsministeriets notat af 6. februar 2017 om overdragelse af it-drift, punkt 7.*

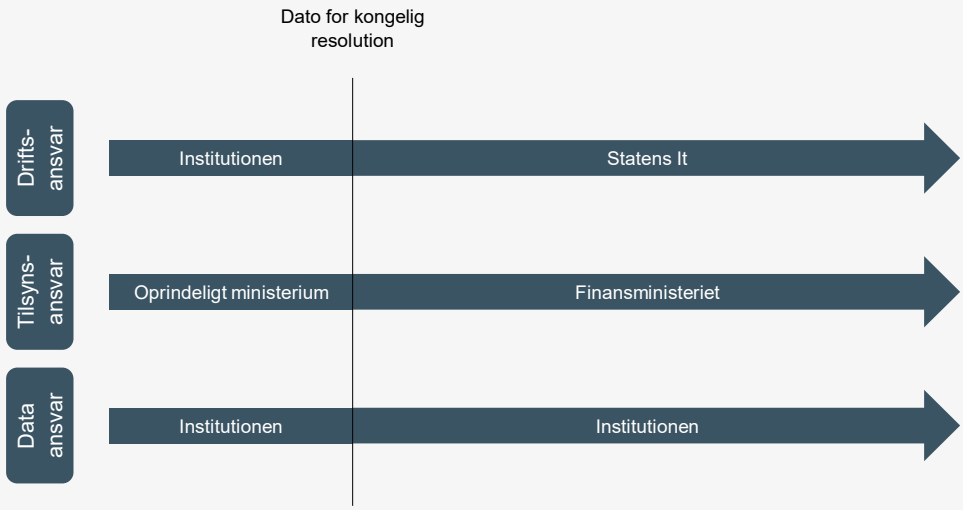
1.2 Dataansvar og FM's departementale tilsyn

Ressortoverdragelsen ved kongelig resolution ændrer ikke på ansvaret i forhold til GDPR[1]. Den kongelige resolution flytter det politiske ansvar for basal it-drift, mens det ansvar institutionerne har som dataansvarlige i henhold til GDPR fortsat er den enkelte kundes. Dette ansvar omfatter blandt andet deres forpligtelse til at føre tilsyn med SIT som deres databehandler, hvilket også er beskrevet i de indgåede databehandleraftaler.

Det er målet for tilsynet, at den enkelte kundes forpligtelse til at føre tilsyn med SIT som deres databehandler, kan varetages gennem den mundtlige og skriftlige rapportering om tilsynet, som er udarbejdet af Finansministeriets departement (FM-DEP) vedrørende tilsynet med SIT.

FM-DEP har en departemental forpligtelse til at føre tilsyn med de opgaver, som SIT varetager som en styrelse under Finansministeriet, herunder med opgavevaretagelse af den ressortoverdragne basale it-drift.

Figur 1.1
Fordeling af ansvar



[1] General Data Protection Regulation – eller databeskyttelsesforordningen.

Der er et stor sammenfald mellem opgaverne relateret til basal it-drift og de opgaver, som SIT varetager som databehandler for institutionerne, idet databehandlingen, som foretages for institutioner, i meget vid udstrækning *er* basal it-drift.

De tilsyn, der skal føres for at overholde forpligtelserne for henholdsvis de dataansvarlige og FM-DEP, er således i meget vidt omfang to sider af samme sag.

1.3 Tilsynsmodel

For at effektivisere opgavevaretagelsen og lette "byrden" for såvel institutionerne som SIT er der implementeret en tilsynsmodel, hvor FM-DEP fører tilsyn med SIT's opgavevaretagelse og dermed også funktionen som databehandler på institutionernes vegne.

Formålet hermed er at varetage så stor en del af institutionernes tilsynsforpligtelse som muligt, således at institutionerne kan basere sig på FM-DEP's tilsyn og derigennem varetage deres tilsynsforpligtelse. En forudsætning for at det kan opfyldes er, at FM-DEP's tilsyn i tilstrækkelig grad omfatter de opgaver og databehandlinger, som institutionerne får udført af SIT. FM-DEP søger at dække behovet ved at føre et grundigt og omfangsrigt tilsyn, som beskrives nærmere i kapitel 2.

Tilsynsmodellen, hvor FM-DEP fører tilsynet med SIT i deres rolle som databehandler på vegne af kunderne i SIT, er i tråd med Datatilsynets koncept 5 i deres "*Vejledning om tilsyn med databehandlere"* fra oktober 2021.

Tilsynet, som udføres af FM-DEP, foretages uafhængig af ledelsen i SIT. Tilsynsenheden er under selvstændig ledelse af en tilsynschef, som rapporterer til Finansministeriets øverste ledelse (Departementschef og Driftsledelse), og som ikke er underlagt instruktion fra ledelserne i Finansministeriets institutioner. Tilsynsenheden har en særskilt funktionsbeskrivelse, som er godkendt af departementets øverste ledelse. Det fremgår af funktionsbeskrivelsen, at tilsynsenheden har ubegrænset adgang til samtlige informationer, registreringer, systemer mv. i Finansministeriets koncern, som tilsynschefen vurderer er nødvendige for opgaveudførelsen.

Selvom FM-DEP søger at dække alle institutionernes behov for tilsyn med SIT's behandling af de personoplysninger, som institutionerne er ansvarlige for, vil det naturligvis kunne forekomme, at enkelte institutioner har yderligere behov. FM's tilsynsmodel er ikke til hinder herfor, og de dataansvarlige har, som der fremgår af databehandleraftalerne, altid krav på at få stillet alle nødvendige oplysninger til rådighed, for at de kan overholde deres forpligtelser som dataansvarlige, herunder også deres ansvar for at sikre, at der føres tilstrækkeligt tilsyn med SIT som

databehandler. Med konstruktionen af tilsynsmodellen er det målet, at de dataansvarliges behov i alt overvejende grad dækkes af FM DEP's tilsynsundersøgelser og rapporteringer. Skulle dette ikke være tilfældet – og har den dataansvarlige behov for flere oplysninger for at kunne leve op til sit dataansvar – skal den dataansvarlige først sørge for at have orienteret sig i de informationer, SIT stiller til rådighed, fx Kundeaftalen, Servicekataloget og Kundeaftalens bilag 2 "*Varedeklarationen for informationssikkerhed*", samt de informationer, som FM-DEP stiller til rådighed vedrørende det førte tilsyn. Dette kan fx være de løbende afrapporteringer i Arbejdsgruppen for informationssikkerhed, den samlede årlige tilsynsberetning og de enkelte underliggende tilsynsrapporter, jf. nærmere i kapitel 3 om FM-DEP's rapportering.

