FINANSMINISTERIET

Vejledning om tilsynet med Statens it

December 2017

2017

Vejledning om tilsynet med Statens it
December 2017

Denne publikation er udarbejdet af
Finansministeriet
Kontor for revision og tilsyn
Christiansborg Slotsplads 1
1218 København K
Telefon 33 92 33 33

Elektronisk publikation:
ISBN: 978-87-93531-31-4

Publikationen kan hentes på
Finansministeriets hjemmeside
fm.dk

Indhold

1. Indledning

Læsevejledning

Efter et indledende afsnit om baggrunden for vejledningen beskrives grundlaget for tilsyn ved ressortoverførsel af it-drift.

I kapitel 3 beskrives, hvilke dele af Statens It[1]s drift, der er omfattet af Finansministeriets departements tilsyn, og hvilket ansvar, der påhviler de enkelte institutioner i den forbindelse.

Endeligt redegøres der til sidst for rapporteringen af tilsynet med SIT.

Formålet med vejledningen er at uddybe og præcisere ansvars- og opgavefordelingen for varetagelsen af tilsynet med SIT's opgavevaretagelse i forhold til de institutioner, der har fået deres basale it-drift ressortoverdraget. Vejledningen skal give et klart billede af den opgave, der påhviler de enkelte institutioner i relation til Finansministeriets[2] varetagelse af tilsynet med SIT.

Rigsrevisionen[3] afgav i november 2016 en beretning om Styring af it-sikkerhed hos it-leverandører, hvor Erhvervs- og vækstministeriet (Søfartsstyrelsen) og Beskæftigelsesministeriet (Styrelsen for Arbejdsmarked og rekruttering) var omfattet af undersøgelsen. Begge var kunder i SIT på tidspunktet for revisionen.

I RR's beretning skete ikke en skelnen mellem de krav, der stilles til kunderne hos private it-leverandører og kunderne i SIT. RR fandt grundlag for at bemærke, at der bestod en uklarhed hos de enkelte institutioner omkring ansvars- og opgavefordelin-

[1] Statens It, herefter SIT.
[2] Finansministeriet, herefter FM.
[3] Rigsrevisionen, herefter RR.

gen i forhold til tilsynet med SIT – dette mellem FM og de to SIT-kunder, som var omfattet af undersøgelsen.

Beretningen gav anledning til, at Ministeren for Offentlig Innovation oplyste til statsrevisorerne, at Finansministeriet ville tage initiativ til at beskrive omfanget af sit tilsyn med SIT.

FM's departement[4] nedsatte efterfølgende en arbejdsgruppe med FM-DEP og SIT samt følgende institutioner, der alle har fået deres basale it-drift ressortoverdraget til SIT:

- Erhvervsministeriet
- Beskæftigelsesministeriet
- Miljø- og fødevareministeriet
- Uddannelses- og forskningsministeriet

Arbejdsgruppen har givet værdifuld indsigt i institutionernes behov for beskrivelse og præcisering af tilsynet og har givet input til niveau og omfang af beskrivelsen, således at deres behov kan imødekommes.

Arbejdsgruppen har drøftet vejledningens indhold med RR på i alt 3 møder – dette set i lyset af RR's konklusioner i beretning om styring af it-sikkerhed hos it-leverandører. Drøftelserne har haft til formål også at sikre forankringen hos RR.

Vejledningen adresserer ikke tilsynet med GDPR, herunder muligheden for at SIT's kunder kan uddelegere varetagelsen af tilsynet med SIT's overholdelse af reglerne omkring persondata. Dette behandles i særskilt vejledning.

Vejledningen har været udsendt i udkast til orientering for deltagerne i SIT's informationssikkerhedskomité og deres bemærkninger er indarbejdet i vejledningen.

Vejledningen er godkendt af Finansministeriets ledelse og fremsendes til SIT's kundestrategiske forum til orientering.

[4] Departement, herefter DEP.

2. Ressortoverførsel til Statens It

Regeringens Økonomiudvalg har i august 2016 besluttet, at ministerområder og institutioner, der står uden for et større it-fællesskab, skal overgå til SIT. Dette har givet anledning til, at Statsministeriet har udarbejdet et notat om overdragelse af it-drift af 6. februar 2017.

I Statsministeriets notat gøres det klart, at den korrekte måde at overføre it-drift til SIT er ved kongelig resolution (ressortoverførsel). Det tydeliggøres, at alene én minister kan være ansvarlig for den opgavevaretagelse, som overføres.

> ”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 indenfor 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 ressortoverførsel indebærer dette, ”at også ansvaret for ressortområdet, herunder også tilsynet for det 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 om overdragelse af it-drift, punkt 7.*

Ved ressortoverførsel af den basale IT-drift fra de enkelte institutioner til SIT (FM) overgår tilsynet med den basale it-drift således også til FM, hvilket fritager det afgivende ministerium for at udføre tilsynet.

It-drift hænger meget nært sammen med driften af et ministerium. Således vil der også være en række grænseflader i forhold til overførsel af tilsynsforpligtelsen, som skal præciseres. Dette afhænger af indholdet af den pågældende ressortoverførsel og dermed valget af driftsmodeller[5].

[5] Driftsmodeller: Statens It har på systemniveau struktureret sine leverancer overfor kunderne i driftsmodeller. Hvis driftsmodellen omfatter alle niveauer (applikationer, middleware, operativsystem, server/storage, netværk og fysisk lokation) benævnes det driftsmodel 1. Jo færre områder, der er omfattet af aftalen, jo højere benævnes driftsmodellen, hvis driftsmodellen fx kun omfatter netværk og fysisk lokation, benævnes den driftsmodel 5.

3. Tilsynets omfang

Det essentielle i tilsynsmodellen er, at tilsynsopgaven med SIT udføres af FM på vegne af de øvrige ministerier, som følge af ressortoverførslen.

Tilsynet omfatter al den basale it-drift, som udføres i SIT på vegne af andre ministerier og for FM selv.

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 og
- om der er taget hensigtsmæssig stilling til og håndtering af bemærkninger og anbefalinger fra revisions- og tilsynsmyndigheder.

FM-DEP planlægger, udfører og afrapporterer tilsynet med SIT. Den endelige tilsynsrapport forelægges og drøftes årligt med kundestrategisk forum, ligesom den fremsendes til de enkelte institutioner.

3.1 Indenfor SIT standard drift

Med udgangspunkt i ISO 27001 fører FM's DEP tilsyn med SIT's standard driftsmiljø på alle relevante områder.

Statens It har i dokumentet "IT sikkerhedskontroller i Statens It's standardydelser" beskrevet de IT sikkerhedskontroller, der udføres i forbindelse med SIT's standard driftsydelser. Dokumentet er fremsendt til de enkelte institutioner og går i daglig tale under navnet "varedeklarationen" eller "SIT's varedeklaration".

I hvilket omfang FM's DEP's tilsyn med SIT's standard driftsmiljø fritager den enkelte institution for at udføre tilsyn, afhænger af driftsmodellen for det enkelte system.

Tilsynsoversigt

<table>
<tr><th></th><th>Model 5
Outsourcet drift til 3. part</th><th>Model 3
Infrastruktur-service</th><th>Model 2A
Platformdrift</th><th>Model 2
Platform-service</th><th>Model 1A
Applikations-drift</th><th>Model 1
Applikations-service</th><th>ISO 27001:2013 referencer</th></tr>
<tr><td>Ledelsens Informations-sikkerheds-styring</td><td colspan="6">Vil være omfattet af tilsynsaktiviteter i en turnusordning</td><td>ISO 27001 punkt 4-10, samt:
A.5 Informationssikkerhedspolitikker
A.6 Organisering af informationssikkerhed</td></tr>
<tr><td>Applikationer

ESDH,
Fagsystemer,
Portaler,
Sharepoint,
Web, etc.</td><td>Ikke omfattet af FM's tilsyn
Til højre har vi noteret de ISO 27001 områder, der er mest relevante for applikationslaget, og som derfor er den enkelte institutions eget ansvar. For driftsmodel 5 omfatter ansvaret primært:

6.1 Den enkelte institution udarbejder risikovurderinger, som bl.a. omfatter anvendte applikationer.

A.9 Den enkelte institution fører fx tilsyn med oprettede brugere i (eller til) selve applikationen, inklusive leverandørens medarbejdere, konsulenter m.fl.

A.17 Den enkelte institution udarbejder egne beredskabsplaner om fx manuelle procedurer i en beredskabssituation.</td><td colspan="3">Ikke omfattet af FM's tilsyn
Til højre har vi noteret de ISO 27001 områder, der er mest relevante for applikationslaget, og som derfor er den enkelte institutions eget ansvar. Ansvaret omfatter fx:

6.1 Den enkelte institution udarbejder risikovurderinger, som bl.a. omfatter anvendte applikationer.

A.9 Den enkelte institution fører fx tilsyn med oprettede brugere i (eller til) selve applikationen, inklusive SIT medarbejdere, konsulenter m.fl.

A.12 Sårbarhedsstyring: Den enkelte institution skal sikre, at applikationen kan afvikles på supporterbare versioner af software.

A.15.1.2 Den enkelte institution har initiativpligten omkring udarbejdelsen af en databehandleraftale for applikationer (data)

A.17 Den enkelte institution udarbejder egne beredskabsplaner om fx manuelle procedurer i en beredskabssituation

Omfattet af FM's tilsyn

A.12 Backup: I det omfang der er etableret aftale med SIT om backup, vil denne være omfattet af FM's tilsyn.

A.17 Reetablering efter en større hændelse er omfattet af tilsynet.

Enkeltstående regnskabsrelevante systemer kan være omfattet af den finansielle revision eller review.</td><td>Omfattet af FM's tilsyn

Applikationer 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><td>6.1.2 Vurdering af informationssikkerhedsrisici
A.8.2.1 Klassifikation af information
A.9 Adgangsstyring
A.12 Driftssikkerhed, herunder:
*Ændringsstyring
* Backup
* Logning og overvågning
A.15.1.2 Håndtering af sikkerhed i leverandøraftaler
* Sårbarhedsstyring
A.17 Informationssikkerhedsaspekter ved nød-, beredskabs-og reetablerings-styring</td></tr>
<tr><td>Middleware

Oracle,
SQL, etc.</td><td>Omfattet af FM's tilsyn
Det vil være SIT's ansvar at følge op på sikkerheden hos 3. parts leverandøren med udgangspunkt i kontrakten og som et led i leverandørstyringen.

FM DEP fører tilsyn med SIT's leveran-dørstyring.</td><td>Ikke omfattet af FM's tilsyn
Det vil være institu-tionens eget an-svar, at databaser lever op til SIT's "Krav til database-sikkerhed".</td><td>Ikke omfattet af FM's tilsyn
Det vil være institutionens eget ansvar, at databaser lever op til SIT's "Krav til databasesikkerhed".

Omfattet af FM's tilsyn
Standard komponenter som backup, patchning af supporterede databaseversioner, ændringsstyring mv.</td><td colspan="2">Omfattet af FM's tilsyn
Tilsynet omfatter SIT's håndtering af de nævnte områder i ISO 27001 i en turnusordning.

Adgangsstyring og ændringsstyring gennemgås hvert år.
Fysisk sikkerhed og backup vurderes hvert år.

