tet

Tilsynet med Efterretningstjenesterne

Standarder for TETs virksomhed

Kortlægning af it-infrastruktur v. 2.0

Risiko- og væsentlighedsvurdering v. 2.1

Metode, gennemførelse af kontrol og verificering af oplysninger v. 2.0

Standarder for TETs virksomhed

Kortlægning af it-infrastruktur v. 2.0

Risiko- og væsentlighedsvurdering v. 2.1

Metode, gennemførelse af kontrol og verificering af oplysninger v. 2.0

Februar 2024

INDHOLD

APPENDIKS

BILAG

VERSIONER SIDEN OFFENTLIGGØRELSEN AF TETS STANDARDER

Standard for TETs kortlægning af it-infrastruktur

VERSION	OFFENTLIGGJORT	ÆNDRINGER
2.0 (gældende)	19. februar 2024	Gennemgribende opdatering af TETs standard for kortlægning af it-infrastruktur i PET, FE, CFCS og PPNR
1.1	2. juni 2022	Mindre rettelser som konsekvens af årlig opdatering
1.0	24. juni 2021	Oprindelig version

Standard for TETs risiko- og væsentlighedsvurdering

VERSION	OFFENTLIGGJORT	ÆNDRINGER
2.1 (gældende)	19. februar 2024	Mindre rettelser, herunder ved udbygning af grafisk understøttelse, som konsekvens af årlig opdatering
2.0	2. juni 2022	Gennemgribende opdatering af TETs model for risiko- og væsentlighedsvurdering af PET, FE, CFCS og RPNR
1.0	24. juni 2021	Oprindelig version

Standard for TETs metode, gennemførelse af kontrol og verificering af oplysninger

VERSION	OFFENTLIGGJORT	ÆNDRINGER
2.0 (gældende)	19. februar 2024	Gennemgribende opdatering af TETs standard for valg af metode og gennemførelse af kontrol af PET, FE, CFCS og PPNR
1.1	2. juni 2022	Mindre rettelser som konsekvens af årlig opdatering
1.0	24. juni 2021	Oprindelig version

Indledning

TETs kontrol af Politiets Efterretningstjeneste (PET), Forsvarets Efterretningstjeneste (FE), Center for Cybersikkerhed (CFCS) og Politiets PNR-enhed (PPNR) forudsætter kendskab til myndighedernes it-infrastruktur, prioritering af tilsynets ressourcer og effektive metoder til gennemførelse af kontrollen.

TET kan alene kontrollere de dele af PET, FE, CFCS og PPNR, som tilsynet har kendskab til. Endvidere har TET ikke ressourcer til at foretage en fuldstændig kontrol af alle dele af PET, FE, CFCS og PPNR. Endelig skal TETs kontroller kunne dokumentere forholdene i PET, FE, CFCS og PPNR med et begrænset ressourceforbrug.

TETs standarder har til formål at håndtere disse grundlæggende udfordringer. Derfor består TETs arbejde overordnet af tre delelementer:

TETs 1 kortlægning af it-infrastruktur i henholdsvis PET, FE, CFCS og PPNR har til formål at give tilsynet det nødvendige kendskab til tjenesternes, centrets og enhedens tilvejebringelse, behandling og videregivelse af oplysninger.

TET sammenstiller og vurderer informationer om relevante dele af it-infrastrukturen med henblik på at skabe det rette grundlag for at kunne foretage fuldstændige risiko- og væsentlighedsvurderinger af samtlige processer og systemer i tjenesterne, centret og enheden.

TETs metode til kortlægning af it-infrastruktur er egenudviklet. Metoden er en videreudvikling af TETs indledende kortlægning af it-systemer i PET og FE i 2014-2015, som har afstedkommet et behov for både tilpasning, strukturering og formalisering af metode.

Valget af metode afspejler en afvejning mellem behov for teknisk detaljegrad i kortlægningen til at kunne understøtte TETs kontrolvirksomhed, mængden af it-ressourcer og niveauet af modenhed for it-governance i såvel tilsynet som PET, FE, CFCS og PPNR.

Standarden for TETs kortlægning af it-infrastruktur i PET, FE, CFCS og PPNR er nærmere beskrevet i afsnit 1.

TETs 2 planlægning af kontroller for det kommende år har til formål at prioritere tilsynets ressourcer, således at kontrollen rettes mod de dele af PET, FE, CFCS og PPNR, hvor der vurderes at være den største risiko for lovbrud.

Planlægningen sker på baggrund af en årlig risiko- og væsentlighedsvurdering af processer og systemer (herefter kontrolobjekter) i PET, FE, CFCS og PPNR med det formål at vurdere risici for lovbrud ved tjenesternes, centrets og enhedens aktiviteter. TET udarbejder på denne baggrund risikoanalyser, som danner grundlag for udvælgelsen af det kommende års kontroller. De udvalgte kontroller samles i kontrolplaner for PET, FE, CFCS og PPNR for det kommende år.

Formålet med risikoanalyserne er at sikre, at TETs kontrol fokuseres på områder, hvor der er størst risiko for lovbrud, samt at der tages højde for andre relevante faktorer, eksempelvis områder hvor tilsynets kontrol fra lovgivers side er tillagt særlig vægt, såsom reglerne om lovlig politisk virksomhed.

Områder, hvor der vurderes at være en lavere risiko for lovbrud, kontrolleres som hovedregel hvert femte år med henblik på at skabe fuldstændighed i kontrollen af PET, FE, CFCS og PPNR og sikre, at vurderingen af risiko for lovbrud på området fortsat er retvisende.

Standarden for TETs risiko- og væsentlighedsvurdering af PET, FE, CFCS og PPNR er nærmere beskrevet i afsnit 2.

TETs kontroller 3 gennemføres løbende hen over året på baggrund af kontrolplanerne for henholdsvis PET, FE, CFCS og PPNR. TET fastlægger ikke metoder for de enkelte kontroller i forbindelse med udarbejdelsen af risikovurderinger og -analyser, men først efter en forudgående teknisk og juridisk afdækning af det enkelte kontrolobjekt.

TET benytter sig af en række forskellige metoder i kontrollen af de enkelte kontrolobjekter, heriblandt fuldstændig kontrol, tilfældige eller målrettede stikprøver, indholdsscreening, inspektioner samt interview- og høringsbaserede kontroller.

TETs valg af kontrolmetode sker på baggrund af en konkret risikovurdering af kontrolobjektet, erfaringer fra tidligere kontroller samt de faktiske forhold, som tilsynet konstaterer i forbindelse med den specifikke kontrol. I den sammenhæng afholder TET forud for kontrol af ikke tidligere kontrollerede områder et opstartsmøde med relevante medarbejdere i PET, FE, CFCS eller PPNR med henblik på at sikre en tilstrækkelig politi- og/eller efterretningsfaglig samt teknisk og juridisk forståelse af området, således at kontrollen kan tilpasses og gennemføres hensigtsmæssigt.

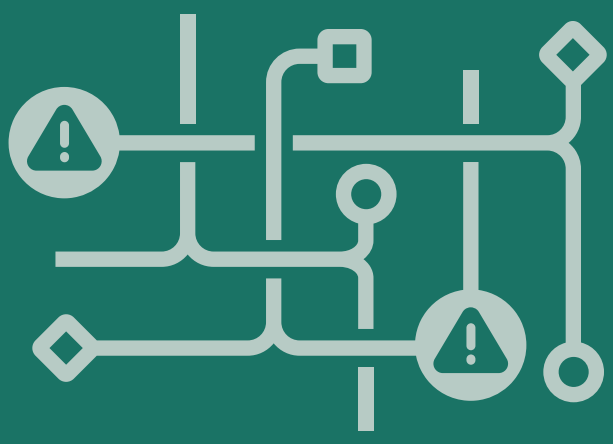
Som en del af TETs gennemførelse af kontroller foretages tillige verificeringskontroller af PETs, FEs, CFCS' og PPNRs it-infrastruktur. Formålet er herved at sikre, at TETs kontrol beror på oplysninger fra PET, FE, CFCS og PPNR, hvis rigtighed tilsynet har efterprøvet.