Hvis den dataansvarlige ikke finder de tilgængelige kilder dækkende, kan den dataansvarlige henvende sig til kundepartneren i SIT, som må vurdere, om de ønskede oplysninger kan udleveres, idet sikkerhedsmæssige hensyn kan gøre, at ikke alt vil kunne oplyses.

Hvis den dataansvarlige oplever, at SIT ikke reagerer tilstrækkeligt på konkrete risici eller sikkerhedsmæssige problemstillinger fremført af den dataansvarlige, kan den dataansvarlige altid henvende sig til FM-DEP via kontaktoplysninger på departementets hjemmeside eller via Tilsyn@fm.dk.

Input og ønsker til kommende tilsynsundersøgelser kan altid rettes direkte til FM-DEP, som vil tage input og ønsker med i planlægningen af tilsyn.

1.4 Revision og revisionsansvar

Der kan være situationer, hvor det er nødvendigt for SIT's kunder at give erklæringer eller lignende sikkerhed til eksterne parter, fx EU-organer, EU-revisioner, kvalitetssikringsmyndigheder eller lignende, omkring varetagelsen af informationssikkerheden.

FM-DEP udsteder ikke revisorerklæringer.

Som følge af Rigsrevisorloven er det Rigsrevisionen, der udfører revision af SIT. Rigsrevisionen afgiver erklæring på det samlede statsregnskab, men afgiver ikke specifik erklæring om revisionen af SIT.

FM-DEP's årlige tilsynsberetning vil kunne dække behovet hos flere eksterne interessenter og således i mange tilfælde kunne træde i stedet for en erklæring.

Der kan dog være institutioner, der er underlagt særlig lovgivning eller særlige revisionsmæssige forpligtelser, hvor tilsynsberetningen ikke er tilstrækkelig til at dække forpligtelsen for den enkelte institution. I disse tilfælde kan institutionen henvende sig til tilsynet, hvorefter det afklares, hvorledes de særlige revisionskrav kan imødekommes. Der kan således gives adgang til, at tredjepart kan udføre revision eller lignende i SIT. Sådanne revisioner skal dog altid praktisk koordineres med FM-DEP, og der aftales relevant deltagelse herfra. Et eksempel på særlige lovgivningsmæssige krav er på områder, som modtager EU-tilskud, hvor der stilles særlige krav omkring EU-tilskudsforvaltning og revision heraf.

1.5 Tilsyn på vegne af kunder, som ikke er ressortoverdraget

SIT har kunder, hvor kunden som institution eller driften af den specifikke ydelse ikke er ressortoverdraget ved kongelig resolution, hvilket skyldes helt særlige forhold, eller at kundeforholdet drejer sig om et enkelt produkt, som fx TTJ, Filkassen eller brugen af Statens Whistleblowersystem.

Disse kunder skal ligeledes basere deres tilsyn med SIT som leverandør/databehandler på FM-DEP's udførte tilsyn.

Det er ikke muligt at rekvirere revisorerklæringer vedrørende SIT's virke. De eneste, der kan revidere SIT, er Rigsrevisionen, og der henvises til Rigsrevisionens beretninger mv., jf. også afsnit 1.4 ovenfor.

De udførte revisioner og tilsyn tager ikke hensyn til, om den enkelte kunde er ressortoverdraget eller ikke, hvorfor generelle konklusioner dækker begge kundegrupper. FM-DEP anbefaler, at ikke-ressortoverdragede kunder gør brug af tilsynets arbejde fx i form af den årlige tilsynsberetning eller tilsynsrapporter vedr. konkrete ydelser, som SIT leverer til både ressortoverførte og ikke-ressortoverførte kunder.

Disse konkrete tilsynsrapporter kan altid rekvireres hos FM-DEP. Det bemærkes dog, at der ikke føres målrettede tilsyn med disse konkrete ydelser eller specifikke produkter hvert år, men at de indgår i en turnusordning og udvælges til gennemgang efter FM-DEP's vurdering af risiko og væsentlighed. De fleste af sådanne konkrete ydelser/specifikke produkter vil imidlertid være delvist dækket af de løbende tilsynsundersøgelser, som omhandler SIT's generelle processer, hvorfor disse undersøgelser i vid udstrækning også vil kunne bruges af institutioner, som ikke har ressortoverdraget hele den basale it-drift.

2. Indholdet af tilsynet

Det essentielle i tilsynsmodellen er, at tilsynsopgaven med SIT udføres af FM-DEP som følge af ressortoverdragelsen, og at resultaterne heraf deles med de institutioner, som er kunder hos SIT, således at kunderne får en tilstrækkelig indsigt i driften og kan varetage deres rolle som myndighed og dataansvarlig.

Tilsynet omfatter den basale it-drift, som udføres i SIT på vegne af andre ministerier og for FM-DEP selv. Den enkelte ressortoverdragelse kan indeholde undtagelser herfor.

Formålet med tilsynet er at vurdere:

- om styringen af informationssikkerheden er tilrettelagt og håndteret hensigtsmæssigt,
- om de generelle it-kontroller sikrer et betryggende sikkerhedsniveau,
- om der er foretaget en periodisk risikovurdering af informationssikkerheden for at identificere risiko for tab af fortrolighed, integritet og tilgængelighed,
- om der er fastlagt politikker og retningslinjer for informationssikkerheden,
- om SIT efterlever de aftalte krav til sikkerhedsforanstaltninger, som følger af kundeaftalen og databehandleraftalerne,
- om der er taget hensigtsmæssig stilling til og håndtering af bemærkninger og anbefalinger fra revisions- og tilsynsmyndigheder,
- overholdelse af relevant lovgivning i forhold til basal it-drift, herunder GDPR.