Kræver at databaserne lever op til SIT's "Krav til databasesikkerhed". Det vil kortfattet sige:
* Et supporteret databasesystem
* En database der kan holdes løbende opdateret</td><td>A.9 Adgangsstyring
A.12 Driftssikkerhed, herunder:
* Ændringsstyring
* Backup
* Logning og overvågning
* Sårbarhedsstyring</td></tr>
<tr><td>Operativsystem

Windows,
Linux, etc.</td><td>Omfattet af FM's tilsyn
Det vil være SIT's ansvar at følge op på sikkerheden hos 3. parts leverandøren med udgangspunkt i kontrakten og som et led i leverandørstyringen.

FM DEP fører tilsyn med SIT's leveran-dørstyring.</td><td colspan="4">Omfattet af FM's tilsyn

Tilsynet omfatter SIT's håndtering af de nævnte områder i ISO 27001 i en turnusordning.

Adgangsstyring og ændringsstyring gennemgås hvert år.
Fysisk sikkerhed og backup vurderes hvert år.
FM fokuserer på standard operativsystem og -version.</td><td>A.9 Adgangsstyring
A.10 Kryptografi
A.12 Driftssikkerhed, herunder:
* Ændringsstyring
* Beskyttelse mod malware
* Backup
* Logning og overvågning
* Sårbarhedsstyring</td></tr>
<tr><td>Server/Storage

Virtuel server,
fysisk server,
datalagring, etc.</td><td>Omfattet af FM's tilsyn
Det vil være SIT's ansvar at følge op på sikkerheden hos 3. parts leverandøren med udgangspunkt i kontrakten og som et led i leverandørstyringen.

FM DEP fører tilsyn med SIT's leveran-dørstyring.</td><td colspan="4">Omfattet af FM's tilsyn
Tilsynet omfatter SIT's håndtering af de nævnte områder i ISO 27001 i en turnusordning.

Adgangsstyring og ændringsstyring gennemgås hvert år.
Fysisk sikkerhed og backup vurderes hvert år.
FM fokuserer på standard miljøet.</td><td>A.8 Styring af aktiver
A.9 Adgangsstyring
A.10 Kryptografi
A.12 Driftssikkerhed, herunder:
* Ændringsstyring
* Beskyttelse mod malware
* Logning og overvågning
* Sårbarhedsstyring</td></tr>
<tr><td>Netværk

Core, WAN,
LAN, Firewall, etc.</td><td>Omfattet af FM's tilsyn
Det vil være SIT's ansvar at følge op på sikkerheden hos 3. parts leverandøren med udgangspunkt i kontrakten og som et led i leverandørstyringen.

FM DEP fører tilsyn med SIT's leveran-dørstyring</td><td colspan="4">Omfattet af FM's tilsyn
Tilsynet omfatter SIT's håndtering af de nævnte områder i ISO 27001 i en turnusordning.
Adgangsstyring og ændringsstyring gennemgås hvert år.
Fysisk sikkerhed og backup vurderes hvert år.</td><td>A.8 Styring af aktiver
A.9 Adgangsstyring
A.10 Kryptografi
A.12 Driftssikkerhed, herunder:
* Ændringsstyring
* Beskyttelse mod malware
* Logning og overvågning
* Sårbarhedsstyring
A.13 Kommunikationssikkerhed</td></tr>
<tr><td>Fysisk lokation

M2, Køl, Strøm,
Racks,
Fysisk sikkerhed etc.</td><td>Omfattet af FM's tilsyn
Det vil være SIT's ansvar at følge op på sikkerheden hos 3. parts leverandøren med udgangspunkt i kontrakten og som et led i leverandørstyringen.

FM DEP fører tilsyn med SIT's leveran-dørstyring.</td><td colspan="4">Omfattet af FM's tilsyn
Tilsynet omfatter SIT's håndtering af de nævnte områder i ISO 27001 i en turnusordning.
Adgangsstyring gennemgås hvert år.
Fysisk sikkerhed vurderes hvert år.</td><td>A.8 Styring af aktiver
A.9 Adgangsstyring
A.11 Fysisk sikring og miljøsikring</td></tr>
<tr><td>Tværgående områder</td><td colspan="5">Omfattet af FM's tilsyn

Tilsynet omfatter SIT's håndtering af de nævnte områder i ISO 27001 i en turnusordning.</td><td>A.7 Personalesikkerhed
A.14 Anskaffelse, udvikling og vedlige-holdelse af systemer
A.15 Leverandørforhold
A.16 Styring af informationssikkerhedsbrud
A.17 Informationssikkerhedsaspekter ved nød-, beredskabs-og reetableringsstyring
A.18 Overensstemmelse</td></tr>
</table>

Opdeling af driftsmodeller

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

Lag i it-infrastrukturen

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

I RR's beretning om Styring af it-sikkerhed hos it-leverandører anvendes en anden opdeling af teknologistakken. RR har opdelt applikation i "Brugergrænseflade" og "Applikation", og server/storage i "Eventuel hypervisor" og "Fysisk server (fx iLO™ og DRAC)™".

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.

ISO 27001:2013 referencer

I denne kolonne har vi noteret de ISO 27001 områder, der er mest relevante for laget i teknologistakken. Vi har gjort det samme for Ledelsens informationssikkerhedsstyring og Tværgående områder.

Tilsynets udførelse

Tilsynet udføres dels i form af en række uddybende tilsyn, og dels i form af en række tilsynsaktiviteter ud fra en spørgeramme, jf. Digitaliseringsstyrelsens vejledning om it-tilsyn. Begge områder tager udgangspunkt i ISO 27001, og vurderer den implementerede informationssikkerhed i SIT mod varedeklarationen, mod ISO 27002, mod anerkendt eller bedste praksis (best practice[6]) og mod gældende lovgivning.

FM fører tilsyn ud fra en turnus, hvor alle væsentlige områder i ISO-standarden gennemgås inden for en 3-årig periode. FM-DEP deltager herudover i RR's revisioner hos SIT.

FM-DEP påser endvidere, at SIT foretager opfølgning på RR og DEP's tidligere fremsatte bemærkninger.

---

[6] Kilde: BusinessDictionary.com. **Best Practice** – A method or technique that has consistently shown results superior to those achieved with other means, and that is used as a benchmark

Kundens ansvar og handlinger som følge af tilsynsoversigten

I de kommende afsnit er det for hver driftsmodel beskrevet hvilke opgaver, der påhviler den enkelte institution, og hvilke opgaver der udføres af FM-DEP. I bilag 1 er det for udvalgte driftsmodeller og for konkrete systemer anvist, hvorledes en risikoanalyse kan struktureres og hvilke opgaver, der påhviler den enkelte institution.

Driftsmodel 1 (Applikations-service):
Hvis en institution har et system, som SIT drifter i henhold til driftsmodel 1, vil institutionen af tilsynsoversigten kunne aflæse, at FM's tilsyn dækker alle lag i it-infrastrukturen.

Dette betyder således, at såfremt institutionen i sin risikovurdering har vurderet, at systemet ikke kræver særlige sikkerhedsforanstaltninger, og derfor er dækket af SIT's standard sikkerhedsniveau[7], som beskrevet i varedeklarationen, så skal institutionen ikke gøre yderligere. Den enkelte institution skal dog altid læse den årlige tilsynsrapport fra FM og vurdere, om eventuelle kritikpunkter heri kan have betydning for institutionens egne systemer.

Typiske eksempler på systemer i driftsmodel 1 er SIA[8], VIA[9], MIA[10], Exchange (e-mail), Fællesdrev m.fl.

SIA, VIA, MIA og andre løsninger er valgfrie og kan tilkøbes.

Hvis institutionen har et system i driftsmodel 1, vil de således skulle:

- Foretage risikovurdering af systemet. Risikovurderingen skal bl.a. tage udgangspunkt i følgende forhold.
    - Såfremt institutionen har tilkøbt særlige sikkerhedsforanstaltninger, skal institutionen føre tilsyn med, at disse er effektive. Dette sker gennem kontrol af den aftalte rapportering[11].
    - Forholde sig til FM's tilsynsrapport med fokus på, om kritiske forhold har relevans for systemet.
    - Deltage i relevante kundefora, som SIT stiller til rådighed.
- Systematisk dokumentere at have gennemført ovenstående punkter.

I bilag 1.1 er vist en case for driftsmodel 1 omkring risikovurdering af Exchange for FM.

---

[7] Hvis institutionen i sin risikovurdering har vurderet, at et standard sikkerhedsniveau er tilstrækkeligt for det enkelte system, vil det normalt ikke være nødvendigt at gennemgå SIT's varedeklaration i detaljer. SIT's varedeklaration anvendes primært i forbindelse med definition af særlige sikkerhedsforanstaltninger.
[8] SIA, Statens It Arbejdsplads.
[9] VIA, Virtuel It Arbejdsplads.
[10] MIA, Mobil It Arbejdsplads.
[11] Se afsnittet "Rapportering" for yderligere beskrivelse af afrapportering på særlige sikkerhedsforanstaltninger.

Driftsmodel 1A (Applikations-drift) og 2 (Platform-service):
Hvis en institution har et system, som SIT drifter i henhold til driftsmodel 1A eller driftsmodel 2, vil institutionen af tilsynsoversigten kunne aflæse, at FM's tilsyn ikke dækker alle lag i it-infrastrukturen (grøn markering for dele af applikationslaget).

Dette betyder således, at såfremt institutionen i sin risikovurdering har vurderet, at systemet ikke kræver særlige sikkerhedsforanstaltninger, og derfor er dækket af SIT's standard sikkerhedsniveau[12], som beskrevet i varedeklarationen, så skal institutionen ikke gøre yderligere for de lag i it-infrastrukturen, som dækkes af FM's tilsyn. Den enkelte institution skal dog altid læse den årlige tilsynsrapport fra FM og vurdere, om eventuelle kritikpunkter heri kan have betydning for institutionens egne systemer.

Et typisk eksempel på et system i driftsmodel 1A kunne være journaliseringssystemet Public 360.

Hvis institutionen har et system i driftsmodel 1A eller driftsmodel 2, vil de således skulle:

- Foretage risikovurdering af systemet. Risikovurderingen skal bl.a. tage udgangspunkt i følgende forhold.
    - Foretage tilsyn med applikationslaget, hvilket typisk omfatter de områder fra ISO 27001, som er listet i tilsynsoversigten.
    - Såfremt institutionen har tilkøbt særlige sikkerhedsforanstaltninger, skal institutionen føre tilsyn med, at disse er effektive. Dette sker gennem kontrol af den aftalte rapportering[13].
    - Forholde sig til FM's tilsynsrapport med fokus på, om kritiske forhold har relevans for systemet.
    - Deltage i relevante kundefora, som SIT stiller til rådighed.
- Systematisk dokumentere at have gennemført ovenstående punkter.

I bilag 1.2 er vist en case for driftsmodel 1A vedrørende risikovurdering af Public 360 for EM[14].

[12] Hvis institutionen i sin risikovurdering har vurderet, at et standard sikkerhedsniveau er tilstrækkeligt for det enkelte system, vil det normalt ikke være nødvendigt at gennemgå SIT's varedeklaration i detaljer. SIT's varedeklaration anvendes primært i forbindelse med definition af særlige sikkerhedsforanstaltninger.
[13] Se afsnittet "Rapportering" for yderligere beskrivelse af afrapportering på særlige sikkerhedsforanstaltninger.
[14] EM – Erhvervsministeriet.