Standarden for TETs valg af metode, gennemførelse af kontrol og verificering er nærmere beskrevet i afsnit 3.

Processerne for TETs 1 kortlægning, 2 planlægning samt 3 gennemførelse og verificering fremgår af følgende figur. Processerne er understøttet af løbende kvalitetssikring ved godkendelse på henholdsvis chefniveau og tilsynsniveau samt ved høringer af eksterne parter om juridiske, faktuelle eller klassifikationsmæssige forhold.


Se standard for TETs kortlægning af it-infrastruktur (afsnit 1)
Kortlægning af PETs, FEs, CFCS' og PPNRs it-infrastruktur
KVALITETSSIKRING
Ekstern høring om faktuelle forhold
KVALITETSSIKRING
Godkendelse på chefniveau
Se standard for TETs risiko- og væsentlighedsvurdering (afsnit 2)
Risiko- og væsentlighedsvurdering af PET, FE, CFCS og PPNR
KVALITETSSIKRING
Godkendelse på chefniveau
Forelæggelse af risiko- og væsentlighedsvurdering af PET, FE, CFCS og PPNR og beslutning om kontrolplaner for det kommende år
KVALITETSSIKRING
Drøftelse og godkendelse på tilsynsniveau
Se standard for TETs valg af metode, gennemførelse af kontrol og verificering af oplysninger (afsnit 3)
Afklaring af kontroltype for samtlige planlagte kontroller
KVALITETSSIKRING
Godkendelse på chefniveau
Orientering af PET, FE, CFCS og PPNR om TETs kontrolplaner
Teknisk og juridisk afdækning af kontrolobjekter
KVALITETSSIKRING
Ekstern høring om juridiske og faktuelle forhold
Beslutning om metode for de enkelte kontroller
KVALITETSSIKRING
Godkendelse på chefniveau
Gennemførelse af kontroller
KVALITETSSIKRING
Godkendelse på chefniveau
Høring af PET, FE, CFCS eller PPNR i forbindelse med kontroller
KVALITETSSIKRING
Ekstern høring om juridiske og faktuelle forhold
Forelæggelse og afslutning af kontroller
KVALITETSSIKRING
Drøftelse og godkendelse på tilsynsniveau
Fremsendelse af opfølgningsbreve til PET, FE, CFCS eller PPNR
KVALITETSSIKRING
Ekstern kvalitetssikring ved eventuelle bemærkninger vedrørende kontrollen
Udarbejdelse af årlige redegørelser om PET og PPNR, FE samt CFCS
KVALITETSSIKRING
Drøftelse og godkendelse på tilsynsniveau
KVALITETSSIKRING
Ekstern kvalitetssikring ved høring om faktuelle eller klassifikationsmæssige forhold
Offentliggørelse af TETs årlige redegørelser

1 Kortlægning af it-infrastruktur



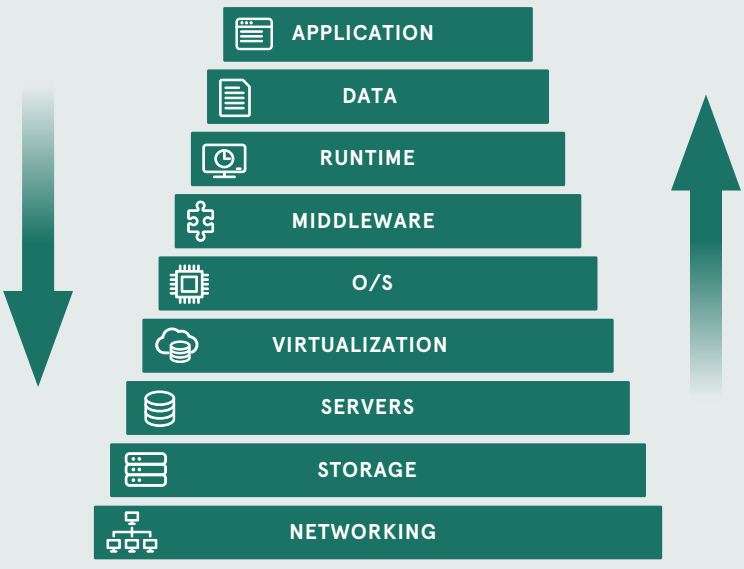
TETs kortlægning af it-infrastruktur i henholdsvis PET, FE, CFCS og PPNR har til formål at sammenstille og vurdere informationer om relevante server-baserede dele af tjenesternes, centrets og enhedens it-infrastruktur. TETs kortlægning bidrager til at skabe det rette grundlag for tilsynets årlige risiko- og væsentlighedsvurderinger, som danner grundlag for beslutning om tilsynets årlige kontrolplaner.

TETs metode til kortlægning af it-infrastruktur er egenudviklet, idet der ikke findes en offentlig standard på kortlægningsområdet med tilsynets specifikke formål. Metoden er en videreudvikling af TETs indledende kortlægning af it-systemer i PET og FE i 2014-2015, som har afstedkommet et behov for både tilpasning, strukturering og formalisering af metode.

Valget af metode afspejler således en afvejning mellem behov for teknisk detaljegrad i kortlægningen til at kunne understøtte TETs kontrolvirksomhed, mængden af it-ressourcer og niveauet af modenhed for it-governance i såvel tilsynet som PET, FE, CFCS og PPNR.

TET er som ekstern myndighed i høj grad afhængig af, hvilke it-værktøjer der i forvejen findes og benyttes i PET, FE, CFCS og PPNR samt typen af de systemadgange, som er til rådighed. TET tilstræber at anvende læseadgang til systemer og data i PET, FE, CFCS og PPNR, men hvor dette ikke lader sig gøre kan det være nødvendigt for tilsynet at benytte privilegerede adgange.

TETs standard for kortlægning af it-infrastruktur tager udgangspunkt i krydsvalidering af komponenter i forskellige niveauer af it-infrastrukturen. TET kortlægger således blandt andet netværk, faciliteter til opbevaring, servere mv. og sammenholder resultatet heraf med applikationsniveauet og tildelte brugerrettigheder. Herved er det muligt for TET at identificere servere eller databaser, som tilsynet endnu ikke har kortlagt eller i øvrigt identificeret. Dette indbefatter også test- og udviklingsmiljøer, som findes i de fleste virksomheder, som bedriver udvikling og/eller drift af egne it-systemer.



TETs metode for kortlægning af it-infrastruktur skal sikre sammenlignelighed – både inden for et givent år og over tid – foruden at vurderingerne skal være reproducerbare. Samtidig skal metoden være dynamisk og mulig at videreudvikle over tid, herunder i forhold til informationer, der efterfølgende måtte inddrages i fremtidige risikovurderinger.

Denne standard indeholder en detaljeret beskrivelse af processen for kortlægningsaktiviteterne og udarbejdelse af TETs interne systemliste samt en metode for analyse og vurdering af de indsamlede data, som resulterer i input til tilsynets årlige risiko- og væsentlighedsvurderinger i form af opdaterede systemlister indeholdende en it-faglig relevansscore.

Samlet består procesdokumentationen for TETs årlige kortlægning af it-infrastruktur i PET, FE, CFCS og PPNR af følgende delprodukter:

- *Procesvejledning* vedrørende TETs kortlægning af it-infrastrukturer i henholdsvis PET, FE, CFCS og PPNR (denne standard).
- Skematisk skabelon for en *infrastrukturoversigt* til indsamling af relevante informationer om it-infrastrukturen i PET, FE, CFCS og PPNR vedrørende alle netværk og idriftsatte servere (se bilag 1).
- Skematisk skabelon for TETs interne *systemliste*, der udarbejdes på baggrund af analyse og vurdering af de indsamlede informationer (se bilag 2).
- *Kontrolnotater* udarbejdet siden sidste opdatering af TETs kortlægning af it-infrastruktur (se bilag 6).