Planlægningen af årets tilsyn starter typisk op i november-december året før og munder ud i en tilsynsplan for året, som deles med SIT og Arbejdsgruppen for informationssikkerhed. I Arbejdsgruppen fortæller tilsynet løbende om status på årets planlagte undersøgelser, herunder også hvis der sker ændringer i planen.

I tilsynsplanen er indholdet og omfanget af tilsynet fastlagt på baggrund af en vurdering af væsentlighed og risiko på tværs af den samlede portefølje af kunder.

Udførelsen af tilsynet sker hele året rundt. De specifikke tilsynsundersøgelser for tilsynsåret starter op fra ca. marts og indtil ca. ultimo marts året efter.

Afrapporteringen af tilsynet sker løbende til SIT's kunder på møder i Arbejdsgruppen for informationssikkerhed samt afslutningsvist ved tilsynsberetningen for året ca. primo maj i det efterfølgende år, jf. mere herom i kapitel 3.

2.1 Typer af drift hos SIT

SIT's drift kan med fordel beskrives som to grupper med forskellige karakteristika, som skitseret i nedenstående figur "Typer af drift hos SIT".

Figur 2.1
Typer af drift hos SIT

SIT standard drift

SIT standard drift omfatter alle de elementer af basal it-drift, som institutionerne på den ene eller anden måde er fælles om, og som SIT drifter ensartet på tværs af kunder. SIT standard drift omfatter fællessystemer som fx SIA, VIA, MIA, Exchange (e-mail), fællesdrev og tilsvarende, men også firewall, ServiceNow og den type systemer. Derudover omfatter standarddriften også standardprocesser som fx adgangsstyring, ændringsstyring, sikkerhedskopiering mv., som med få undtagelser håndteres ensartet på tværs af SIT.

Kundespecifik drift

Mange af SIT's kunder har i forbindelse med transitionsprocessen fået deres eget domæne og/eller netværk. I dette domæne og netværk placeres alle institutionens servere, som ikke er overgået til SIT standard drift. Dette benævnes kundespecifik drift[2].

---

2 Enkelte kunder har flere kundespecifikke domæner og/eller netværk

Der kan være flere økonomiske såvel som sikkerhedsmæssige fordele ved, at drift flyttes fra den kundespecifikke drift til SIT standard drift, hvorfor mange kunder løbende har projekter af denne art.

Se afsnit 2.3 Tilsyn med SIT kundespecifik drift for yderligere uddybning af tilsynet med den kundespecifikke drift.

2.2 Tilsyn med SIT standard drift

Med udgangspunkt i ISO 27001 fører FM-DEP løbende tilsyn med SIT's standard driftsmiljø således, at alle relevante områder gennemgås inden for en 3-4-årig periode.

SIT har i dokumentet "*Kundeaftalens bilag 2, Varedeklaration for Informationssikkerhed*" beskrevet de it-sikkerhedsforanstaltninger, der udføres i forbindelse med SIT's standard driftsydelser. Dokumentet går i daglig tale under navnet 'varedeklarationen' eller 'SIT's varedeklaration'.

SIT har på systemniveau struktureret leverancerne til kunderne i forskellige driftsmodeller, som definerer ansvarsdelingen mellem SIT og kunden. Driftsmodellerne har således betydning for, i hvilket omfang FM-DEP's tilsyn med SIT's standard driftsmiljø dækker, idet tilsynet dækker de driftsområder, som SIT har ansvaret for.

Oversigt over tilsynets omfang

Oversigten nedenfor viser et overblik over de områder, som tilsynet omfatter, og de områder, hvor kunderne skal være opmærksomme på, at de fortsat har en opgave at udføre.

Oversigten er ikke fuldstændig, men indeholder eksempler på sådanne opgaver under de forskellige driftsmodeller.

Helt overordnet er det vigtigt, at kunderne fortsat udfører risikovurderingen af deres drift. Det er alene kunderne, som har indsigten i, hvorledes it-driften understøtter de administrative og politiske opgaver, og alene kunderne der i sidste ende kan lave risikovurderingerne.

Tabel 2.1
Oversigt over tilsynets omfang

<table>
<tr><th></th><th>Driftsmodel 5</th><th>Driftsmodel 3</th><th>Driftsmodel 2A</th><th>Driftsmodel 2</th><th>Driftsmodel 1A</th><th>Driftsmodel 1</th></tr>
<tr><td></td><td>Outsourcet drift til tredjepart</td><td>Infrastrukturservice</td><td>Platformsdrift</td><td>Platformservice</td><td>Applikationsdrift</td><td>Applikationsservice</td></tr>
<tr><td>Ledelsens Informations-sikkerheds-styring</td><td colspan="6">Vil være omfattet af tilsynsaktiviteter i en turnusordning</td></tr>
<tr><td>Applikationer

ESDH, Fagsystemer, Portaler, Sharepoint, Web, etc.</td><td>Ikke omfattet af FM-DEP's tilsyn

Den enkelte institution fører fx tilsyn med oprettede brugere i (eller til) selve applikationen, inklusive leverandørens med-arbejdere, konsulenter m.fl.

Den enkelte institution udar-bejder egne beredskabsplaner om fx manuelle procedurer i en beredskabssituation.</td><td colspan="4">Ikke omfattet af FM-DEP's tilsyn

Den enkelte institutions eget ansvar, fx:
- Den enkelte institution fører fx tilsyn med oprettede brugere i (eller til) selve applikationen, inklusive SIT medarbejdere, konsulenter m.fl.
- Sårbarhedsstyring: Den enkelte institution skal sikre, at applikationen kan afvikles på supporterbare versioner af software.
- Den enkelte institution udarbejder egne beredskabsplaner om fx manuelle procedurer i en beredskabs-situation.

Omfattet af FM-DEP's tilsyn
- Sikkerhedskopiering: I det omfang der er etableret aftale med SIT om backup, vil denne være omfattet af FM-DEP's tilsyn.
- SIT's processer for reetablering er omfattet af tilsynet.</td><td>Omfattet af FM-DEP's tilsyn
SIT's standardapplikationer der efter tilvalg stilles til rådighed for institutionen af SIT.