Driftsmodel 2A (Platform-drift):
Hvis en institution har et system, som SIT drifter i henhold til driftsmodel 2A, vil institutionen af tilsynsoversigten kunne aflæse, at FM's tilsyn ikke dækker alle lag i it-infrastrukturen (grøn markering for dele af applikationslaget og dele af middlewarelaget).

Dette betyder således, at såfremt institutionen i sin risikovurdering har vurderet, at systemet ikke kræver særlige sikkerhedsforanstaltninger, og derfor er dækket af SIT's standard sikkerhedsniveau[15], som beskrevet i varedeklaration, så skal institutionen ikke gøre yderligere for de lag i it-infrastrukturen, som dækkes af FM's tilsyn. Den enkelte institution skal dog altid læse den årlige tilsynsrapport fra FM's DEP og vurdere, om eventuelle kritikpunkter heri kan have betydning for institutionens egne systemer.

Et typisk eksempel på et system i driftsmodel 2A kunne være Skibsregisteret Martha 1.

Hvis institutionen har et system i driftsmodel 2A, vil de således skulle:

- Foretage risikovurdering af systemet. Risikovurderingen skal bl.a. tage udgangspunkt i følgende forhold.
  - Foretage tilsyn med applikationslaget, hvilket typisk omfatter de områder fra ISO 27001, som er listet i tilsynsoversigten.
  - Foretage tilsyn med middlewarelaget (databaser), hvilket typisk omfatter de områder fra ISO 27001, som er listet i tilsynsoversigten.
  - Såfremt institutionen har tilkøbt særlige sikkerhedsforanstaltninger, skal institutionen føre tilsyn med, at disse er effektive. Dette sker gennem kontrol af den aftalte rapportering[16].
  - Forholde sig til FM's tilsynsrapport med fokus på, om kritiske forhold har relevans for systemet.
  - Deltage i relevante kundefora, som SIT stiller til rådighed.
- Systematisk dokumentere at have gennemført ovenstående punkter.

I bilag 1.3 er vist en case for driftsmodel 2.A vedrørende risikovurdering af Skibsregisteret Martha 1 for EM.

---

[15] Hvis institutionen i sin risikovurdering har vurderet, at et standard sikkerhedsniveau er tilstrækkeligt for det enkelte system, vil det normalt ikke være nødvendigt at gennemgå SIT's varedeklaration i detaljer. SIT's varedeklaration anvendes primært i forbindelse med definition af særlige sikkerhedsforanstaltninger.
[16] Se afsnittet "Rapportering" for yderligere beskrivelse af afrapportering på særlige sikkerhedsforanstaltninger.

Driftsmodel 3 (Infrastruktur-service):
Hvis en institution har et system, som SIT drifter i henhold til driftsmodel 3, vil institutionen af tilsynsoversigten kunne aflæse, at FM's tilsyn ikke dækker alle lag i it-infrastrukturen (grøn markering for dele af applikationslaget og hele middlewarelaget).

Dette betyder således, at såfremt institutionen i sin risikovurdering har vurderet, at systemet ikke kræver særlige sikkerhedsforanstaltninger, og derfor er dækket af SIT's standard sikkerhedsniveau[17], som beskrevet i varedeklarationen, så skal institutionen ikke gøre yderligere for de lag i it-infrastrukturen, som dækkes af FM's tilsyn. Den enkelte institution skal dog altid læse den årlige tilsynsrapport fra FM og vurdere, om eventuelle kritikpunkter heri kan have betydning for institutionens egne systemer.

Hvis institutionen har et system i driftsmodel 3, vil de således skulle:

- Foretage risikovurdering af systemet. Risikovurderingen skal bl.a. tage udgangspunkt i følgende forhold.
  - Foretage tilsyn med applikationslaget, hvilket typisk omfatter de områder fra ISO 27001, som er listet i tilsynsoversigten.
  - Foretage tilsyn med middlewarelaget (databaser), hvilket typisk omfatter de områder fra ISO 27001, som er listet i tilsynsoversigten.
  - Såfremt institutionen har tilkøbt særlige sikkerhedsforanstaltninger, skal institutionen føre tilsyn med, at disse er effektive. Dette sker gennem kontrol af den aftalte rapportering[18].
  - Forholde sig til FM's tilsynsrapport med fokus på, om kritiske forhold har relevans for systemet.
  - Deltage i relevante kundefora, som SIT stiller til rådighed.
- Systematisk dokumentere at have gennemført ovenstående punkter.

Driftsmodel 5 (Outsourcet drift til 3. part):
Hvis en institution har et system, som SIT drifter i henhold til driftsmodel 5, vil institutionen af tilsynsoversigten kunne aflæse, at FM's tilsyn ikke dækker alle lag i it-infrastrukturen (grøn markering for applikationslaget).

Dette betyder således, at såfremt institutionen i sin risikovurdering har vurderet, at systemet ikke kræver særlige sikkerhedsforanstaltninger, ud over de der er beskrevet i kontrakten med den eksterne leverandør, så skal institutionen ikke gøre yderligere for de lag i it-infrastrukturen, som tilsynet i FM dækker. Den enkelte institution skal dog altid læse revisorerklæringer, referat af SIT's årlige sikkerhedsaudit hos eksterne leve-

---

[17] Hvis institutionen i sin risikovurdering har vurderet, at et standard sikkerhedsniveau er tilstrækkeligt for det enkelte system, vil det normalt ikke være nødvendigt at gennemgå SIT's varedeklaration i detaljer. SIT's varedeklaration anvendes primært i forbindelse med definition af særlige sikkerhedsforanstaltninger.

[18] Se afsnittet "Rapportering" for yderligere beskrivelse af afrapportering på særlige sikkerhedsforanstaltninger.

randør og den årlige tilsynsrapport fra FM, og vurdere om eventuelle forbehold, bemærkninger eller kritikpunkter heri kan have betydning for institutionens system.

Hvis institutionen har et system i driftsmodel 5, vil de således skulle:

- Foretage detaljeret risikovurdering af systemet, i forbindelse med udbud og kontraktindgåelse.
- Foretage løbende risikovurdering af systemet. Risikovurderingen skal bl.a. tage udgangspunkt i følgende forhold.
    - Såfremt institutionen har tilkøbt særlige sikkerhedsforanstaltninger, skal institutionen føre tilsyn med, at disse er effektive (SIT såvel som den eksterne leverandør). Dette sker gennem kontrol af den aftalte rapportering[19].
    - Forholde sig til FM's tilsynsrapport med fokus på, om kritiske forhold har relevans for systemet.
    - Indhente revisorerklæringer fra SIT og forholde sig til, om der er forbehold eller supplerende oplysninger, som kræver reaktioner.
    - Rekvirere og forholde sig til SIT's årlige sikkerhedsaudit af eksterne leverandører.
    - Deltage i relevante kundefora, som SIT stiller til rådighed.
- Systematisk dokumentere at have gennemført ovenstående punkter.

I bilag 1.4 er vist en case for driftsmodel 5 omkring risikovurdering af Det fælles data grundlag (DFDG) for STAR[20].

Revisorerklæringer

Institutioner, hvor den basale it-drift er overdraget til SIT, har ikke mulighed for at modtage en revisorerklæring fra SIT. Dette idet ressortansvaret er overgået til SIT.

I de tilfælde, hvor leverandørstyringen er ressortoverført til SIT (driftsmodel 5) og hvor den basale drift at et system således sker hos en ekstern leverandør, er det muligt at indhente revisorerklæring fra den eksterne leverandørs revisor. Ofte sker valget af typen af revisorerklæringer hos eksterne leverandører på tidspunktet for indgåelse af kontrakten og kan efterfølgende kun svært ændres uden økonomiske konsekvenser.

Valget af typen af revisorerklæring skal ske på baggrund af risikovurderingen. Omfanget af revisorerklæringen er givet i kontrakten og bør omfatte det aftalte sikkerhedsniveau. Som oftest er der to parametre, som institutionen skal forholde sig til:

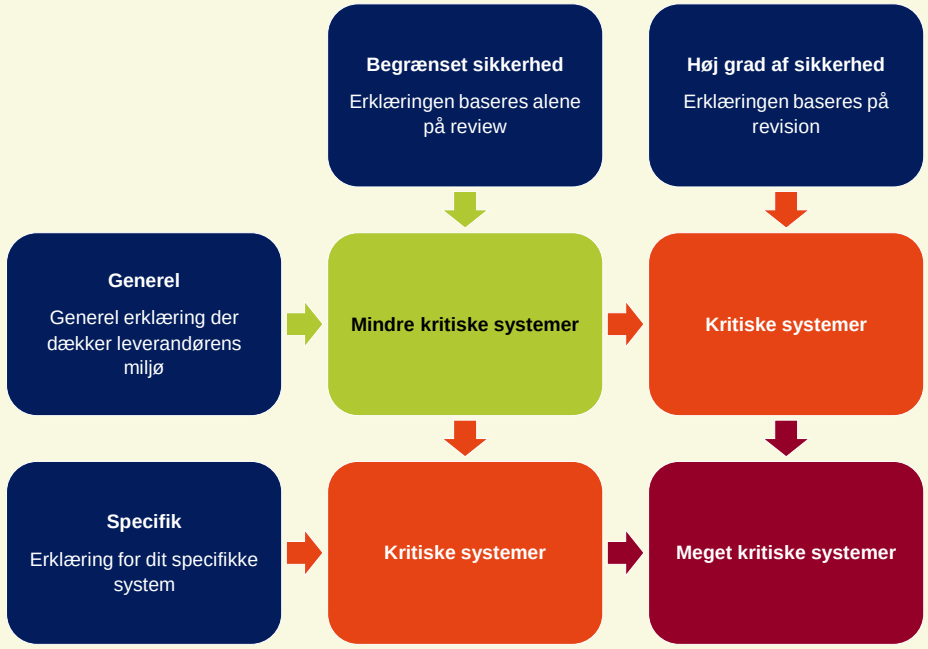
---

[19] Se afsnittet "Rapportering" for yderligere beskrivelse af afrapportering på særlige sikkerhedsforanstaltninger.
[20] STAR – Styrelsen for Arbejdsmarked og Rekruttering.

1. Har institutionen brug for en revisorerklæring, der dækker det specifikke system, eller kan institutionen nøjes med en generel revisorerklæring, der dækker leverandørens miljø?
2. Har institutionen brug for en revisorerklæring med høj grad af overbevisning, som er baseret på revision, eller kan institutionen nøjes med en revisorerklæring med begrænset overbevisning, som er baseret på review?

I figuren "Valg af revisorerklæring" vises de forskellige typer. Det er således den enkelte institution, der vælger hvilken revisorerklæring, der skal leveres fra den eksterne leverandør baseret på risikovurderingen. SIT sikrer på baggrund af revisorerklæringen, at leverandøren leverer de aftalte ydelser. Valget og omfanget af revisorerklæringen kan efterfølgende blive genstand for revision fra RR, FM-DEP eller andre.

Figur 1
Valg af revisorerklæring



For driftsmodel 5 gælder således særlige forhold, da arbejdsfordelingen internt i FM er anderledes. Det er SIT, der gennem varetagelsen af leverandørstyringen følger op på sikkerheden hos 3. parts leverandøren, mens FM-DEP fører tilsyn med SIT's varetagelse af leverandørstyringen. FM-DEP er derfor ikke selv ude hos den eksterne leverandør og udføre tilsyn.