Hensigten med opdeling af TETs kortlægning af it-infrastruktur i ovenstående delprodukter er, at indsamlingen og håndteringen af data af praktiske hensyn håndteres i et regneark, hvor det er nemt at sortere og filtrere data.

Med henblik på at udnytte it-ressourcerne optimalt i såvel TET som PET, FE, CFCS og PPNR, har tilsynet fokus på udelukkende at efterspørge informationer, som finder anvendelse i udarbejdelsen af tilsynets produkter samt at bibeholde en overskuelig datastruktur, som er nem at arbejde med for såvel tilsynet som tjenesterne, centret og enheden.

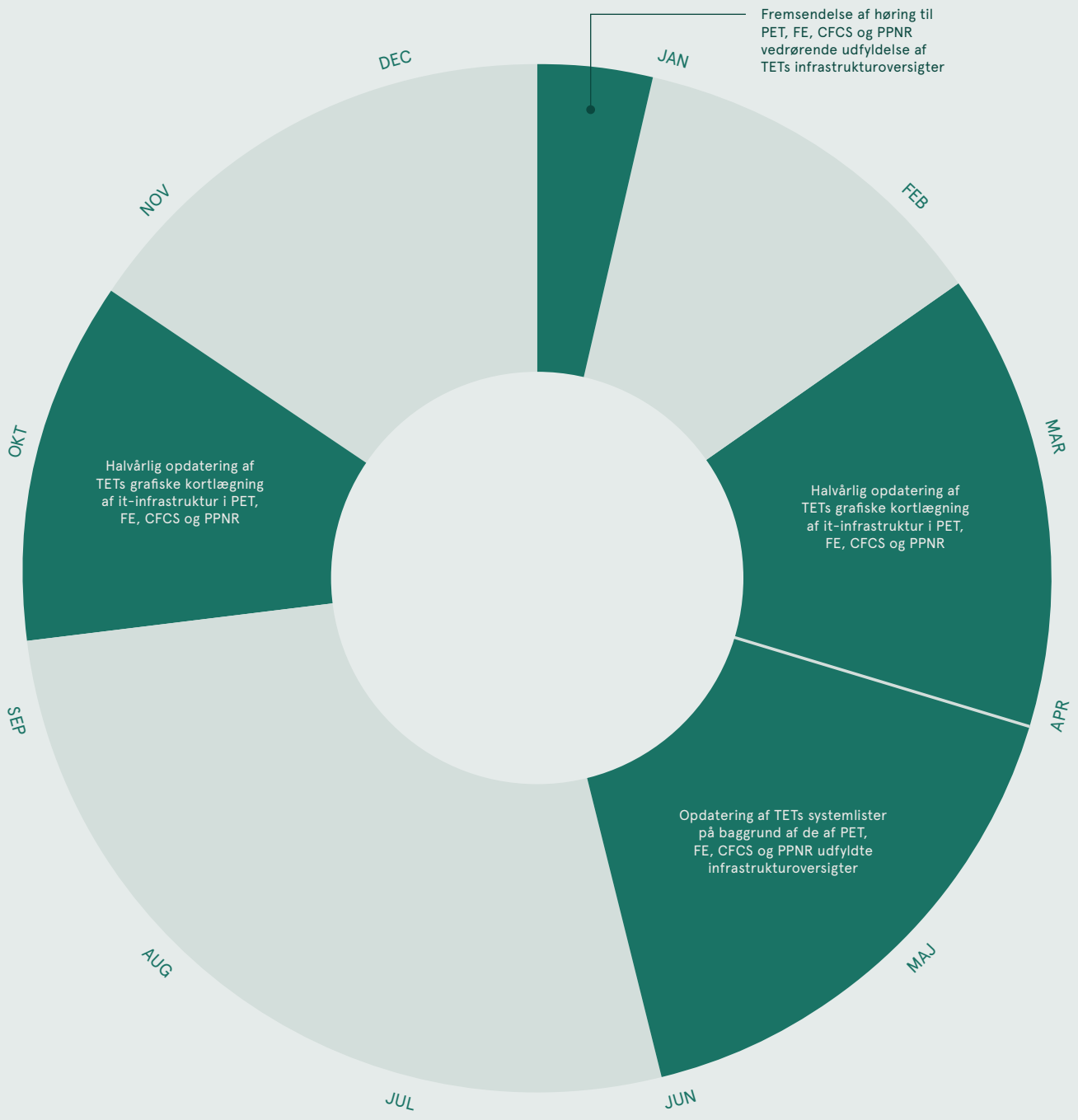
Behovet for information ændrer sig løbende i takt med at TETs kontrolbehov ændrer sig, at tilsynets kendskab til systemer og data forbedres samt at it-systemer, datamængder, værktøjer og anvendte teknologier ændrer sig i PET, FE, CFCS og PPNR.

1.1 Proces for kortlægning af it-infrastruktur

Processen for TETs kortlægning af it-infrastruktur i henholdsvis PET, FE, CFCS og PPNR påbegyndes primo januar ved, at tilsynet anmoder tjenesterne, centret og enheden om relevante informationer. Processen afsluttes i juni med udarbejdelse af input til TETs årlige risiko- og væsentlighedsvurderinger i form opdaterede systemlister over alle eksisterende it-systemer i PET, FE, CFCS og PPNR.

Systemlisterne indeholder en it-faglig vurdering af, hvilke systemer der bør medtages i TETs risiko- og væsentlighedsvurderinger, og sikrer, at nye systemer medtages og udfasede systemer fjernes. Systemlisterne sikrer dermed det nødvendige it-faglige input, så TETs viden vedrørende ændringer i it-infrastrukturen (nye eller ændrede systemers størrelse, antal brugere mv.) kommer til at indgå i tilsynets samlede prioritering af kontroller. Kortlægningsprocessen fordeler sig på året som følger:

Årshjul for TETs kortlægning af it-infrastrukturen



JANUAR: Fremsendelse af høring til PET, FE, CFCS og PPNR indeholdende skabelon for infrastrukturoversigten med anmodning om at indsætte relevante data for samtlige netværk og servere i tjenesterne, centret eller enheden. Efter fremsendelsen af høringerne indgår TET i en dialog med PET, FE, CFCS eller PPNR, såfremt der måtte være spørgsmål til processen eller skabelonernes udformning.

MARTS: På baggrund af kontrolnotater, som TET har udarbejdet i forbindelse med specifikke kontroller i det forgangne halve år, opdateres tilsynets grafiske it-landskaber over it-infrastrukturen i henholdsvis PET, FE, CFCS og PPNR.

APRIL-JUNI: TET modtager høringssvar fra PET, FE, CFCS og PPNR, bearbejder indsamlede data samt opdaterer tilsynets interne systemlister.

OKTOBER: På baggrund af kontrolnotater, som TET har udarbejdet i forbindelse med specifikke kontroller i det forgangne halve år, opdateres tilsynets grafiske it-landskaber over it-infrastrukturen i henholdsvis PET, FE, CFCS og PPNR.

Processen for TETs kortlægning af it-infrastrukturen i henholdsvis PET, FE, CFCS og PPNR følger af årshjulet.

1.2 Udformning og anvendelse af infrastrukturoversigt

TET har valgt at strukturere sine kontroller således, at der inden for et kontrolobjekt tages udgangspunkt i de enkelte it-systemer. Metoden medvirker til at sikre fuldstændighed i TETs kontrol. TETs kortlægning af it-infrastruktur i henholdsvis PET, FE, CFCS og PPNR tager derfor udgangspunkt i de enkelte it-systemer. Sammenhængen mellem forretningsforhold, systemer og arbejdsgange, herunder kortlægning af dataflow, kortlægges efterfølgende i forbindelse med TETs enkelte kontroller (se afsnit 3).