Kunne være e-mail, SIA, VIA, MIA, fællesdrev m.fl.

Tilsynet omfatter SIT's håndtering af de nævnte områder i ISO 27001 i en turnusordning.</td></tr>
<tr><td>Middleware

Oracle, SQL, etc.</td><td rowspan="3">Omfattet af FM-DEP's tilsyn
Det vil være SIT's ansvar at følge op på sikkerheden hos tredjepartsleverandøren med udgangspunkt i kontrakten og som et led i leverandør-styringen.

FM-DEP fører tilsyn med SIT's leverandørstyring.</td><td>Ikke omfattet af FM-DEP's tilsyn
Det vil være institutio-nens eget ansvar, at databaser lever op til SIT's "Krav til database-sikkerhed".</td><td>Ikke omfattet af FM-DEP's tilsyn
Det vil være institutionens eget ansvar, at databaser lever op til SIT's "Krav til databasesikkerhed".

Omfattet af FM-DEP's tilsyn
Standard komponenter som backup, patchning af sup-porterede databaseversio-ner, ændringsstyring mv.</td><td colspan="2">Omfattet af FM-DEP's tilsyn

Tilsynet baseres på ISO 27001 i en turnusordning. Adgangsstyring, ændringsstyring, fysisk sikkerhed, sikkerhedskopiering og beredskab gennemgås hvert år.

Kræver at databaserne lever op til SIT's "Krav til databasesikkerhed". Et supporteret databasesystem med databaser, der kan holdes løbende opdateret</td><td></td></tr>
<tr><td>Operativsystem

Windows, Linux, etc.

Server/Storage

Virtuel server, fysisk server, datalagring, etc.

Netværk

Core, WAN, LAN, Firewall, etc.

Fysisk lokation

M^2, Køl, Strøm, Racks, Fysisk sikkerhed etc.</td><td colspan="4">Omfattet af FM-DEP's tilsyn

Fx Adgangsstyring, ændringsstyring, fysisk sikkerhed, sikkerhedskopiering og beredskab samt GDPR-overholdelse, som gennemgås hvert år.</td><td></td></tr>
<tr><td>Tværgående områder</td><td colspan="6">Omfattet af FM-DEP's tilsyn</td></tr>
</table>

Opdeling af driftsmodeller

Når man som kunde i SIT skal afklare sin forpligtelse i forhold til driften af sit it-system, skal man først og fremmest afklare, hvilken driftsmodel, der er valgt for det pågældende system. Herefter vil man i ovenstående oversigt kunne aflæse, hvilke dele af it-infrastrukturen, som dækkes af FM-DEP's tilsyn, og hvilke opgaver, som påhviler institutionen selv (markeret i figuren med mørkere grå).

Lag i it-infrastrukturen

De forskellige lag i it-infrastrukturen benævnes også teknologistakken. I oversigten er teknologistakken opdelt i henhold til den opdeling, der anvendes af SIT i deres beskrivelse af driftsmodellerne.

Enkelte institutioner har desuden valgt at anvende OSI modellens 7 lag i deres risikovurderinger. Disse modeller er ikke væsentligt forskellige, så valget af den ene model frem for den anden vurderes ikke at have praktisk betydning.

Indholdet af tilsynet

Det udførte tilsyn består af en række tilsynsaktiviteter, som udføres hen over hele tilsynsåret, herunder fx:

- Tilsynets detaljerede gennemgange omkring informationssikkerhed som rapporteres i tilsynsrapporter (emner udvælges årligt i en tilsynsplan)
- Gennemgang af SIT's overholdelse af GDPR i deres rolle som databehandler
- Løbende møder med SIT's ledelse og medarbejdere
- Deltagelse i forskellige kundefora i SIT
- Deltagelse i analysen af nye kunder hos SIT, hvor indkomne risici vurderes
- Status på SIT's ISO 27001 og 27701 certificeringer
- Deltagelse i Rigsrevisionens revisioner af SIT
- Opfølgning på Rigsrevisionens bemærkninger
- Opfølgning på tilsynets bemærkninger fra tidligere år
- Henvendelser fra SIT's kunder

Hovedbestanddelen af tilsynet er de detaljerede gennemgange, som løbende afrapporteres i tilsynsrapporter.

Tilsynets detaljerede gennemgange planlægges og udføres ud fra en turnus, hvor alle væsentlige områder i ISO-standarden gennemgås inden for en 3-4-årig periode. Områderne adgangsstyring, ændringsstyring, fysisk sikkerhed, it-beredskab og sikkerhedskopiering samt overholdelse af GDPR i SIT's rolle som databehandler er dog udvalgt hvert år, idet disse udgør et væsentligt fundament for god sikkerhed.

Iblandt tilsynets detaljerede gennemgange indgår også gennemgang af systemer og driftsområder, som går på tværs af flere ISO-områder, fx gennemgang af Statens Whistleblowersystem, Filkassen, databasesikkerhed, netværksadministration mv. Kendetegnende for disse er, at alle aspekter af driften af disse systemer kan indgå, fx risikovurdering, adgangsstyring, sikkerhedskopiering, konfigurationsstyring, logning mv. Frekvensen for sådanne systemgennemgange varierer afhængig af tilsynets vurdering af risici og væsentlighed, men de samme systemer udvælges dog ikke til gennemgang hvert år.

Tilsynet laver en samlet vurdering af risikoen, når tilsynsplanen udarbejdes og de forskellige tilsynsgennemgange for året udvælges. Der sker en vurdering af risiko både overordnet i årsplanen for tilsynet, men også i de detaljerede planer inden et specifikt tilsyn igangsættes. Input til vurderingen af risikoen kan fx være ny lovgivning på området, nye eller ændrede processer, nye teams, nye chefer, nye risici opstået i omverdenen, samt risici som er kommet tilsynet til kendskab gennem forskellige tilsynsaktiviteter eller henvendelser fra SIT's kunder.