3.2 Udenfor SIT standard drift

SIT's driftsmiljøer kan med fordel beskrives som 3 grupper med forskellige karakteristika, som skitseret i efterfølgende figur "Typer af drift hos SIT".

Figur 2
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. Nogle elementer skal tilkøbes, mens hovedparten altid er omfattet. SIT standard drift omfatter SIA, VIA, MIA, Exchange (e-mail), Fællesdrev og tilsvarende, men også Firewall, ServiceNow og den type systemer.

FM har ansvar for tilsyn med SIT standard drift.

For SIT standard drift omfatter FM's tilsyn alle relevante områder i ISO 27001 standarden, som gennemgås indenfor en treårig periode.

I det omfang der skulle være implementeret særlige sikkerhedsforanstaltninger på vegne af en enkelt institution, er dette forhold ikke omfattet af FM's tilsyn, da de særlige sikkerhedsforanstaltninger ligger udover den basale it-drift, som er ressortoverført.

SIT 1:1 drift

Alle oprindelige institutioner, som blev overført til SIT ved opstarten, har fået deres eget netværkssegment[21], ligesom nye institutioner får ét i forbindelse med transitionsprocessen. I dette netværkssegment, som benævnes 1:1 drift (1 til 1), placeres alle institutionens systemer, som ikke er overtaget af SIT standard drift (eller overført til SIT afsondring).

1:1 drift-miljøet består, så længe ressortoverførslen er gældende.

[21] I denne sammenhæng er et netværkssegment et eller flere netværk, som kan anskues som et hele, typisk beskyttet af en firewall.

Systemer, der anvender forældet software, vil som udgangspunkt være placeret i 1:1 drift og kan derfor udgøre en særlig risiko for institutionens øvrige systemer (se også SIT afsondring).

I 1:1 drift-miljøet findes en række SIT standard drift komponenter som backup, patch, database-drift m.fl., som også beskrevet i tilsynsoversigten[22].

FM har ansvar for tilsyn med SIT 1:1 drift.

For SIT 1:1 drift omfatter FM's tilsyn alle SIT standard drift komponenter, som beskrevet i tilsynsoversigten. Alle relevante områder gennemgås indenfor en treårig periode.

For systemer eller systemkomponenter (OS[23] eller databaser), der anvendes i forældede versioner, indskrænkes tilsynet til at omfatte kontrol med, at SIT løbende orienterer institutionerne om den øgede risiko. Det er FM's udgangspunkt, at den enkelte institution har accepteret risikoen ved anvendelse af forældede versioner.

I det omfang der skulle være implementeret særlige sikkerhedsforanstaltninger i SIT 1:1 drift på vegne af institutionen, er dette forhold ikke omfattet af FM's tilsyn, idet særlige sikkerhedsforanstaltninger ikke er omfattet af ressortoverførslen.

SIT Afsondring

SIT tilbyder en afsondringstjeneste hvori systemer, der anvendes i forældede versioner, kan placeres. Afsondringstjenesten anvendes, hvis risikoen vurderes for værende høj, men hvor systemet af forskellige årsager ikke kan bringes til et tidssvarede sikkerhedsniveau. Der placeres kun ét system i hver afsondringstjeneste.

FM har ansvar for tilsyn med SIT Afsondring.

Det er FM's udgangspunkt, at den enkelte institution har accepteret risikoen ved anvendelse af forældede versioner, og håndteret denne gennem anvendelse af afsondringstjenesten. For SIT Afsondring indskrænkes tilsynet til at omfatte kontrol med selve afsondringstjenesten.

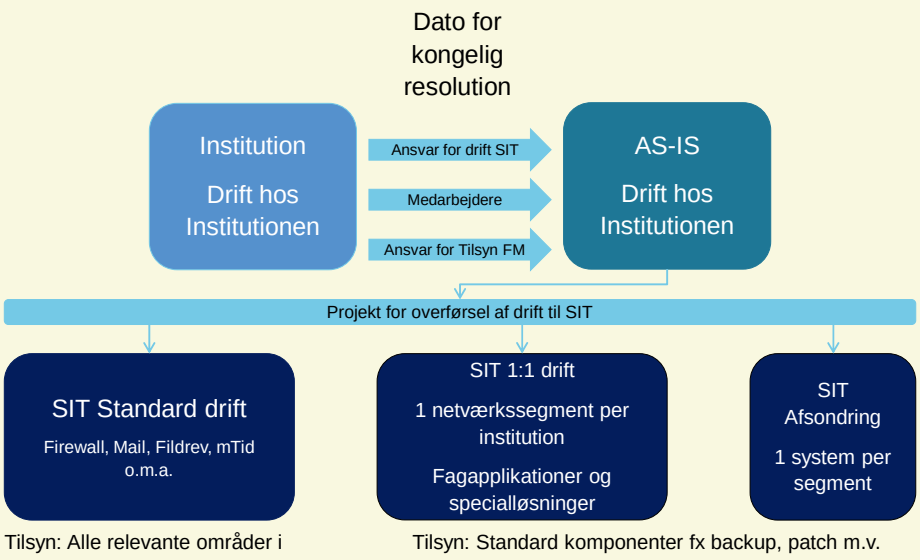
---

[22] Modsvarer driftsmodel 1.
[23] OS – Operativ System.

3.3 Tilsyn under ressortoverførsel/implementerings-proces

For nye institutioner i SIT gælder særlige forhold i ressortoverførsel/implementeringsprocessen, som skitseret i efterfølgende figur "Typer af drift hos SIT – transition".

Figur 3
Typer af drift hos SIT - transition



Institution

I perioden indtil den kongelige resolution træder i kraft, og hvor selve ressortoverførslen sker, har den enkelte institution det fulde ansvar for it-driften.

Som et led i tilsynet med det kommende AS-IS miljøet indgår også, at FM i samarbejde med SIT foretager en IT-sikkerhedsmæssig vurdering af de områder, som skal ressortoverdrages allerede *inden* overførslen – dvs. udfører en form for "due-diligence" inden områder ressortoverdrages. Dette sker for at være tidligt opmærksom på den risiko, der overdrages til FM.

AS-IS

I perioden efter selve ressortoverførelsen fortsætter it-driften uændret, mens ansvaret og medarbejderne er overført til SIT. Samtidigt er ansvaret for tilsynet nu overført til FM.

Som udgangspunkt består der samme risiko i AS-IS-miljøet efter ressortoverførslen som hos institutionen før ressortoverførslen.

Tilsynet med AS-IS-miljøet vil være baseret på kvartalsvise drøftelser med SIT omkring risikoen i AS-IS driften og SIT's håndtering heraf. Tilsynet holder sig således løbende orienteret om udviklingen i denne risiko gennem drøftelser med SIT. Der vil kun i sjældne tilfælde blive foretaget revisionsmæssige test mv. (test af kontroller) fra tilsynets side på AS-IS-drift.

Tilsynet vil have fokus på, at SIT orienterer kunderne om eventuelle risici i AS-IS-driften, og at der er fremdrift i nedlæggelse eller begrænsning af AS-IS-driften.

Efter ressortoverførslen etableres et projekt (eller flere) for successiv overførsel af AS-IS driften fra de bestående lokationer til et af de 3 driftsmiljøer hos SIT.

SIT Standard drift
Funktionalitet, der skal overføres til SIT Standard drift, etableres hos SIT, hvorefter servere m.v. udfases i den enkelte institutions AS-IS miljø.

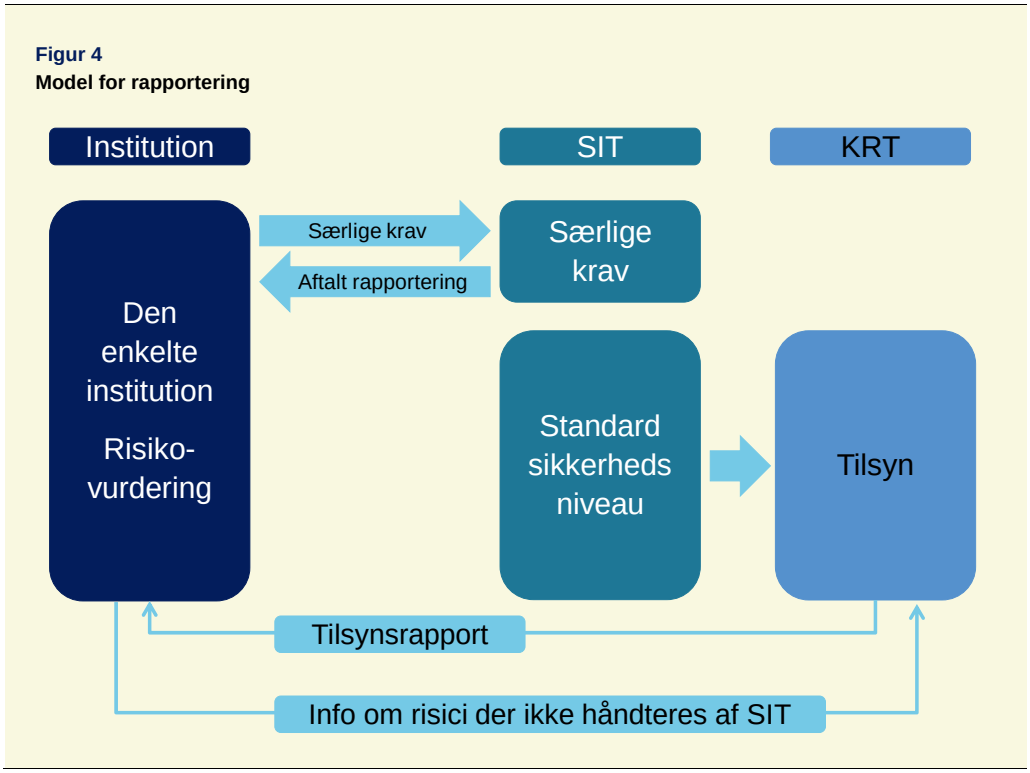
SIT 1:1 drift
Systemer, der skal overføres til SIT 1:1 drift, flyttes som de er. Der kan være tale om etablering af funktionalitet på SIT standard servere, men i udgangspunktet flyttes serverne med til den enkelte institutions 1:1 driftsmiljø.

SIT Afsondring
I det omfang de enkelte institutioner anvender forældede versioner af software, kan institutionen i samarbejde med SIT vælge at flytte disse systemer direkte til en afsondringstjeneste.

Det er projektets mål, at AS-IS miljøet nedlægges fuldstændigt. Der kan dog gå meget lang tid, før dette mål nås, da man i nogle tilfælde må afvente udløbet af kontrakter, licenser, lejemål mv.

3.4 Rapportering

Figur 4
Model for rapportering



Risikovurderinger

Som figuren ovenfor viser, er det den enkelte institutions ansvar at risikovurdere deres systemer. Se en række case-eksempler til inspiration i bilag 1.

Risikovurderingen munder ud i en vurdering af, om den identificerede risiko for det enkelte system stiller særlige krav til sikkerhedsforanstaltninger. Når man har etableret sit overblik over særlige krav til sikkerhedsforanstaltninger, måske i form af en liste, vurderer institutionen, om den enkelte sikkerhedsforanstaltning ligger udover SIT's standard sikkerhedsniveau, som beskrevet i varedeklarationen.