TET har valgt årligt at kortlægge it-infrastrukturen i PET, FE, CFCS og PPNR ved anvendelse af en skabelon, som omfatter det minimum af oplysninger, som tilsynet aktuelt skønner nødvendigt for at opnå et overblik over, hvad der aktuelt findes af netværk og domæner samt hvilke it-systemer, der findes på disse. Skabelonen indeholder tillige oplysning om, hvilke servere it-systemerne afvikles på, og hvilken primær software der anvendes.

Disse relativt få oplysninger gør TET i stand til at foretage en overordnet vurdering af, hvilke it-systemer der indeholder forretningsdata, som er relevant for tilsynets kontrol.

For en nærmere gennemgang af de enkelte punkter i TETs infrastrukturoversigt henvises til skabelonen herfor (se bilag 1). Infrastrukturoversigtens indhold justeres og opdateres årligt efter behov.

1.3 Analyse og vurdering af data i infrastrukturoversigt

I TETs analyse og vurdering af data vedrørende it-infrastrukturen i PET, FE, CFCS og PPNR er det systemnavnet, der udgør den primære nøgle i tilsynets infrastrukturoversigt og

systemliste. Systemnavnet binder de to lister sammen og indgår som input til TETs årlige risiko- og væsentlighedsvurderinger.

Infrastrukturoversigten knytter de enkelte servere til et it-system og kan derfor anvendes til at krydstjekke og validere, hvorvidt der findes

- it-systemer, som ikke har servere tilknyttet,
- servere, som ikke er en del af et it-system,
- it-systemer og/eller servere, som TET endnu ikke har kendskab til, og
- it-systemer og/eller servere der er tilkommet eller bortfaldet siden senest opdaterede infrastrukturoversigt.

Infrastrukturoversigten giver endvidere TET mulighed for at krydstjekke og validere, om servere, der fremgår af infrastrukturoversigten, svarer til de servere, som i praksis kører i PETs, FEs, CFCS' og PPNRs it-miljøer. Dette tjekkes dels ved inspektionskontrol af tjenesternes, centrets og enhedens virtualiseringslag (hypervisor-administrationsværktøjer) samt af fysiske servere i serverrum. Samtidig kontrolleres det, hvorvidt der findes slukkede servere eller servere, der er taget ud af produktion (se afsnit 3).

TET foretager tillige screening og vurdering af de enkelte serveres relevans for kontrol ved at afdække følgende:

- Primære software, der afvikles på serveren
- Serverens primære rolle
- Serverens netværksmæssige placering
- Serverens navngivning, idet servere af rent praktiske grunde ofte navngives efter fastlagte regler og konventioner, som knytter sig til serverens funktion
- Hvilke andre servere, der indgår i samme it-system eller kontekst

Særligt serverens primære software er væsentlig, da det af hensyn til blandt andet overskuelighed, performance og driftssikkerhed i forhold til fejlsøgning, overvågning og redundans (fejltolerance) i større it-installationer er hensigtsmæssigt og derfor normalt at placere kritiske eller centrale funktioner i et it-system på en selvstændig server.

Endvidere placeres forretningssystemer og rene it-infrastrukturservere (for eksempel til administration, antivirus, softwareudrulning mv.) normalt ikke på de samme servere.

TETs vurdering af servere er derudover baseret på tilsynets akkumulerede viden om PET, FE, CFCS og PPNR samt deres it-systemer, herunder resultater af tidligere års kontroller samt den løbende dialog med relevante medarbejdere i tjenesterne, centret eller enheden.

1.4 Verifikation af data i infrastrukturoversigten

Verificering af de af PET, FE, CFCS og PPNRs indtastede oplysninger i infrastrukturoversigterne sker ved TETs løbende verificeringskontroller (se afsnit 3.4). Endvidere anvendes infrastrukturoversigterne løbende ved TETs almindelige kontroller til validering af de oplysninger, som PET, FE, CFCS og PPNR afgiver i forbindelse med indledende høringer ved kontroltype A (se afsnit 3.2 og 3.8).

1.5 Udformning og anvendelse af systemliste

TETs systemliste udarbejdes på baggrund af ovennævnte infrastrukturoversigt, tilgængelig systemdokumentation i PET, FE, CFCS og PPNR samt tilsynets akkumulerede viden. Systemlisten er et internt værktøj for TET, der løbende opdateres med relevant teknisk information. Systemlisten er vigtig for TETs forståelse af systemer, der anvendes af tjenesterne, centret og enheden, herunder sammenhænge mellem disse.

Systemlisten indeholder en vurdering af relevans og en score herfor af nye og/eller ukendte it-systemer, som TET ikke tidligere har foretaget kontrol af eller som tilsynet vurderer har undergået udvidelser eller ændringer, der kan påvirke tilsynets risiko- og væsentlighedsvurdering af systemet.

Systemlisten indeholder følgende:

- Kildeangivelse
- Systemnavn
- Beskrivelse
- Netværk/kontekst/miljø
- Påført systemliste (årstal)
- Relevansscore
- Relevansvurdering
- Navneændring

En uddybende forklaring på de enkelte punkter i systemlisten findes i skabelonen (se bilag 2). Systemlistens kolonner justeres og opdateres årligt.

1.6 Detaljeret procesbeskrivelse

I det følgende gennemgås processen for gennemførelse af TETs kortlægning af it-infrastruktur i PET, FE, CFCS og PPNR og opdatering af systemlister for hver myndighed. Opdateringen af systemlister skal være tilendebragt forud for TETs årlige risiko- og væsentlighedsvurdering af PET, FE, CFCS og PPNR.

PROCES	DEADLINE
1. Klargøring af det kommende års systemliste	
a. Oprettelse af systemliste for det kommende kalenderår oprettes på baggrund af forrige års liste	September
b. Opdatering af de enkelte kilder med årstal i kildeangivelseskolonnerne.	
c. Fastsættelse af værdierne i kolonnen "Navneændring" til "Nej"	
d. Godkendelse af kontrolnotat vedrørende udarbejdelse af systemliste (afsnit 1-4) hos TETs souschef	
2. Løbende tilføjelser til systemliste	
a. Løbende tilføjelse af nye systemer	Løbende
b. Angivelse af kildetype der ligger til grund for tilføjelsen	
c. Angivelse af hvilket års systemliste systemet første gang blev påført	
3. Årlig anmodning om kilder til systemliste	
a. Høring af PET, FE, CFCS og PPNR vedrørende infrastrukturoversigten	Januar
4. Udarbejdelse af systemliste	
a. Gennemgang af udvalgte kilder med henblik på at validere eksisterende systemer på systemliste samt identificere nye systemer	April-maj
b. Oprettelse af identificerede systemer, der ikke i forvejen fremgår af systemliste	
c. Angivelse i kildekolonnen af kilden, hvori systemet er identificeret	
d. Angivelse af systemliste for det år, hvor systemet første gang blev påført	
e. Angivelse af samtlige kilder, hvori både eksisterende og nye systemer er identificeret	
f. Angivelse af, om et eksisterende system har ændret navn	
5. Identifikation af nye, nedlagte og ændrede systemer	
a. Identifikation af nye systemer ved sortering af systemlistens kolonne "Påført systemliste" således, at kun systemer påført dette års systemliste fremgår	April-maj
b. Identifikation af nedlagte systemer udfindes ved sortering af aktuelle kildekolonner således, at kun systemer hvor der ikke er markeret aktuelle kilder fremgår	