Under udførelsen af de detaljerede tilsynsgennemgange tager tilsynet udgangspunkt i ISO 27001/2 og vurderer den implementerede informationssikkerhed i SIT mod varedeklarationen, mod ISO 27002, mod SIT's standard kundeaftale og standarddatabehandleraftale, mod SIT's servicekatalog, mod anerkendt eller bedste praksis og mod gældende lovgivning. Tilsynet efterprøver fx, om SIT overholder deres egne retningslinjer og forretningsgange, samt om forretningsgangene er hensigtsmæssige, eller om der kunne være risici, som SIT ikke imødegår mv.

Tilsynet udføres ikke specifikt for de enkelte kunders systemer og tilhørende instrukser, jf. GDPR-systemlisterne.

Hovedfokus for tilsynet er standarddriften og standarddatabehandleraftalerne, idet langt de fleste behandlingsaktiviteter, som SIT udfører for kunderne, følger ensartede procedurer, som er tværgående i forhold til systemer og kunder. Tilsynet omfatter dog SIT's procedurer for, hvordan SIT sikrer, at de kan efterleve eventuelle kundeinstrukser, som afviger fra standarden, og tilsynet kan på stikprøvebasis omfatte konkrete særlige krav fra kunderne.

Tilsynet påser endvidere, at SIT foretager opfølgning på Rigsrevisionens, Datatilsynets og tilsynets egne tidligere fremsatte bemærkninger. Tilsynet rapporterer om opfølgningen i tilsynsberetningen.

Kundens ansvar og handlinger

Generelt
Som oversigten over tilsynets omfang viser, er opgave-/ansvarssnittet mellem SIT og kunderne forskelligt inden for de forskellige driftsmodeller. Der er dog en række opgaver og handlinger, som altid vil være relevante for kunderne at udføre, uanset driftsmodellen.

- *Deltagelse i relevante kundefora*: Det er den enkelte institutions opgave at deltage i relevante kundefora, som SIT stiller til rådighed.

  I de tilfælde, hvor en institution lader sig repræsentere af fx en repræsentant fra ministerområdets departement, er det repræsentantens ansvar at videreformidle relevante budskaber. Det enkelte ministerområde, som er helt eller delvist kunde hos SIT, bør have en praksis for formidling af relevante budskaber fra disse kundefora.

  Det er den enkelte institutions ansvar at handle på de informationer, der gives, såfremt dette vurderes relevant for institutionen og herunder vurdere, om deres egen ledelse bør orienteres.

- *Årligt læse og tage stilling til tilsynsberetningen:* Den enkelte institution bør årligt læse tilsynsberetningen og på baggrund heraf vurdere, om der er behov for at udbede sig de underliggende tilsynsrapporter fra tilsynet.

- *Opfølgning på aftalte særlige krav:* Såfremt institutionen har stillet særlige krav, skal kunden selv sikre sig levering af det aftalte, fx i aftalt rapportering.

- *Vurdere om institutionen har instrueret SIT i at udføre behandlingsaktiviteter, der afviger fra SIT's standard:* SIT udfører de fleste databehandlinger ud fra ensartede procedurer, som er tværgående i forhold til systemer og kunder. SIT har udarbejdet vejledningstekster til brug for kunderne ved udfyldelse af deres GDPR-systemlister.

- *Foretage risikovurdering af egne systemer og institutionens brug heraf.*

  Risikovurderingen bør bl.a. tage udgangspunkt i følgende forhold:

  - Institutionens konkrete anvendelse af det pågældende system.
  - Opfølgning på eventuelle særlige krav.
  - FM-DEP's løbende afrapportering af tilsynet med fokus på, om kritiske forhold har relevans for institutionens anvendelse af systemet.
  - FM-DEP's årlige tilsynsrapport omkring SIT's rolle som databehandler.
  - FM-DEP's årlige tilsynsberetning med fokus på, om kritiske forhold har relevans for systemet.

Endeligt vil det for kunder, som anvender Driftsmodel 5, være nødvendigt at:

- *indhente referat af SIT's årlige sikkerhedsaudit* hos eksterne leverandører og vurdere om eventuelle forbehold, bemærkninger eller kritikpunkter heri kan have betydning for institutionens system.

Tilsynet anbefaler, at SIT's kunder systematisk dokumenterer at have gennemført ovenstående punkter.

2.3 Tilsyn med SIT kundespecifik drift

Tilsynet med SIT kundespecifik drift opdeles i fire forskellige elementer.

1) Standardelementer af den kundespecifikke drift

SIT anvender i høj grad ens processer og standarder på tværs af SIT standard drift og SIT kundespecifik drift. Eksempler på dette kunne være:

- Backup
- Firewalladministration
- Brugeradministration
- Fysisk sikkerhed

Disse områder er til fulde dækket af tilsynet med SIT standard drift.

2) Generel SIT kundespecifik drift

Systemer og områder som udelukkende eller næsten udelukkende anvendes i SIT kundespecifik drift. Eksempler på dette kunne være:

- AD trust
- AD synkronisering mellem domæner

Tilsynet med den generelle SIT kundespecifikke drift sker ved udvælgelse af specifikke systemer og områder for gennemgang. Vurdering og udvælgelse sker hvert år i forbindelse med planlægning af årets tilsynsplan.

3) SIT kundespecifik drift på enkelt kundeniveau

Specifikke aftaler som er unikke for den enkelte eller få kunder. Eksempler på dette kunne være:

- Kundespecifik filserver
- Hyppigere backupfrekvens end standard
- Backup på tape
- Delegation af rettigheder
- Aftalt redundans

Tilsynet med SIT kundespecifik drift på enkeltkundeniveau er en meget omkostningsineffektiv måde at føre tilsyn på og sker kun efter individuel vurdering. SIT kundespecifik drift på enkeltkundeniveau omfatter også særlige sikkerhedsforanstaltninger, hvor kunden selv påser, at disse er effektive gennem kontrol af den aftalte rapportering. I nogle tilsynsgennemgange vil tilsynet dog på stikprøvebasis også omfatte særlige kundespecifikke sikkerhedsforanstaltninger.

4) Kundespecifik SIT standard drift

Kundespecifik SIT standard drift er specifikke aftaler, som afsondrer en kunde fuldstændig fra de øvrige kunder. Udgangspunktet vil dog være, at SIT standardprocesser i videst muligt omfang anvendes over for den afsondrede kunde.