Særlige krav

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 varedeklaration, skal styrelsen stille krav til SIT om etablering af den ønskede sikkerhedsforanstaltning. Noget tilsvarende kan være tilfældet overfor 3. parts leverandører 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 dette særlige krav skal afregnes fremover.

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 konkret eksempel kan gives et ESDH[24]-system, hvor risikovurderingen resulterede i et særligt krav om hyppigere reetableringstests, end SIT's standard driftsydelse omfatter. 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 særlige krav, som et led i sin leverandørstyring og skal således på denne baggrund dokumentere at have fulgt op på de særlige krav. FM's tilsyn omfatter ikke særlige krav stillet af institutionerne, og tilsynet kontrollerer ikke, om SIT overholder aftaler om rapportering. Denne forpligtelse hviler på institutionen selv.

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 varedeklaration, skal institutionen ikke gøre yderligere, men kan basere sig på den årlige tilsynsrapport fra FM's DEP. Dette gælder for de arealer i tilsynsoversigten, som er omfattet af FM's tilsyn. Som tidligere klarlagt varierer omfanget af tilsynet i forhold til driftsmodellerne.

For de områder i tilsynsoversigten, som er omfattet af FM's tilsyn, skal den enkelte institution således alene årligt læse tilsynsrapporten fra FM og vurdere relevansen af de eventuelle risici, som er fremhævet heri. Tilsynsrapporten fra FM kan give anledning til justeringer af risikovurderingen, når den årlige revurdering foretages.

Information om risici, der ikke håndteres af SIT

Alle institutioner, som er kunder hos Statens It, kan henvende sig til FM's DEP omkring kritiske forhold, som de ikke finder, er tilstrækkeligt håndteret af SIT. Kontakten kan ske telefonisk eller ved mail til tilsynskontoret. Dette kan være tilfældet, hvis fx institutionen 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, men orientering af tilsynet bør ske i de situationer, hvor SIT ikke håndterer risikoen.

FM orienterer i den årlige tilsynsrapport til SIT's kunder om de indkomne henvendelser, og hvad der er foretaget i den forbindelse.

---

[24] Elektronisk sags- og dokumenthåndteringssystem (ESDH)

4. Bilag til vejledningen

De anvendte cases skal ses som inspiration til risikovurderinger og en illustration af systematikken. Det er således ikke udtryk for et fuldstændigt billede af de vurderede risici for de pågældende systemer. Fx kan der i casen være beskrevet 3 trusler, men hvor den virkelige risikovurdering ville omfatte beskrivelse af 10 trusler, såfremt disse var vurderet relevante. Casebeskrivelserne tager udgangspunkt i konkrete systemer, men det kan forekomme, at vi har tilføjet eller overdrevet risikoelementer m.v. for at synliggøre en problemstilling.

For institutionens egne risikovurderinger kan man med fordel behandle alle relevante lag i teknologistakken jf. Tilsynsoversigten. Hvis man eksempelvis vurderer, at fortrolighed er meget vigtigt for sit system, og at man derfor vil have særlig kontroller omkring logning eller adgangskontrol, bør man vurdere betydningen for alle lag i teknologistakken (applikationen, databasen, operativsystem, serverne, netværk og den fysiske lokation).

Til sidst i hver case er forsøgt fremhævet, hvilket ansvar og hvilken opgave der påhviler kunden i forhold til at følge op og føre tilsyn med SIT's håndtering af systemet.

Casesamlingen indeholder følgende cases, som dækker flere driftsmodeller i SIT:

- Casebeskrivelse driftsmodel 1 – Exchange
- Casebeskrivelse driftsmodel 1A – ESDH-system
- Casebeskrivelse driftsmodel 2A – Skibsregistret (Martha 1)
- Casebeskrivelse driftsmodel 5 – Det fælles datagrundlag (DFDG)

Bilag 4.1 Casebeskrivelse driftsmodel 1 – Exchange

Hvad skal vi beskytte? (System)

System – Stamdata	
Systemnavn	Centralt e-mail-system (Exchange)
Serveroperativsystem for applikationsserver	Ukendt (fælles applikations og DBMS-server)
Database Management System (DBMS)	Exchange
Serveroperativsystem for DBMS	Ukendt (fælles applikations og DBMS-server)

System – Anvendelse	
Hvad anvendes systemet til?	E-mail kommunikation mellem medarbejdere, institutioner, borgere m.fl.
Kan systemet anvendes til formål der kan have værdi for kriminelle? Kan systemet anvendes til udbetalinger? Kan systemet anvendes til at autorisere noget?	E-mail må antages at kunne indeholde alle typer af data, herunder fortrolige data og data omfattet af GDPR. E-mail anvendes mange steder som led i forretningsgange og kan i den forbindelse autorisere en handling gennem "tillid" til afsenderen. Eksempler herpå er bestilling eller godkendelse af en transaktion.
Hvilke data indeholder systemet?	E-mail må antages at kunne indeholde alle typer af data, herunder fortrolige data og data omfattet af GDPR.
Har data værdi udenfor Staten? Kan data fx stjæles og sælges?	E-mail må antages at kunne indeholde alle typer af data, herunder fortrolige data og data omfattet af GDPR. E-mail bør ikke (må ikke?) anvendes til arkivering / journalisering, hvorfor data i E-mail typisk er aktuelle data, som kan have værdi for f.eks. journalister.
Er data omfattet af lovgivning – fx GDPR?	E-mail må antages at kunne indeholde alle typer af data, herunder fortrolige data og data omfattet af GDPR.

System – Driftsmodel

Hvilken driftsmodel er systemet omfattet af?	Exchange driftes som et fælles system af Statens It og omfatter som udgangspunkt alle kunder. Exchange er således omfattet af driftsmodel 1.
For andre driftsmodeller end 1 og 1A, hvem løser opgaven? Ingen, egen it-funktion, eksterne konsulenter, outsourcing.	Ikke relevant

System – Hvad skal vi beskytte imod? (Truslerne)

Hvad er de 3 mest væsentlige trusler mod systemet?	
1. Hackere	Hackere er en konstant trussel mod Exchange, typisk i form af spam og fremsendelse af ondsindede programmer, ondsindede links m.v. Resultatet er typisk tab af data (fortrolighed) og tillid til systemet (integritet), men denne type hackerangreb kan også have konsekvenser for det øvrige it-miljø.
2. Insidere	Insidere i form af medarbejdere eller eksterne konsulenter kan sælge data, som måtte være tilgængelige (enten frit tilgængelige eller tilgængelige efter en eller anden form for hacker aktivitet). Insidere kan måske omgå godkendelsesprocedurer og derigennem skaffe sig fordele.
3. Fejl og mangler i driften af systemet hos SIT	Driften af Exchange hos Statens It udgør en trussel mod systemet. Det kan både være introduktion af fejl i form af miskonfigurationer, men også manglende rettidig omhu i forbindelse med patchning af systemet. Fejl og mangler kan skyldes både manglende kompetence, og bevidste eller ubevidste fejl.

Hvilke sårbarheder har vi? (Kendte og ukendte)

Sårbarheder – Kendte	
Noter 3 kendte sårbarheder i systemet	
1. Fejlkonfigurationer	Det er muligt at konfigurere Exchange således, at det kan få betydning for anvendelsen af systemet, f.eks. således at den enkelte bruger kan få adgang til oplysninger, som ikke var tilsigtet. Fejlkonfigurationer kan udføres af Statens It eller eksterne konsulenter.
2. Fremsendelse af ondsindede e-mails	Det er altid muligt at fremsende e-mails med ondsindet indhold eller spam.
3. Ikke godkendt anvendelse	Exchange kan anvendes til formål, som ikke er godkendte (f.eks. arkivering / journalisering), og som derved kan øge konsekvenserne ved et sikkerhedsbrud.
Sårbarheder – Ukendte	
Hvilke sårbarheder kan vi forestille os systemet indeholder, men som ikke er kommet frem endnu? Fx hackere bliver endnu bedre til at snyde vores brugere. Fx vi har ikke budget til at holde systemet ajour, det er fint nu, men om 5 år kan det være et problem.	Ukendte svagheder i Exchange eller omkringliggende operativsystemer er svagheder, som endnu ikke er identificeret, typisk programfejl. Exchange har historisk set haft sikkerhedshuller.

Hvilke konsekvenser kan det få, hvis en trussel udnytter en sårbarhed i systemet?

Marker med høj / middel / lav		
Fortrolighed	Tab af fortrolighed for data (e-mails) i Exchange kan have alvorlige konsekvenser, også for Ministeren. Vi vurderer derfor konsekvens ved tab af fortrolighed som ”høj”.	Høj
Integritet	Tab af integriteten i Exchange således at brugeren ikke kan have tillid til, at afsenderen er den, vedkommende udgiver sig for at være, eller at indholdet af en e-mail er manipuleret, vil have store konsekvenser. Vi vurderer derfor konsekvensen ved tab af integritet som ”høj”.	Høj
Specifikt vurder sporbarhed	Tab af integriteten i Exchange således at brugeren ikke kan have tillid til, at afsenderen er den vedkommende udgiver sig for at være, vil have store konsekvenser. Vi vurderer derfor konsekvensen ved tab af sporbarhed som ”høj”.	Høj
Tilgængelighed	Selv om manglende tilgængelighed til Exchange vil være vil til stor gene, eksisterer der mange alternative kommunikationsformer, der kan tages i anvendelse. Vi vurderer derfor konsekvensen ved tab af tilgængelighed som ”middel”.	Middel

Hvad er sandsynligheden for, at en trussel udnytter en sårbarhed i systemet?

For hver trussel fra tidligere vurder høj / middel / lav sandsynlighed		
1. Hackere	Sandsynligheden for at hackere vil angribe Staten gennem Statens It, er meget høj. På trods af implementerede sikkerhedsforanstaltninger (spamfilter, antivirusprogrammer, firewall m.fl.) vurderer vi sandsynligheden for, at en hacker udnytter en sårbarhed i systemet som ”høj”.	Høj
2. Insidere	Mange succesfulde angreb er udført af Insidere. I Staten er der kun få fortilfælde hvor Insidere har hacket systemer eller lækket fortrolige oplysninger. Vi vurderer derfor sandsynligheden for, at en Insider udnytter en sårbarhed i systemet som ”middel”.	Middel
3. Fejl og mangler i driften	I Staten er der kun få fortilfælde, hvor fejl og mangler i driften har lækket fortrolige oplysninger eller forhindret adgang til Exchange. Vi vurderer derfor sandsynligheden for, at fejl og mangler i driften lækker fortrolige oplysninger eller forhindret adgang til Exchange som ”lav”.	Lav

Hvad er den samlede vurdering af systemet?

Benyt fx OWASP Risk Rating Methodology

Overall Risk Severity = Likelihood x Impact				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
		Likelihood		

Vurdering	Den samlede konsekvens (impact) vurderes som "høj" og den samlede sandsynlighed (likelihood) som "middel", hvorfor den samlede vurdering af systemet er "høj".
Hvilke særlige sikkerhedsforanstaltninger giver ovenstående (hele analysen) anledning til?	
1. Hackerangreb	Den bedste beskyttelse mod hackerangreb mod Exchange er en god perimeterbeskyttelse (spamfilter, antivirusprogrammer, firewall m.fl.), kombineret med awareness.
2. Insider	Den bedste beskyttelse mod angreb fra Insidere mod Exchange er logning og loggennemgang. Vi er usikre på hvilken logning Exchange stiller til rådighed.
3. Sårbarhedsstyring (patchning)	Den bedste beskyttelse mod ukendte sårbarheder er en systematisk sårbarhedsstyring i Exchange og det omkringliggende miljø.
4. Ændringsstyring (Change Management)	Den bedste beskyttelse mod introduktion af fejl og mangler i driften er en systematisk ændringsstyring i Statens It omfattende Exchange og det omkringliggende miljø.
5. Korrekt brug af Exchange	Forudsætning for korrekt brug af Exchange er, at den enkelte bruger ved, hvad Exchange må anvendes til, og hvad Exchange ikke må anvendes til. En politik for anvendelse af Exchange bør være tilgængelig, sikkert på Ministerområdeniveau.