PROCES	DEADLINE
c. Identifikation af ændrede systemer udfindes ved sortering af systemlistens kolonne "Navneændring" således, at kun systemer, der har ændret navn, fremgår	
d. Udtrækning af nye, nedlagte og ændrede systemer til selvstændige faneblade	
e. Sletning af nedlagte systemer fra årets systemliste	
6. Eventuel supplerende høring af PET, FE, CFCS eller PPNR	
a. Fremsendelse af eventuel supplerende høring af PET, FE, CFCS eller PPNR såfremt der under udarbejdelsen af årets systemliste opstår tvivl om, hvorvidt et systemnavn er en del af et systemkompleks, et redundant navn for et andet system, en applikation eller lignende	Maj
b. Fastsættelse af frist for besvarelse af høringen i overensstemmelse med TETs proces for høring	
c. Opdatering af systemliste på baggrund af høringssvar	
7. Intern overdragelse af systemliste	
a. Intern overdragelse af den færdige systemliste til relevante medarbejdere med henblik på risiko- og væsentlighedsvurdering	Juli
8. Evaluering	
a. Godkendelse af kontrolnotat vedrørende udarbejdelse af systemliste (afsnit 5) hos TETs souschef, hvori erfaringer, der er gjort i forbindelse med udarbejdelsen af årets systemliste, beskrives.	August

2 Risiko- og væsentligheds-vurdering

TETs risiko- og væsentlighedsvurdering af henholdsvis PET, FE, CFCS og PPNR har til formål at sammenstille og vurdere risici med henblik på at skabe det rette grundlag for beslutning om tilsynets egen drift-kontroller og undersøgelser på baggrund af anmodninger om indirekte indsigt efter PET-lovens § 13 og FE-lovens § 10.

TETs metode for risiko- og væsentlighedsvurdering af PET, FE, CFCS og PPNR er egenudviklet. TETs behov for at egenudvikle metoden skyldes den omstændighed, at tilsynet fører legalitetskontrol og at genstandsfeltet for tilsynets risiko- og væsentlighedsvurderinger ikke er interne processer i tilsynets virksomhed, men derimod en vurdering af andre myndigheders processer, systemer og generelle håndtering af personoplysninger. Det er således alene relevant for TET at analysere risici i forhold til brud på lovgivningen, og ikke øvrige strategiske, økonomiske, politiske eller administrative/procesmæssige konsekvenser.

TET gennemførte sin første årlige risikovurdering af PET, FE og CFCS i 2016. Metoden for TETs risikovurdering er blevet opdateret fire gange (senest i 2023 som følge af systemunderstøttelse af processen).

TETs metode for risiko- og væsentlighedsvurdering af PET, FE, CFCS og PPNR skal sikre sammenlignelighed inden for et givent år samt over tid, og sikre at vurderingerne er reproducerbare. Samtidig skal metoden være dynamisk og mulig at videreudvikle over tid, herunder i forhold til faktorer, der efterfølgende måtte inddrages som variabler i fremtidige risikovurderinger.

Denne standard indeholder en beskrivelse af processen for udarbejdelse af TETs årlige risiko- og væsentlighedsvurderinger samt metode for vurdering af risici og prioritering af kontrolobjekter.

Samlet består TETs årlige risiko- og væsentlighedsvurderinger af PET, FE, CFCS og PPNR af følgende:

RISIKOVURDERINGER	TETs systemunderstøttede risikovurderinger af samtlige kontrolobjekter i PET, FE, CFCS og PPNR indeholder risikoscorer for de enkelte kontrolobjekter samt angivelse af, samt hvorvidt der i relation til PET og FE foretages eller bør foretages undersøgelser i et givent system på baggrund af anmodninger om indirekte indsigt.
RISIKOANALYSER (EGEN-DRIFT KONTROLLER)	TETs prioriterede risikoanalyser af henholdsvis PET, FE, CFCS og PPNR vedrørende tilsynets egen drift-kontroller fremhæver faktorer, som gør, at et givent kontrolobjekt bør indgå, op- eller nedprioriteres i tilsynets kontrolplan for det kommende år.
RISIKOANALYSER (INDIREKTE INDSIGT)	TETs prioriterede risikoanalyser af henholdsvis PET og FE vedrørende indsigtsordningen indeholder nærmere vurderinger af, hvorvidt tilsynets undersøgelser på baggrund af anmodninger om indirekte indsigt er tilstrækkelige henset til de risici, der er identificeret og vurderet i risikovurderingerne.
KONTROLPLANER	TETs planer for det kommende års kontroller af henholdsvis PET, FE, CFCS og PPNR godkendes af tilsynet på baggrund af en samlet vurdering af ovenstående materiale.

Hensigten med opdelingen af TETs risiko- og væsentlighedsvurderinger i ovenstående delprodukter er at sikre gennemskuelighed og transparens i tilsynets vurdering af PET, FE, CFCS og PPNR.

2.1 Proces for udarbejdelse af TETs årlige risiko- og væsentlighedsvurderinger

Processen for udarbejdelse af TETs årlige risiko- og væsentlighedsvurderinger er som følger:

HELE ÅRET: Når kontroller afsluttes, reviderer TET sine risikovurderinger af de enkelte kontrolobjekter i PET, FE, CFCS og PPNR.

SEPTEMBER-OKTOBER: TET foretager risikovurdering af nye og ikke tidligere kontrollerede kontrolobjekter i PET, FE, CFCS og PPNR

OKTOBER-NOVEMBER: På baggrund af risikovurderingerne udarbejder TET risikoanalyser af henholdsvis PET, FE, CFCS og PPNR vedrørende tilsynets egen drift-kontroller og risikoanalyser af henholdsvis PET og FE vedrørende anmodninger om indirekte indsigt. Endelig udarbejdes udkast til kontrolplaner for det kommende års egen drift-kontroller af PET, FE, CFCS og PPNR.

NOVEMBER: TETs medlemmer forelægges materialet og godkender kontrolplaner for det kommende års egen drift-kontroller af PET, FE, CFCS og PPNR. TET resolverer tillige på omfanget af tilsynets undersøgelser på baggrund af anmodninger om indirekte indsigt, det vil sige, hvilke systemer der skal indgå i tilsynets undersøgelser heraf.

DECEMBER: TET orienterer henholdsvis PET, FE, CFCS og PPNR om tilsynets kontrolplaner for det kommende år.

Processen for TETs risiko- og væsentlighedsvurdering af PET, FE, CFCS og PPNR følger af årshjulet.

Hensigten med TETs orientering af PET, FE, CFCS og PPNR om tilsynets risiko- og væsentlighedsvurderinger samt kontrolplaner er, at tjenesterne, centret og enheden kan tage højde herfor i den interne kontrol og udarbejdelse af egne risiko- og væsentlighedsvurderinger. Derved sikres en gensidig erfaringsudveksling, der vil styrke såvel den risikoorienterede udvælgelse som effekten af TETs kontroller.