Kundespecifik SIT standard drift vurderes individuelt, og det vurderes specielt i hvilken udstrækning resultaterne af tilsynets gennemgange af SIT standard drift kan genbruges hos den enkelte kunde.

2.4 Tilsyn med SIT's efterlevelse af GDPR

I de fleste af de områder, som tilsynets detaljerede gennemgange omfatter, indgår der behandling af personoplysninger. Tilsynet fokuserer – som beskrevet ovenfor – i disse gennemgange på, om SIT har implementeret passende og effektive foranstaltninger i forhold til behandlingen af data, herunder personoplysninger. Ved udførelsen af disse gennemgange søger tilsynet dermed at dække SIT's overholdelse af GDPR, artikel 32, om behandlingssikkerhed.

I forlængelse af ovennævnte gennemgange udfører FM-DEP desuden en tilsynsgennemgang af SIT's overholdelse af øvrige relevante GDPR-regler end reglerne

om behandlingssikkerhed. I afrapporteringen af denne gennemgang inkluderes behandlingssikkerhed dog ved at inddrage konklusionerne fra tilsynets øvrige gennemgange, hvortil der også henvises.

I nedenstående figur er oplistet de artikler, som gennemgangen primært omhandler.

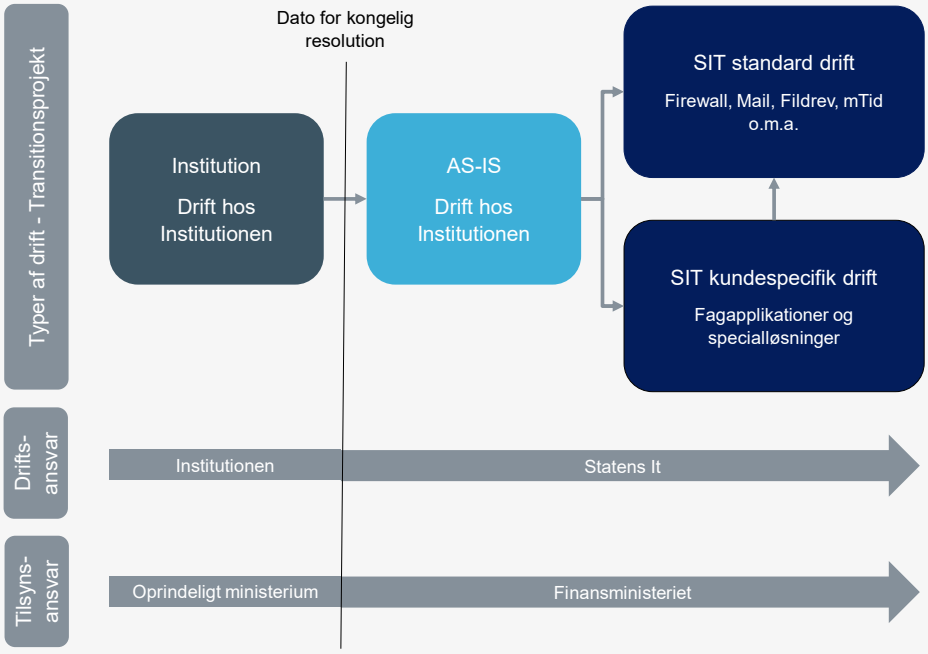
Tabel 2.2
Overblik over artikler og kontrolmål, som er databehandlerens ansvar

Artikel i GDPR	Kontrolmål
28 og 29	Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgåede databehandleraftale.
30.2	Der efterleves procedurer og kontroller, som sikrer, at databehandleren fører en fortegnelse over kategorier af behandlinger, der foretages på vegne af de dataansvarlige.
32	Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske og organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.
33.2	Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.
35 og 28f	Der efterleves procedurer og kontroller, som sikrer, at databehandleren bistår den dataansvarliges forpligtelse til at gennemføre en konsekvensanalyse vedr. databeskyttelse, hvis en type behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder.
36 og 28f	Der efterleves procedurer og kontroller, som sikrer, at databehandleren bistår den dataansvarliges forpligtelse til at høre tilsynsmyndigheden inden behandling, såfremt en konsekvensanalyse vedr. databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.

2.5 Tilsyn under transition

For nye institutioner i SIT gælder særlige ansvarsforhold i transitionsfasen, som skitseret i følgende figur "Typer af drift hos SIT – transition".

Figur 2.2
Typer af drift hos SIT - transition



Institution – Drift hos institutionen

I perioden indtil den kongelige resolution træder i kraft, og hvor selve ressortoverdragelsen sker, vil it-driften hos den enkelte institution være uændret.

AS-IS – Drift hos institutionen

I perioden efter selve ressortoverdragelsen fortsætter it-driften uændret, mens ansvaret, og i nogle tilfælde også udvalgte medarbejdere, er overført til SIT.

Dele af AS-IS driften kan fortsætte i længere tid efter selve ressortoverdragelsen, hvilket fx kan skyldes kontraktlige eller licensmæssige forhold.

SIT standard drift

I perioden efter selve ressortoverdragelsen vil udvalgte dele af institutionens drift blive flyttet fra det oprindelige miljø i institutionen til SIT standard drift. SIT standard drift og tilsynet hermed er beskrevet i tidligere afsnit.

SIT kundespecifik drift

I perioden efter selve ressortoverdragelsen vil udvalgte dele af institutionens drift blive flyttet fra det oprindelige miljø i institutionen til SIT kundespecifik drift. SIT kundespecifik drift og tilsynet hermed er beskrevet i tidligere afsnit.

Den kundespecifikke drift består som tidligere beskrevet, så længe ressortoverdragelsen er gældende. Der kan dog være flere økonomiske såvel som sikkerhedsmæssige fordele, ved at drift flyttes fra SIT kundespecifik drift til SIT standard drift, hvorfor mange nye kunder i perioden efter ressortoverdragelsen løbende har projekter af denne art.

Driftsansvar

Driftsansvaret overgår formelt på datoen for den kongelige resolution fra den afgivende minister til finansministeren, i det omfang som er beskrevet i resolutionen.