Vurder systemet mod eksisterende sikkerhedsforanstaltninger
(med fokus på de særlige sikkerhedsforanstaltninger identificeret ovenfor)

For de områder vi ikke har beskrevet i risikovurderingen, vurderer vi, at et standard sikkerhedsniveau er tilstrækkeligt.

Med behørig hensyntagen til den driftsmodel, som systemet driftes under (anvend fx Tilsynsoversigten), vurderes følgende:

Sikkerhedsniveauet hos SIT Er sikkerhedsniveauet hos SIT, som beskrevet i SIT's varedeklaration, tilstrækkeligt til systemet?	Vores vurdering er, at perimetersikringen hos Statens It er tilstrækkelig til opfyldelse af krav for sikring af Exchange som identificeret i nærværende risikovurdering.
Tilkøbte særlige sikkerhedsforanstaltninger Er eventuelt tilkøbte særlige sikkerhedsforanstaltninger hos SIT tilstrækkelige til systemet?	Ikke relevant, da vi ikke har tilkøbt særlige sikkerhedsforanstaltninger for Exchange.
Egne sikkerhedsforanstaltninger Er institutionens egne sikkerhedsforanstaltninger tilstrækkelige til systemet?	Ikke relevant, da vi ikke har implementeret egne sikkerhedsforanstaltninger for Exchange.
FM's seneste tilsynsrapport Giver FM's seneste tilsynsrapport grund til handlinger fx i form af kompenserende kontroller?	For Exchange giver FM's seneste tilsynsrapport ikke anledning til yderligere handlinger.
Revisorerklæring Giver revisorerklæring for systemet eller hosting leverandøren (ikke SIT) grund til handlinger fx i form af kompenserende kontroller?	Ikke relevant for Exchange, som bliver hostet hos SIT under driftsmodel 1.
SIT's årlige sikkerhedsaudit af eksterne leverandører Giver SIT's årlige sikkerhedsaudit af eksterne leverandører grund til handlinger fx i form af kompenserende kontroller?	Ikke relevant for Exchange, som bliver hostet hos SIT under driftsmodel 1.
Relevante kundefora Har oplysninger givet under relevante kundefora hos SIT givet grund til handlinger fx i form af kompenserende kontroller?	Ikke relevant for Exchange, som bliver hostet hos SIT under driftsmodel 1.

Nye kontroller

Hvilke kontroller skal udbygges og til hvilket niveau?	Vores vurdering er, at perimetersikringen hos Statens It er tilstrækkelig til opfyldelse af krav for sikring af Exchange, som identificeret i nærværende risikovurdering.
Hvilke ny kontroller skal tilføjes?	Vores vurdering er, at perimetersikringen hos Statens It er tilstrækkelig til opfyldelse af krav for sikring af Exchange, som identificeret i nærværende risikovurdering. I det omfang det ikke allerede er defineret, bør hvert Ministerområde udarbejde en politik for korrekt anvendelse af Exchange, en sådan politik bør tage højde for GDPR. Awareness kampagner bør efterfølgende tages i anvendelse.

FM-DEP's (egne) tilsynsaktiviteter

FM DEP's egne tilsynsaktiviteter bør således omfatte:

- Foretage risikovurdering af systemet. Risikovurderingen skal bl.a. tage udgangspunkt i følgende forhold.
  - Såfremt institutionen har tilkøbt særlige sikkerhedsforanstaltninger, skal institutionen føre tilsyn med, at disse er effektive. Dette sker gennem kontrol af den aftalte rapportering[25].
  - Forholde sig til FM's tilsynsrapport med fokus på, om kritiske forhold har relevans for systemet.
  - Deltage i relevante kundefora, som SIT stiller til rådighed.

- Systematisk dokumentere at have gennemført ovenstående punkter.

[25] Se afsnittet "Rapportering" for yderligere beskrivelse af afrapportering på særlige sikkerhedsforanstaltninger.

Bilag 4.2 Casebeskrivelse driftsmodel 1A – ESDH-system

Hvad skal vi beskytte? (System)

System – Stamdata	
Systemnavn	Public 360, version SP8 – update 3
Virtuel Platform	VmWare ver. 5,5 – 6
Serveroperativsystem	Microsoft Server 2012R2
Database server	Microsoft SQL Server 2014
Database Management System (DBMS)	Microsoft SQL Server 2014 Management Studio
Application server	Microsoft SharePoint Foundation 2013
Backup system	Symantec Netbackup
Application	Tieto Public360 ver. 4.1 SP8 UPD3

System – Anvendelse

Hvad anvendes systemet til?	Registrering af sager (inkl. personalesager) og dokumenter, herunder forelæggelser for departementschef og minister.
Kan systemet anvendes til formål der kan have værdi for kriminelle? Kan systemet anvendes til udbetalinger? Kan systemet anvendes til at autorisere noget?	Dokumenter i systemet indeholder bl.a. cpr.nr., da det bruges til behandling af personalesager. Endvidere indeholder systemet fortrolige data, som kan have værdi for kriminelle. Nej - systemet kan ikke anvendes til udbetalinger eller til at autorisere noget.
Hvilke data indeholder systemet?	Indeholder data, som kan dokumentere ministerens og ministeriets arbejde, herunder fortrolige data og data omfattet af GDPR, da systemet også bruges til bl.a. behandlingen af personalesager.
Har data værdi udenfor Staten? – Kan data fx stjæles og sælges?	Ja – data kan have værdi uden for staten og vil derfor have værdi at stjæle og sælge.
Er data omfattet af lovgivning – fx GDPR?	Da systemet bruges til behandling af fx personalesager er data omfattet af GDPR.

System – Driftsmodel

Hvilken driftsmodel er systemet omfattet af?	Public 360 er omfattet af driftsmodel 1a
For andre driftsmodeller end 1 og 1A, hvem løser opgaven? Ingen, egen it-funktion, eksterne konsulenter, outsourcing.	Ikke relevant

System – Hvad skal vi beskytte imod? (Truslerne)

Hvad er de 3 mest væsentlige trusler mod systemet?	
1. Hackere	Hvis systemets integritet bliver kompromitteret af hackere.
2. Insidere	Manglende mulighed for retablering. Hvis det ved systemnedbrud ikke er muligt at reetablere adgang til data i Public 360.
3. Misbrug af adgang og data	Hvis systemets integritet bliver kompromitteret ved datalæk af insidere fx konsulenter, systemteknikere el. lign.

Hvilke sårbarheder har vi? (Kendte og ukendte)

Sårbarheder – Kendte	
Noter 3 kendte sårbarheder i systemet	
1. Systematisk gennemgang af log	Der er ikke systematisk gennemgang af log på brugerniveau med henblik på evt. misbrug af data. Der er ikke i ministeriet en forhistorie for misbrug af systemadgang, og det vurderes, at ressourceforbruget ved systematisk gennemgang af log ikke står mål med indsatsen, jf. sikkerhed i balance, beskrevet i "National strategi for cyber- og informationssikkerhed. Samtidig beskyttes særlig fortroligt materiale af chefgodkendte begrænsede adgangsgrupper.
2. Hackerangreb	Uautoriseret adgang til systemet via fx et hackerangreb.
Sårbarheder – Ukendte	
Hvilke sårbarheder kan vi forestille os systemet indeholder, men som ikke er kommet frem endnu? Fx hackere bliver endnu bedre til at snyde vores brugere. Fx vi har ikke budget til at holde systemet ajour, det er fint nu, men om 5 år kan det være et problem.	Hvis en hacker overtager en brugers systemadgang, så kan systemets integritet blive kompromitteret eller hvis andre svagheder i it-infrastrukturen kan give adgang til systemet.

Hvilke konsekvenser kan det få, hvis en trussel udnytter en sårbarhed i systemet?

Marker med høj / middel / lav		
Fortrolighed	Tab af fortrolighed for data i Public 360 kan have alvorlige konsekvenser for ministeriet. Vi vurderer derfor konsekvens ved tab af fortrolighed som ”høj”.	Høj
Integritet	Tab af integritet i Public 360 vil have stor betydning for ministeriet, ministeriets samarbejdspartnere og borgerne. Vi vurderer derfor konsekvens ved tab af integritet som ”høj”.	Høj
Specifikt vurder sporbarhed	Høj, jf. ovenstående.	Høj
Tilgængelighed	Tab af tilgængelighed for data i Public 360 kan have store konsekvenser for ministeriet, da det dokumenterer ministeriets arbejde og betjening af folketinget, herunder lovgivningsprocessen. Der vil i en kortere periode kunne findes alternative arbejdsmetoder, men data vil ikke kunne være utilgængeligt over en længere periode. Vi vurderer derfor konsekvens ved tab af tilgængelighed som ”høj”.	Høj

Hvad er sandsynligheden for, at en trussel udnytter en sårbarhed i systemet?

For hver trussel fra tidligere vurder høj / middel / lav sandsynlighed		
1. Hackere	Hvis systemets integritet bliver kompromitteret af eksterne parter eller hackere. Vi vurderer sandsynligheden som ”lav”, da vi ikke mener, vores system er mere udsat en andre systemer af denne karakter i staten.	Lav
2. Manglende mulighed for reetablering	Hvis det ved systemnedbrud ikke er muligt at reetablere adgangen til data. Vi vurderer sandsynligheden som ”lav”, da systemet PRE-PROD og PROD miljø ligger i to forskellige datacentre hos SIT, og vi en gang årligt får udført en disaster recovery for at teste, at systemet kan reetableres.	Lav
3. Misbrug af adgang og data	Hvis systemets integritet bliver kompromitteret ved datalæk af insidere fx konsulenter, systemteknikere el. lign. Vi vurderer sandsynligheden som ”lav”, da vi ikke historisk set har været ramt af denne type af angreb.	Lav

Hvad er den samlede vurdering af systemet?

Benyt fx OWASP Risk Rating Methodology

Overall Risk Severity = Likelihood x Impact				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
		Likelihood		

Vurdering	Den samlede konsekvens (impact) vurderes som ”høj” og den samlede sandsynlighed (likelihood) er ”lav”, hvor den samlede vurdering af systemet er ”medium”.
Hvilke særlige sikkerhedsforanstaltninger giver ovenstående (hele analysen) anledning til?	
1. Kvalitetssikring af data	Sikring af datakvalitet og håndteringen af data. Ved systematisk gennemgang af datakvalitet og øget opmærksomhed på brugernes adfærd højnes sikkerheden og kvaliteten for data i systemet.
2. Brugeradfærd	Brugeradfærd sikres bl.a. gennem uddannelse og brugervejledning, hvilket bidrager til en øget forståelse for, hvordan data skal håndteres, behandles og beskyttes – herunder oplysninger omfattet af GDPR eller som en del af ministeriets lovgivningsproces.
3. Leverandørstyring	Gennem tilsyn med leverandører skal det sikres, at systemet patches og at kendte sårbarheder håndteres.
4. Ændringsstyring	Gennem FM’s tilsyn og det forhold at Statens It er en ISO-certificeret it-driftsleverandør sikres det, at der følges en systematisk change management proces.