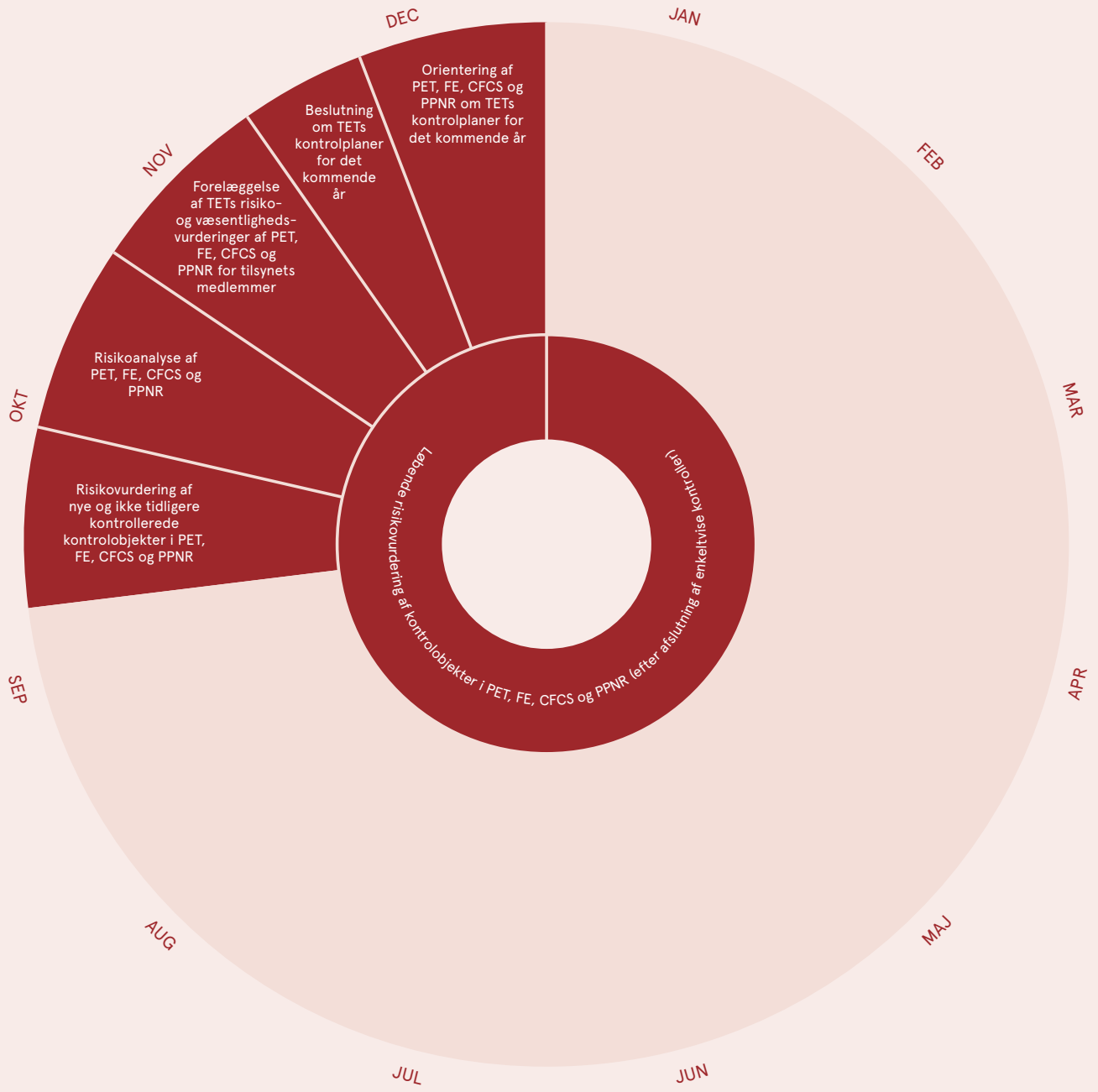
TETs direkte adgang til systemer i PET, FE, CFCS og PPNR sikrer i øvrigt, at tjenesterne, centret og enheden ikke kan forudse, hvilke sager og oplysninger der bliver genstand for tilsynets kontrol. Det kan imidlertid være nødvendigt for TET at varsle PET, FE, CFCS eller PPNR om tidspunktet og nærmere metode for en given kontrol, eksempelvis hvis tilsynet skal have adgang til særlige fysiske lokaliteter eller interviewe specifikke medarbejdere.

2.2 Risikovurdering af kontrolobjekter

Det er afgørende for TETs mulighed for at kunne foretage en risikobaseret udvælgelse af kontrolobjekter, og som følge heraf udføre en effektiv og målrettet kontrol, at tilsynet har et indgående kendskab til PET, FE, CFCS og PPNR.

TETs risikovurdering af kontrolobjekter er baseret på tilsynets akkumulerede viden om PET, FE, CFCS og PPNR, herunder særligt erfaringer fra gennemførelsen af tidligere års kontroller

Årshjul for TETs risiko- og væsentlighedsvurdering



samt den løbende dialog med relevante medarbejdere i henholdsvis tjenesterne, centret og enheden. Herved sikres en høj grad af validitet i risikovurderingen og den efterfølgende prioritering og udvælgelse af kontrolobjekter.

Som grundlag for TETs prioriterede risikoanalyser af PET, FE, CFCS og PPNR har tilsynet opstillet en model for udregning af risikoscorer for de enkelte kontrolobjekter. Risikoscoren er et udtryk for den samlede risiko/sandsynlighed for at der sker brud på en given lovregel i forbindelse med PETs, FEs, CFCS' og PPNRs aktiviteter relateret til kontrolobjektet.

Modellen vægter på forskellig vis følgende variabler med udgangspunkt i relevante lovbestemmelser (se bilag 1):

- *Kvaliteten af data* indeholdt i kontrolobjektet, dvs. hvorvidt data er struktureret, således at metadata er fikseret og ikke kan ændres af den almindelige bruger.

- *Omfanget af personoplysninger* indeholdt i kontrolobjektet.

- *Processen for databehandling* i kontrolobjektet, dvs. hvorvidt dette finder sted ved fuldt ud automatiserede processer, eller om behandlingen foregår ved helt eller delvise manuelle processer.

- *Placeringen af databehandlingen* for kontrolobjektet, dvs. hvorvidt behandlingen foregår centralt, hvor TET har egenhændig adgang, eller om den foregår decentralt, hvor tilsynets adgang forudsætter PETs, FEs, CFCS' eller PPNRs mellemkomst.

- *Logning og rettighedsstyring* i relation til databehandlingen i kontrolobjektet, dvs. hvorvidt alle relevante brugerhandlinger registreres korrekt, herunder om integriteten heraf er sikret, samt i hvilket omfang det sikres, at alene personer med behov for at kunne tilgå data indeholdt i kontrolobjektet har mulighed herfor.

- Omfanget af PETs, FEs, CFCS' og PPNRs *interne legalitetssikring* af kontrolobjektet, herunder en vurdering af

  - hvorvidt tjenesterne, centret og enheden har en fast praksis for juridisk godkendelse af efterretningsmæssige eller operationelle aktiviteter, og

  - i bekræftende fald, om denne godkendelse foregår via automatiserede stop-and-go processer uden mulighed for omgåelse, samt

  - hvorvidt relevant personale undervises i reglerne for brug af det givne kontrolobjekt, herunder om denne undervisning er baseret på introduktionsmæssig undervisning eller løbende dialog.

- Omfanget af PETs, FEs, CFCS' og PPNRs *interne kontrol* af kontrolobjektet, herunder

  - hvorvidt tjenesterne, centret og enheden foretager efterfølgende juridisk kontrol af et givent kontrolobjekt, og i bekræftende fald,

  - hvorvidt denne interne kontrol er planlagt på baggrund af en fastlagt praksis eller om den foregår på ad hoc eller decentral basis, og

  - hvorvidt den interne kontrol har vist lovbrud.

- Om *TET tidligere har foretaget kontrol* af kontrolobjektet, herunder angivelse af
  - hvornår tilsynet senest foretog kontrol,
  - hvorvidt tilsynets kontroller inden for de seneste 3 år har vist lovbrud,
  - hvorvidt tilsynets kontroller inden for de seneste 3 år har givet anledning til bemærkninger, og
  - hvad karakteren af de tidligere påpegede lovbrud og bemærkninger har været.