Tilsynsansvar

Tilsynsansvaret følger driftsansvaret og overgår formelt på datoen for den kongelige resolution fra den afgivende minister til finansministeren – se mere nuanceret beskrivelse i kapitel 1.

Efterhånden som den nye kundes drift flyttes til henholdsvis SIT standard drift og SIT kundespecifik drift, er kundens systemer m.v. automatisk omfattet af de tilsynsaktiviteter, der foregår på disse områder.

FM-DEP deltager i hovedparten af alle transitionsprojekternes analysefaser. I samarbejde med SIT foretages en it-sikkerhedsmæssig vurdering af de områder, som skal ressortoverdrages allerede inden overdragelsen. Dette sker for at være tidligt opmærksom på den risiko, der overdrages til FM.

2.6 Tilsyn med samfundsansvar (CSR, ESG eller lign.)

Statslige institutioner er ikke forpligtet til at rapportere om socialt ansvar, miljøansvarlighed, etiske problemstillinger mv. Dette udelukker dog ikke, at tilsynet altid kan tage relevante emner op i tilsynet, som relaterer hertil.

Hvad er CSR og ESG?

- Corporate Social Responsibility (CSR) er betegnelsen for virksomheders arbejde med at integrere sociale og miljømæssige hensyn i deres forretningsaktiviteter og i deres interaktion med interessenterne. 'Virksomhedens samfundsansvar' er en dansk betegnelse for begrebet[3]. Virksomheder viser samfundsansvar og skaber værdi for både virksomhed og samfund ved i dialog med deres interessenter at håndtere sociale, miljømæssige og etiske udfordringer i overensstemmelse med internationalt anerkendte principper for samfundsansvar[4].

- Det er frivilligt for danske virksomheder, om de ønsker at arbejde med samfundsansvar. Lovkravene i årsregnskabsloven betyder imidlertid, at de største danske virksomheder har pligt til at afgive en redegørelse for samfundsansvar[5]. For en række virksomheder er der introduceret specifikke krav til rapportering af ESG, som dækker over Environmental, Social and corporate Governance. Ved ESG-rapportering skal virksomheder rapportere om en række miljøpåvirkninger, bæredygtighed, social påvirkning fx i forhold til arbejdsklausuler, ligestilling mv.

Krav om redegørelse for samfundsansvar i regnskabet, gælder kun virksomheder underlagt årsregnskabsloven, og kun virksomheder af en vis størrelse. SIT er således ikke – som en offentlig myndighed – underlagt kravet om redegørelse for samfundsansvar i regnskabet. Tilsynet kan dog altid tage emner omkring fx bæredygtighed, samfundsansvar, grønne initiativer mv. op, hvor det vurderes relevant, og rapportere dette på linje med øvrigt tilsyn. Alle institutioner har sociale, miljømæssige og etiske problemstillinger i større eller mindre grad. For SIT kan dette fx give udslag i:

- Energiforbrug og miljøpåvirkning af datacentre
- Krav til leverandører af udstyr og andet
- Genanvendelse frem for destruktion af udtjent udstyr

---

3 Kilde: CSR Kompasset ved Nordisk Ministerråd, Erhvervsministeriet og Dansk Industri
4 Kilde: CSR Kompasset ved Nordisk Ministerråd, Erhvervsministeriet og Dansk Industri
5 Kilde: Erhvervsstyrelsen

3. Rapportering

FM-DEP planlægger, udfører og afrapporterer tilsynet. Dette sker i forskellige dokumenter, som deles med SIT og med kunderne.

De nærmere rapporteringer gennemgås nedenfor, herunder vejledes SIT's kunder i behandlingen af tilsynets rapporteringer.

3.1 Løbende skriftlige tilsynsrapporter

Tilsynet afgiver løbende tilsynsrapporter omkring specifikke tilsynsgennemgange.

I tilsynsrapporterne afgives bedømmelse af det undersøgte område (Rød: Ikke tilfredsstillende, Gul: Ikke helt tilfredsstillende og Grøn: Tilfredsstillende). Derudover afgives eventuelle specifikke bemærkninger og anbefalinger til SIT, som indtastes i Finansministeriets Revisionsstyrings- og tilsynssystem (FIRST).

Det er altid muligt at rekvirere tilsynsrapporterne hos FM-DEP. Enkelte rapporter kan dog være helt eller delvist fortrolige. Den årlige tilsynsrapport om SIT's rolle som databehandler udsendes i maj måned af SIT.

3.2 Årlig tilsynsberetning

Tilsynets konklusioner samles i en årlig "*Beretning om tilsynet med Statens It*" ('tilsynsberetningen'), som indledningsvist forelægges og drøftes med Finansministeriets ledelse. Efterfølgende deles og drøftes tilsynsberetningen med SIT's kunder.

SIT udsender tilsynsberetningen til alle kunder ca. primo maj måned.

Tilsynsrapporten omkring SIT's rolle som databehandler indgår på lige fod med andre tilsynsrapporter i den årlige tilsynsberetning.

I den årlige tilsynsberetning redegøres der endvidere for resultatet af eventuelle tilsyn med SIT udført fra Datatilsynet samt om resultatet af SIT's eksterne ISO-audit. Endvidere rapporteres om eventuelle resultater af Rigsrevisionens undersøgelser i SIT.

I tilsynsberetningen rapporteres endvidere om fremdriften på opfølgning på tidligere bemærkninger fra tilsynet og Rigsrevisionen.

3.3 Mundtlige afrapporteringer

FM-DEP deltager fast i SIT's Arbejdsgruppe for informationssikkerhed, hvor alle kunder har mulighed for at deltage.