Vurder systemet mod eksisterende sikkerhedsforanstaltninger
(med fokus på de særlige sikkerhedsforanstaltninger identificeret ovenfor)

For de områder vi ikke har beskrevet i risikovurderingen, vurderer vi, at et standard sikkerhedsniveau er tilstrækkeligt.

Med behørig hensyntagen til den driftsmodel systemet driftes under (anvend fx Tilsynsoversigten), vurderes følgende:

Sikkerhedsniveauet hos SIT Er sikkerhedsniveauet hos SIT, som beskrevet i SIT's varedeklaration, tilstrækkeligt til systemet?	Vores vurdering er, at standardsikkerhedsniveauet hos Statens It er tilstrækkelig til opfyldelse af krav for sikring af Public 360, som identificeret i nærværende risikovurdering.
Tilkøbte særlige sikkerhedsforanstaltninger Er eventuelt tilkøbte særlige sikkerhedsforanstaltninger hos SIT tilstrækkelige til systemet?	Vi har tilkøbt disaster recovery og vurderer, at den lige p.t. er et tilstrækkeligt tilkøb af særlig sikkerhedsforanstaltning.
Egne sikkerhedsforanstaltninger Er Institutionens egne sikkerhedsforanstaltninger tilstrækkelige til systemet?	Ikke relevant, da vi ikke har implementeret egne sikkerhedsforanstaltninger for Public 360.
FM's seneste tilsynsrapport Giver FM's seneste tilsynsrapport grund til handlinger fx i form af kompenserende kontroller?	For Public 360 giver FM's seneste tilsynsrapport ikke anledning til yderligere handlinger.
Revisorerklæring Giver revisorerklæring for systemet eller hosting leverandøren (ikke SIT) grund til handlinger fx i form af kompenserende kontroller?	Ikke relevant for Public 360, som bliver hostet hos SIT under driftsmodel 1a.
SIT's årlige sikkerhedsaudit af eksterne leverandører Giver SIT's årlige sikkerhedsaudit af eksterne leverandører grund til handlinger fx i form af kompenserende kontroller?	Ikke relevant for Public 360, som bliver hostet hos SIT under driftsmodel 1a.
Relevante kundefora Har oplysninger givet under relevante kundefora hos SIT givet grund til handlinger fx i form af kompenserende kontroller?	Nej

Nye kontroller

Hvilke kontroller skal udbygges og til hvilket niveau?	Udførelse af disaster recovery.
Hvilke ny kontroller skal tilføjes?	EM skal have tilføjet en kontrol på bestilling, gennemførelse og test af den årlige disaster recovery.

EM's egne tilsynsaktiviteter

- Foretage risikovurdering af systemet. Risikovurderingen skal bl.a. tage udgangspunkt i følgende forhold.
  - Foretage tilsyn med applikationslaget, hvilket typisk omfatter de områder fra ISO 27001, som er listet i tilsynsoversigten.

    - Da institutionen har identificeret behov for at tilkøbe særlig sikkerhedsforanstaltning, skal institutionen føre tilsyn med, at denne er effektiv. Dette sker gennem kontrol af den aftalte rapportering[26].
    - Forholde sig til FM's tilsynsrapport med fokus på, om kritiske forhold har relevans for systemet.
    - Deltage i relevante kundefora, som SIT stiller til rådighed.
- Systematisk dokumentere at have gennemført ovenstående punkter.

[26] Se afsnittet "Rapportering" for yderligere beskrivelse af afrapportering på særlige sikkerhedsforanstaltninger.

Bilag 4.3 Casebeskrivelse driftsmodel 2A – Skibsregister (Martha 1)

Hvad skal vi beskytte? (System)

System – Stamdata	
Systemnavn	Skibsregister (Martha 1)
Serveroperativsystem for applikationsserver	Microsoft Windows Server 2012 (64-bit)
Database Management System (DBMS)	Oracle
Serveroperativsystem for DBMS:	Microsoft Windows Server 2012 (64-bit)

System – Anvendelse

Hvad anvendes systemet til?	Registrering af skibe
Kan systemet anvendes til formål der kan have værdi for kriminelle? Kan systemet anvendes til udbetalinger? Kan systemet anvendes til at autorisere noget?	NEJ, NEJ, NEJ
Hvilke data indeholder systemet?	Skibsregistrering, herunder ejerskab og fx pantretigheder. Der er ingen fortrolige oplysninger i systemet. Alle registreringer og de underliggende dokumenter er offentligt tilgængelige. Det svarer til, hvad der gælder for tinglysning og tinglyste dokumenter.
Har data værdi udenfor Staten? – Kan data fx stjæles og sælges?	Nej
Er data omfattet af lovgivning – fx GDPR?	Ja – Søloven

System – Driftsmodel

Hvilken driftsmodel er systemet omfattet af?	2A
For andre driftsmodeller end 1 og 1A, hvem løser opgaven? Ingen, egen it-funktion, eksterne konsulenter, outsourcing.	Visma Consulting A/S (IT udvikling & Application Management)

System – Hvad skal vi beskytte imod? (Truslerne)

Hvad er de 3 mest væsentlige trusler mod systemet?	
1. Hackere	Hvis systemets integritet bliver kompromitteret
2. Insidere	Applikationsnedbrud (Fagsystem & Database)
3. SIT	Generelt systemnedbrud ved Statens-It

Hvilke sårbarheder har vi? (Kendte og ukendte)

Sårbarheder – Kendte	
Noter 3 kendte sårbarheder i systemet	
1. Forældet teknologi	Martha 1 er baseret på en forældet teknologi, der kræver specialviden i forbindelse med applikation management og udvikling.
2. Datamigrering	Migrering af data. Gennem Søfartsstyrelsens migrerings-projekter løftes data trinvis fra Martha 1 til Martha 2. Den-ne migreringsproces sikrer, at Martha 1 med tiden kan udfases samt, at data gennem fx ”datavask” bliver valide-ret og bedre struktureret i CRM (Martha 2). Der kan være en lille risiko for, at ”ikke-struktureret” historiske data bliver ”glemt” i Martha 1 i forbindelse med migreringen.
3. Utilgængelig datastruktur	Datastruktur i Martha 1 er uklar og svært tilgængelig.
Sårbarheder – Ukendte	
Hvilke sårbarheder kan vi forestille os sy-stemet indeholder men som ikke er kommet frem endnu? Fx hackere bliver endnu bedre til at snyde vores brugere. Fx vi har ikke budget til at holde systemet ajour, det er fint nu men om 5 år kan det være et problem.	Martha 1 er et ældre fagsystem, der på sigt kan blive vanskeligt at supportere pga. manglende kendskab til fx forældet kodesprog.

Hvilke konsekvenser kan det få, hvis en trussel udnytter en sårbarhed i systemet?

Marker med høj / middel / lav	
Fortrolighed	Lav
Integritet	Lav
Specifikt vurder sporbarhed	Lav
Tilgængelighed	Lav

Hvad er sandsynligheden for, at en trussel udnytter en sårbarhed i systemet?

For hver trussel fra tidligere vurder høj / middel / lav sandsynlighed		
1. Hackere	Systemets integritet bliver kompromitteret	Lav
2. Insidere	Applikationsnedbrud (Fagsystem & Database)	Middel
3. SIT	Generelt systemnedbrud ved Statens-It	Lav

Hvad er den samlede vurdering af systemet?

Benyt fx OWASP Risk Rating Methodology

Overall Risk Severity = Likelihood x Impact				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
		Likelihood		

Vurdering	Den samlede konsekvens (impact) vurderes som ”lav” og den samlede sandsynlighed (likelihood) er ”lav” til ”middel”, hvor den samlede vurdering af systemet er ”lav”. Martha 1 systemet er i 2016 blevet migreret fra en gammel ikke supporteret Windows NT 4 platform til en fuldt ud supporteret Windows Server 2012 platform. Martha 1 er således i dag placeret på servere der løbende sikkerhedspatches med opdateringer og antivirus. Martha 1 er dog stadigvæk en gammel applikation, der forventes udfaset i takt med at data migreres til CRM (Martha 2) og et nyt fuldt digitaliseret skibsregister indfases. Risikovurdering for Martha 1 er tilfredsstillende.
Hvilke særlige sikkerhedsforanstaltninger giver ovenstående (hele analysen) anledning til?	
1. **12.3 Backup**	Denne kontrol anvendes, fordi Søfartsstyrelsen ønsker at sikre regelmæssig backupkopier og genskabelsesprocedure, der holdes i live, og løbende opdateres. På den måde er Søfartsstyrelsen altid i kontrol over at opbevaring, backupfrekvens og restore processen effektiveres i organisationen.
2. **12.4 Logning og overvågning**	Denne kontrol anvendes, fordi Søfartsstyrelsen ønsker at sikre etablering af hændelseslogning til registrering af brugeraktivitet, der holdes i live, og løbende opdateres. På denne måde er Søfartsstyrelsen altid i kontrol over hvilke hændelser, brugeraktiviteten har udført i organisationen.
3. **12.5 Styring af driftssoftware**	Denne kontrol anvendes, fordi Søfartsstyrelsen ønsker at sikre opdatering og styring af software udføres af autoriseret administratorer. På denne måde er Søfartsstyrelsen altid i kontrol over, hvilke software der er installeret på Martha 1
4. **12.6 Sårbarhedsstyring**	Denne kontrol anvendes, fordi Søfartsstyrelsen ønsker at sikre opdatering og styring af eventuelle tekniske sårbarheder i vores informationssystemer.

Vurder systemet mod eksisterende sikkerhedsforanstaltninger
(med fokus på de særlige sikkerhedsforanstaltninger identificeret ovenfor)

For de områder vi ikke har beskrevet i risikovurderingen, vurderer vi, at et standard sikkerhedsniveau er tilstrækkeligt.

Med behørig hensyntagen til den driftsmodel systemet driftes under (anvend fx Tilsynsoversigten), vurderes følgende:

Sikkerhedsniveauet hos SIT Er sikkerhedsniveauet hos SIT, som beskrevet i SIT's varedeklaration, tilstrækkeligt til systemet?	12.3 Backup: Test af restore, således at fx Recovery Time Objective kan fastlægges, bør udføres mindst 2 gange om året på udvalgte systemer.
Tilkøbte særlige sikkerhedsforanstaltninger Er eventuelt tilkøbte særlige sikkerhedsforanstaltninger hos SIT tilstrækkelige til systemet?	Ikke vurderet
Egne sikkerhedsforanstaltninger Er institutionens egne sikkerhedsforanstaltninger tilstrækkelige til systemet?	Ikke vurderet
FM's seneste tilsynsrapport Giver FM's seneste tilsynsrapport grund til handlinger fx i form af kompenserende kontroller?	Ikke vurderet
Revisorerklæring Giver revisorerklæring for systemet eller hosting leverandøren (ikke SIT) grund til handlinger fx i form af kompenserende kontroller?	Ikke vurderet
SIT's årlige sikkerhedsaudit af eksterne leverandører Giver SIT's årlige sikkerhedsaudit af eksterne leverandører grund til handlinger fx i form af kompenserende kontroller?	Ikke vurderet
Relevante kundefora Har oplysninger givet under relevante kundefora hos SIT givet grund til handlinger fx i form af kompenserende kontroller?	Ikke vurderet

Nye kontroller

Hvilke kontroller skal udbygges og til hvilket niveau?	12.3 Backup: Test af restore, således at fx Recovery Time Objective kan fastlægges, bør udføres mindst 2 gange om året.
Hvilke ny kontroller skal tilføjes?	Ingen

EM's egne tilsynsaktiviteter

- Foretage risikovurdering af systemet. Risikovurderingen skal bl.a. tage udgangspunkt i følgende forhold.
  - Foretage tilsyn med applikationslaget, hvilket typisk omfatter de områder fra ISO 27001, som er listet i tilsynsoversigten.
  - Foretage tilsyn med middlewarelaget (databaser), hvilket typisk omfatter de områder fra ISO 27001, som er listet i tilsynsoversigten.