Således omfatter TETs model for udregning af risikoscorer for de enkelte processer og systemer i PET, FE, CFCS og PPNR følgende variabler og mulige værdier:

TETs model for udregning af risikoscorer

VARIABLER	VÆRDIER	
Datakvalitet	Struktureret	0
	Ustruktureret	2
	Ukendt	3
Omfang af personoplysninger	Mindre omfang	0
	Væsentligt omfang	2
	Ukendt	3
Proces for behandling	Automatiseret	0
	Delvist automatiseret	1
	Manuel	2
	Ukendt	3
Placering af behandling	Central, og TET har egenhændig adgang	0
	Central, men TET har ikke egenhændig adgang	1
	Decentral	2
	Ukendt	3
Logning og rettighedsstyring	Ja, i relevant omfang	0
	Ja, men i mindre relevant omfang	1
	Nej	2
	Ukendt	3
	N/A	0
Foretages intern legalitetssikring?	Ja, inkl. fast praksis for juridisk godkendelse	0
	Ja, dog ikke fast praksis for juridisk godkendelse	1
	Nej	3
	Ukendt	3
Foretages intern kontrol?	Ja, tilfredsstillende	0
	Ja, men ad hoc/decentralt/ikke tilfredsstillende	1
	Nej	3
	Ukendt	3
Har interne kontrol vist lovbrud?	Ja, lovbrud	2
	Ja, mindre lovbrud	1
	Nej	0
	N/A	0
Har TET foretaget kontrol?	Ja	0
	Nej	2
Hvornår foretog TET senest kontrol?	≥ 4 år	3
	3 år	2
	2 år	1
	≤ 1 år	0
	N/A	0
Har TETs tidligere kontrol vist lovbrud?	Nej	0
	Ja, mindre fejl ved seneste kontrol	2
	Ja, lovbrud ved seneste kontrol	5
	Ja, mindre fejl ved tidligere kontrol (≤ 3 år)	1
	Ja, lovbrud ved tidligere kontrol (≤ 3 år)	3
	N/A	0
Har TETs tidligere kontrol givet anledning til bemærkninger?	Nej	0
	Ja, mindre væsentlige bemærkninger ved seneste kontrol	2
	Ja, væsentlige bemærkninger ved seneste kontrol (kritisabelt/overordentligt kritisabelt)	5
	Ja, mindre væsentlige bemærkninger ved tidligere kontrol (≤ 3 år)	1
	Ja, væsentlige bemærkninger ved tidligere kontrol (kritisabelt/overordentligt kritisabelt) (≤ 3 år)	3
	N/A	0

TETs risikovurdering af de enkelte kontrolobjekter i PET, FE, CFCS og PPNR er systemunderstøttet således, at besvarelse af ovenstående variabler medfører udregning af risikoscorer for de enkelte kontrolobjekter i forhold til risikoen for brud på de enkelte lovbestemmelser inden for kontrolobjektet.

Risikoscorerne angives på en skala fra 0-26 med følgende angivelser:

Risikoscore 0-5	**Lav risiko** for lovbrud
Risikoscore 6-12	**Begrænset risiko** for lovbrud
Risikoscore 13-19	**Middel risiko** for lovbrud
Risikoscore 20-26	**Høj risiko** for lovbrud

Foruden besvarelse af ovenstående parametre i risikovurderingerne af de enkelte kontrolobjekter er det muligt at anføre bemærkninger omkring karakteren og mængden af de lovbrud, som TETs, PETs, FEs, CFCS' eller PPNRs hidtidige kontroller har afdækket, herunder om lovbrudene har været brud på lovbestemmelser eller interne retningslinjer, eller om de hidtidige kontroller har givet anledning til øvrige bemærkninger fra tilsynet, som ikke har omhandlet konkrete brud på lovregler eller interne retningslinjer mv.

Det er væsentligt, at denne mulighed for yderligere bemærkninger anvendes systematisk med henblik på at sikre muligheden for at holde risikoscoren op imod faktorer, som modellen ikke umiddelbart tager højde for. Derved vil det i prioriteringen af det givne kontrolobjekt i den efterfølgende risikoanalyse være muligt at differentiere og vægte de enkelte risikoscorer.

2.3 Prioriterede risikoanalyser og kontrolplaner

Med udgangspunkt i risikovurderingerne og de enkelte risikoscorer udarbejder TET risikoanalyser af henholdsvis PET, FE, CFCS og PPNR vedrørende tilsynets egen drift-kontroller og på baggrund heraf udkast til kontrolplaner for det kommende år. Endvidere udarbejder TETs særskilte risikoanalyser af henholdsvis PET og FE vedrørende tilsynets undersøgelser på baggrund af anmodninger om indirekte indsigt.

I risikoanalyserne vedrørende TETs egen drift-kontroller prioriteres kontrolobjekter ved fremhævelse af de faktorer, som gør, at et givent kontrolobjekt bør indgå, op- eller nedprioriteres i tilsynets kontrolplan for det kommende år.

Risikoscoren, som er udfundet ved de forudgående risikovurderinger af kontrolobjekterne, danner udgangspunktet for prioriteringen af kontrolobjekter. TET har ved risikoanalysen mulighed inddrage supplerende faktorer, herunder oplysninger anført i risikovurderingernes bemærkningsfelt, hvilket muliggør en kvalificeret differentiering og prioritering mellem de udfundne risikoscorer.

I TETs risikoanalyser inddrages følgende supplerende faktorer i prioriteringen af kontrolobjekter:

Faktorer der inddrages i TETs risikoanalyse af PET, FE, CFCS og PPNR

KATEGORI	FAKTOR/OVERVEJELSER
Eksterne forhold	**Politisk opmærksomhed**. Er der i det forgangne år udtrykt interesse fra politisk niveau om kontrol af områder inden for TETs mandat, som ikke tidligere har været genstand for kontrol eller ikke har været kontrolleret inden for de seneste 3 år?
	Offentlighedens opmærksomhed. Har der i det forgangne år været sager i offentligheden/medierne, som bør foranledige en nærmere kontrol af områder inden for TETs mandat, som ikke tidligere har været genstand for kontrol eller ikke har været kontrolleret inden for de seneste 3 år?
	Internationalt samarbejde. Er der i det forgangne år i TETs internationale samarbejde tilgået oplysninger om kontrolområder inden for tilsynets mandat, som ikke behandles i tilsynets risiko- og væsentlighedsvurdering af PET, FE, CFCS eller PPNR?
Interne forhold i PET, FE, CFCS eller PPNR	**Whistleblowing**. Er der i det forgangne år tilgået TET oplysninger fra nuværende eller tidligere ansatte i PET, FE, CFCS eller PPNR, som tilsynet bør foretage en nærmere kontrol på baggrund af?
	Områder under udvikling. Er der områder i PET, FE, CFCS eller PPNR vedrørende håndtering af personoplysninger, som er eller har været under betydelig udvikling i det forgangne år?
	Opfølgning på tidligere kontroller. Har TETs opfølgning på tidligere gennemførte kontroller af PET, FE, CFCS eller PPNR afdækket risici i det forgangne år, som ikke inddrages i tilsynets årlige risiko- og væsentlighedsvurderinger?
	PETs, FEs, CFCS' og PPNRs interne kontrol. Har PETs, FEs, CFCS' eller PPNRs interne kontrol afdækket risici i det forgangne år, som ikke inddrages i TETs årlige risiko- og væsentlighedsvurderinger?
	Behandlingssikkerhed. Har TETs kontrol af PETs, FEs, CFCS' eller PPNRs behandlingssikkerhed afdækket risici i det forgangne år, som ikke inddrages i tilsynets årlige risiko- og væsentlighedsvurderinger?
Teknologi	**Machine Learning (ML) / Artificial Intelligence (AI) og algoritmer**. Er der områder i PET, FE, CFCS eller PPNR, hvor der anvendes automatisk beslutningstagning eller på anden måde gøres brug af selvlærende algoritmer, ML eller AI?
	Bifangst. Er der områder i PET, FE, CFCS eller PPNR, der gør brug af tekniske kapaciteter som medfører en særlig risiko for tilvejebringelse af oplysninger om efterretningsmæssigt ikke-relevante personer?
	Anvendelse af ny teknologi. Er der områder i PET, FE, CFCS eller PPNR, hvor behandling af personoplysninger finder sted ved anvendelse af ikke-tidligere kontrolleret teknologi?