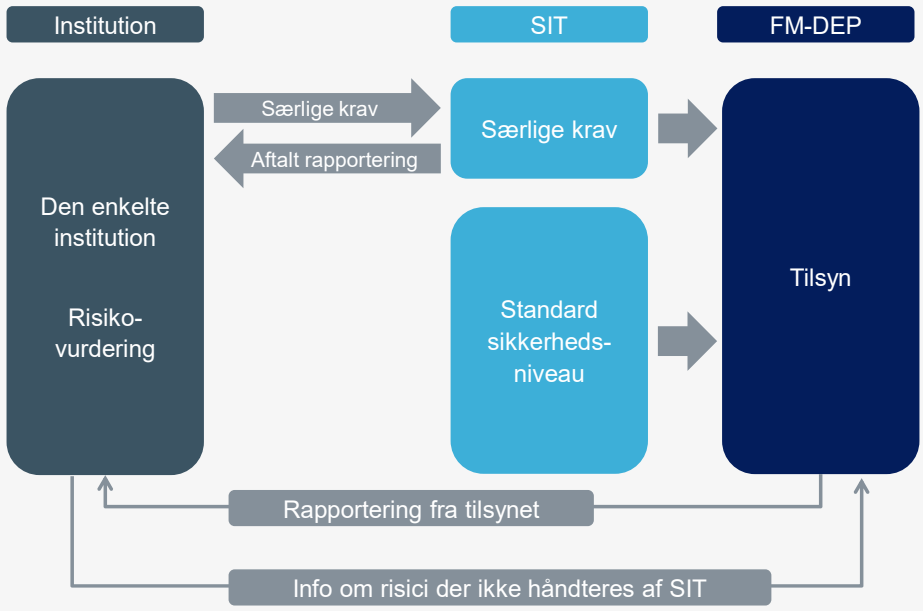
Tilsynet rapporterer på hvert møde i Arbejdsgruppen omkring tilsynsundersøgelser, der er afgivet i endelig form siden seneste møde. På møderne i Arbejdsgruppen har kunderne mulighed for at spørge mere detaljeret ind til resultatet af tilsynsundersøgelserne, og der er dialog omkring risici, handlemuligheder mv. for SIT og for kunderne.

Derudover præsenteres i overordnet form tilsynets plan og status herfor på hvert møde.

Den årlige tilsynsberetning drøftes på et særskilt møde i Arbejdsgruppen for informationssikkerhed samt med DPO-hub og Kundeforum. Disse møder planlægges afholdt i umiddelbar forlængelse af fremsendelsen af tilsynsberetningen.

3.4 Vejledning til kundernes behandling af tilsynets rapportering

Figur 3.1
Model for rapportering



Risikovurderinger

Som figuren ovenfor viser, er det den enkelte institutions ansvar at risikovurdere anvendte systemer. Risikovurderingen munder ud i en vurdering af, om identificerede risici for det enkelte system stiller særlige krav til sikkerhedsforanstaltninger.

Når man har etableret et overblik over særlige krav til sikkerhedsforanstaltninger, vurderer institutionen, om den enkelte sikkerhedsforanstaltning ligger ud over SIT's standard sikkerhedsniveau, som beskrevet i varedeklarationen.

Standard sikkerhedsniveau (varedeklarationen)

Vurderer institutionen, baseret på risikovurderingen, at det aktuelle system ikke kræver særlige sikkerhedsforanstaltninger og derfor er dækket af SIT's standard sikkerhedsniveau, som beskrevet i varedeklarationen, vil det formentligt være tilstrækkeligt for institutionen ikke at gøre yderligere. Institutionen kan således basere sig på den årlige tilsynsberetning fra FM-DEP, samt den løbende afrapportering af tilsynet på møderne i Arbejdsgruppen for informationssikkerhed og vur-

dere relevansen af de eventuelle risici, som påpeges. Alle FM-DEP's afrapporteringer kan give anledning til, at kunderne revurderer deres risikovurdering og justerer heri.

Særlige krav (sikkerhedsforanstaltninger)

Vurderer institutionen, baseret på risikovurderingen, at det aktuelle system kræver særlige sikkerhedsforanstaltninger, der ikke – eller kun delvist – er dækket af SIT's standard sikkerhedsniveau, som beskrevet i varedeklarationen, skal institutionen stille krav til SIT om etablering af den ønskede sikkerhedsforanstaltning. Noget tilsvarende kan være tilfældet over for tredjepartsleverandører under driftsmodel 5.

Dette skal medføre en aftale mellem institutionen og SIT om, hvorledes disse særlige krav imødekommes af SIT, hvorledes SIT afrapporterer leverancen, og hvorledes disse særlige krav skal afregnes fremover. Særlige krav udmøntes typisk i en særlig sikkerhedsforanstaltning, eller en hyppigere udførelse af en bestående. Eksempler kunne være udvidet logning eller kundens adgang til denne i SIEM.

Afrapportering på særlige sikkerhedsforanstaltninger bør være skriftlige og være baseret på fakta mere end på vurderinger. Det bør således være den enkelte institution, der foretager vurderinger baseret på afrapporteringen. Som et eksempel kan gives et ESDH[6]-system, hvor risikovurderingen resulterede i et særligt krav om hyppigere reetableringstests, end SIT's standard driftsydelse omfatter for det pågældende system. Den særlige afrapportering omfatter en rapport om den gennemførte reetableringstest, med angivelse af hvad der er gennemført, hvornår det er gennemført, hvad resultatet var, hvor lang tid det tog osv. Institutionen kan på baggrund af denne rapport vurdere, om den særlige sikkerhedsforanstaltning er gennemført som aftalt, og om den gennemførte reetableringstest giver anledning til ændringer i driften af ESDH-systemet.

Den enkelte institution skal anvende den aftalte afrapportering af den særlige sikkerhedsforanstaltning og kan på denne baggrund dokumentere at have fulgt op på de særlige krav.

Information om risici, der ikke håndteres af SIT

Alle institutioner, som er kunder hos SIT, kan henvende sig til FM-DEP omkring kritiske forhold, som de ikke finder, er tilstrækkeligt håndteret af SIT.

---

6 Elektronisk sags- og dokumenthåndteringssystem (ESDH)

Kontakten kan ske telefonisk eller ved mail til tilsynskontoret Tilsyn@fm.dk.

Dette kan være tilfældet, hvis institutionen fx oplever, at SIT vurderer en trussel helt anderledes end institutionen gør, eller såfremt SIT ikke drifter i henhold til aftalte sikkerhedsprocesser. Første henvendelse bør altid ske til SIT, mens orientering af tilsynet bør ske i de situationer, hvor SIT ikke håndterer risikoen.

fm.dk