    - Såfremt institutionen har tilkøbt særlige sikkerhedsforanstaltninger, skal institutionen føre tilsyn med, at disse er effektive. Dette sker gennem kontrol af den aftalte rapportering[27].
    - Forholde sig til FM's tilsynsrapport med fokus på, om kritiske forhold har relevans for systemet.
    - Deltage i relevante kundefora, som SIT stiller til rådighed.
- Systematisk dokumentere at have gennemført ovenstående punkter.

[27] Se afsnittet "Rapportering" for yderligere beskrivelse af afrapportering på særlige sikkerhedsforanstaltninger.

Bilag 4.4 Casebeskrivelse driftsmodel 5 – Det fælles data grundlag (DFDG)

Hvad skal vi beskytte? (System)

System – Stamdata	
Systemnavn	Det fælles data grundlag (DFDG)
Serveroperativsystem for applikationsserver	Windows 2012
Database Management System (DBMS)	SQL 2016
Serveroperativsystem for DBMS	Windows 2012

System – Anvendelse

Hvad anvendes systemet til?	Opsamling og udveksling af data fra/til Jobnet, Jobcentre og A-kasser. Udvekslingen sker via webservices.
Kan systemet anvendes til formål der kan have værdi for kriminelle? Kan systemet anvendes til udbetalinger? Kan systemet anvendes til at autorisere noget?	Der findes cpr nr. i systemet, derfor et ja.
Hvilke data indeholder systemet?	Persondata. Oplysninger om ledige og beskæftigede i Danmark mellem 15 og 80 år.
Har data værdi udenfor Staten? Kan data fx stjæles og sælges?	Ja
Er data omfattet af lovgivning – fx GDPR?	Ja - beskæftigelseslovgivningen og persondataloven.

System – Driftsmodel

Hvilken driftsmodel er systemet omfattet af?	Model 5
For andre driftsmodeller end 1 og 1A, hvem løser opgaven? Ingen, egen it-funktion, eksterne konsulenter, outsourcing.	Outsourcet til KMD under Statens-It's rammeaftale.

System – Hvad skal vi beskytte imod? (Truslerne)

Hvad er de 3 mest væsentlige trusler mod systemet?	
1. KMD	Drifts nedbrud
2. Insidere	Misbrug af data fra brugere (interne brugere), leverandører, aftagere af data og andre med onde hensigter.
3. Hackere	Ddos og andre former for hackerandgreb.

Hvilke sårbarheder har vi? (Kendte og ukendte)

Sårbarheder – Kendte	
Noter 3 kendte sårbarheder i systemet.	
1. Manglende loggennemgang	Der sker ikke en systematisk gennemgang af loggen. Særligt et problem i forhold til misbrug af data.
2. Manglende test	Manglende eller gennemgribende test (før idriftsættelse af nye releases?). Er de test der gennemføres omfattende nok? Mangel på gennemgribende test kan medfører at alle tre trusler øges.
3. Manglende opfølgning	Manglende opfølgning på sikkerhed, systematiske kampagner (brugerne). I forhold til borgere og sagsbehandlere i forbindelse med misbrug og angreb.
Sårbarheder – Ukendte	
Hvilke sårbarheder kan vi forestille os systemet indeholder men som ikke er kommet frem endnu? Fx hackere bliver endnu bedre til at snyde vores brugere. Fx vi har ikke budget til at holde systemet ajour, det er fint nu men om 5 år kan det være et problem.	
1. Arkitektur	Manglende fokus på it-arkitekturen kan medføre ukendte sårbarheder
2. Gammel kode	DFDG er et meget stort system, som er udviklet gennem mange år og derfor kan gammel kode være et problem.

Hvilke konsekvenser kan det få, hvis en trussel udnytter en sårbarhed i systemet?

Marker med høj / middel / lav		
Fortrolighed	Systemet opsamler og udveksler persondata fra/til Jobnet, Jobcentre og A-kasser, hvilke selvfølgelig skal holdes fortrolige.	Høj
Integritet	Data anvendes bl.a. som baggrund for udbetaling af ydelser, hvorfor integriteten skal være på plads.	Høj
Specifikt vurder sporbarhed	Det er af stor betydning, at man kan se hvor data kommer fra.	Høj
Tilgængelighed	Systemet anvendes bl.a. til borgerbetjening og skal derfor være tilgængeligt når henvendelserne sker.	Høj

Hvad er sandsynligheden for, at en trussel udnytter en sårbarhed i systemet?

For hver trussel fra tidligere vurder høj / middel / lav sandsynlighed		
1. KMD	Driftsnedbrud Systemet er ikke specielt kompliceret at drifte, da det baserer sig på velkendte system-komponenter. Historisk erfaring viser ikke en særlig risiko.	Middel
2. Hackere	Ddos og andre former for hackerangreb Vi vurderer sandsynligheden som ”middel”, da vi ikke mener, at vores system er mere udsat end andre systemer af denne karakter i staten.	Middel
3. Insidere	Misbrug af data – brugere (interne brugere) og leverandører. ”Middel” til ”høj” (vi kan måske ikke følge, hvad der sker bagved linjerne). Vi baserer os bl.a. på verserende sager i dagspressen.	Middel til Høj

Hvad er den samlede vurdering af systemet?

Benyt fx OWASP Risk Rating Methodology

Overall Risk Severity = Likelihood x Impact				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
		Likelihood		

Vurdering	High til Critical Den samlede konsekvens (impact) vurderes som ”høj” og den samlede sandsynlighed (likelihood) som ”middel” til ”høj”, hvorfor den samlede vurdering af systemet er ”high” til ”critical”.
Hvilke særlige sikkerhedsforanstaltninger giver ovenstående (hele analysen) anledning til?	
1. Logopfølgning	Undersøgt mulighederne for opfølgning og kontrol af logs, med henblik på at kunne opdage angreb.
2. Datamisbrug	Ekstra fokus på adgangsstyring herunder awareness.
3. Test	Fokus på test af systemændringer.
4. Sårbarhedsstyring	Sikkerhedspatchning (første beskyttelse mod Hackerangreb).
5. Test	Skærpede procedurer for test af systemændringer, særligt uden for hoved-releases.

Vurder systemet mod eksisterende sikkerhedsforanstaltninger
(med fokus på de særlige sikkerhedsforanstaltninger identificeret ovenfor)

For de områder vi ikke har beskrevet i risikovurderingen, vurderer vi, at et standard sikkerhedsniveau er tilstrækkeligt.

Med behørig hensyntagen til den driftsmodel systemet driftes under (anvend fx Tilsynsover-sigten), vurderes følgende:

Sikkerhedsniveauet hos SIT Er sikkerhedsniveauet hos SIT, som beskrevet i SIT's varedeklaration, tilstrækkeligt til systemet?	DFDG er omfattet af driftsmodel 5, hvilket betyder at SIT kun leverer kommunikation mellem STAR og KMD. For denne ydelse vurderer vi, at et standard sikkerhedsniveau er tilstrækkeligt.
Tilkøbte særlige sikkerhedsforanstaltninger Er eventuelt tilkøbte særlige sikkerhedsforanstaltninger hos SIT tilstrækkelige til systemet?	Ikke relevant, da vi ikke har vurderet behov for tilkøb af særlige sikkerhedsforanstaltninger for DFDG.
Egne sikkerhedsforanstaltninger Er Institutionens egne sikkerhedsforanstaltninger tilstrækkelige til systemet?	Vi har i risikovurderingen identificeret 4 områder, hvor vi vil forbedre eller indføre nye sikkerhedsforanstaltninger.
FM's seneste tilsynsrapport Giver FM's seneste tilsynsrapport grund til handlinger fx i form af kompenserende kontroller?	Vi har gennemgået FM's seneste tilsynsrapport, hvilket ikke har givet anledning til yderligere handlinger.
Revisorerklæring Giver revisorerklæring for systemet eller hosting leverandøren (ikke SIT) grund til handlinger fx i form af kompenserende kontroller?	Vi har gennemgået KMD's seneste revisorerklæring, hvilket ikke har givet anledning til yderligere handlinger.
SIT's årlige sikkerhedsaudit af eksterne leverandører Giver SIT's årlige sikkerhedsaudit af eksterne leverandører grund til handlinger fx i form af kompenserende kontroller?	Vi har gennemgået SIT's seneste rapport/referat af sikkerhedsaudit hos KMD, hvilket ikke har givet anledning til yderligere handlinger.
Relevante kundefora Har oplysninger givet under relevante kundefora hos SIT givet grund til handlinger fx i form af kompenserende kontroller?	Vi har deltaget relevante kundefora, hvilket ikke har givet anledning til yderligere handlinger.

Nye kontroller

Hvilke kontroller skal udbygges og til hvilket niveau?	Ingen
Hvilke ny kontroller skal tilføjes?	**1. Logopfølgning** Undersøge mulighederne for opfølgning og kontrol af logs, med henblik på at kunne opdage angreb. **2. Datamisbrug** Ekstra fokus på adgangsstyring herunder awareness. **3. Test** Fokus på test af systemændringer. **4. Test** Skærpede procedurer for test af systemændringer, særligt uden for hoved-releases.

STAR's egne tilsynsaktiviteter

STAR's egne tilsynsaktiviteter bør således omfatte:

- Foretage detaljeret risikovurdering af systemet, i forbindelse med udbud og kontraktindgåelse.
- Foretage løbende risikovurdering af systemet. Risikovurderingen skal bl.a. tage udgangspunkt i følgende forhold.
  - Såfremt institutionen har tilkøbt særlige sikkerhedsforanstaltninger, skal institutionen føre tilsyn med, at disse er effektive (SIT såvel som den eksterne leverandør). Dette sker gennem kontrol af den aftalte rapportering[28]. I den pågældende case er der dog ikke vurderet behov for særlige sikkerhedsforanstaltninger.
  - Forholde sig til FM's tilsynsrapport med fokus på, om kritiske forhold har relevans for systemet.
  - Indhente revisorerklæringer fra SIT og forholde sig til, om der er forbehold eller supplerende oplysninger, som kræver reaktioner.
  - Rekvirere og forholde sig til SIT's årlige sikkerhedsaudit af eksterne leverandører.
  - Deltage i relevante kundefora, som SIT stiller til rådighed.
- Systematisk dokumentere at have gennemført ovenstående punkter

[28] Se afsnittet "Rapportering" for yderligere beskrivelse af afrapportering på særlige sikkerhedsforanstaltninger.

fm.dk