Derudover skal risikoanalyserne indeholde nærmere beskrivelser af emner, som det på baggrund af ovennævnte model ikke er muligt at udregne en specifik risikoscore for, herunder TETs nærmere vurdering af myndighedens interne kontrol samt en generel vurdering af PETs, FEs, CFCS' og PPNRs it-systemer, og hvorvidt tilsynets løbende kortlægning heraf skal revideres.

På baggrund af risikoanalyserne udarbejdes afslutningsvist udkast til kontrolplaner for det kommende års kontrol af henholdsvis PET, FE, CFCS og PPNR.

I risikoanalyserne vedrørende TETs undersøgelser på baggrund af anmodninger om indirekte indsigt efter PET-lovens § 13 og FE-lovens § 10 foretages vurderinger af, hvorvidt tilsynets undersøgelser af henholdsvis PET og FE er tilstrækkelige henset til de risici, der er identificeret og vurderet i risikovurderingerne. På den baggrund indstilles det til TETs beslutning, hvorvidt undersøgelserne er tilstrækkelige eller om de skal suppleres eller nedskaleres i forhold til udvalgte systemer.

3 Valg af metode, gennemførelse af kontrol og verificering af oplysninger

TET benytter sig af en række forskellige metoder i kontrollen af PET, FE, CFCS og PPNR, heriblandt fuldstændig kontrol, tilfældige eller målrettede stikprøver, indholdsscreening, inspektioner samt interview- og høringsbaserede kontroller.

Valg af metode finder sted efter en konkret risikovurdering af kontrolobjektet på baggrund af erfaringer fra tidligere kontroller, den forudgående tekniske og juridiske afdækning af et kontrolobjekt samt de faktiske forhold, som TET konstaterer i forbindelse med den specifikke kontrol.

Ved valg af kontrolmetode er det afgørende forinden at afdække, hvorvidt TET egenhændigt har adgang til datagrundlaget, og hvorvidt datagrundlaget består af struktureret eller ustruktureret data.

3.1 Proces for valg af metode, gennemførelse af kontrol og verificering af oplysninger

Processen for TETs valg af metode, gennemførelse af kontrol og verificering af oplysninger er som følger:

DECEMBER: Fremsendelse af indledende høringer til PET, FE, CFCS og PPNR vedrørende teknisk og juridisk afdækning af kontrolobjekter for det kommende år, som TET ikke tidligere har kontrolleret, eller hvor forudsætningerne for kontrollen er eller kan være ændret (kontroltype A, jf. afsnit 3.2).

JANUAR-FEBRUAR: Udarbejdelse og godkendelse af kontrolnotater vedrørende kontrolobjekter, som kan gennemføres efter en allerede fastlagt metode uden opstartsmøde med PET, FE, CFCS eller PPNR (kontroltype B, jf. afsnit 3.2).

JANUAR-DECEMBER: Gennemførelse af kontrol af kendte kontrolobjekter (kontroltype B, jf. afsnit 3.2).

FEBRUAR-SEPTEMBER: Afholdelse af opstartsmøder med PET, FE, CFCS og PPNR vedrørende kontrolobjekter, som TET ikke tidligere har kontrolleret, eller hvor forudsætningerne for kontrollen er eller kan være ændret (kontroltype A, jf. afsnit 3.2).

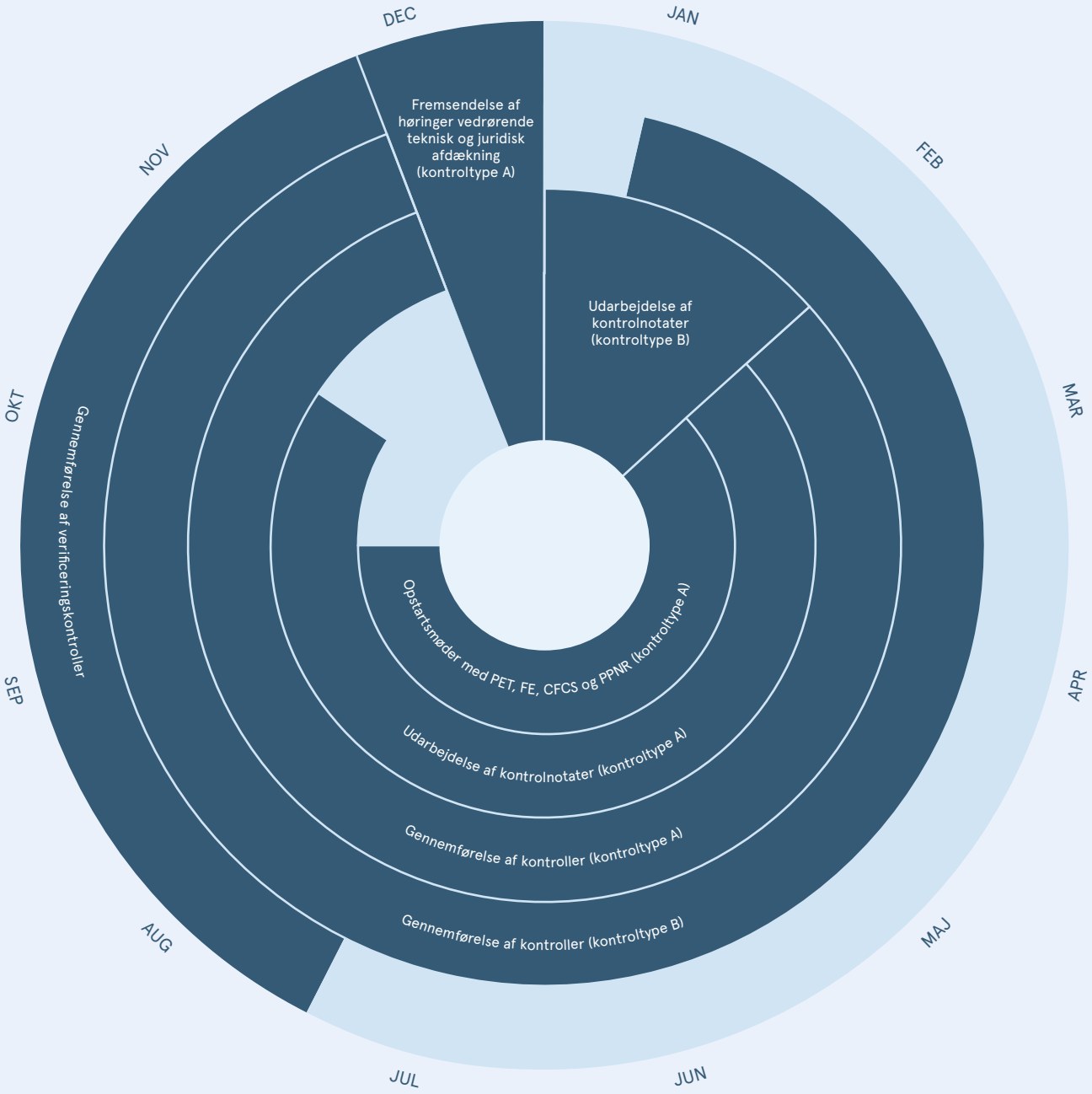
FEBRUAR-OKTOBER: Udarbejdelse og godkendelse af kontrolnotater vedrørende kontrolobjekter, som TET ikke tidligere har kontrolleret, eller hvor forudsætningerne for kontrollen er eller kan være ændret (kontroltype A, jf. afsnit 3.2).

FEBRUAR-DECEMBER: Gennemførelse af kontrol af kontrolobjekter, som TET ikke tidligere har kontrolleret eller hvor forudsætningerne for kontrollen er eller kan være ændret (kontroltype A, jf. afsnit 3.2).

AUGUST-NOVEMBER: Gennemførelse af verificeringskontroller med henblik på at sikre, at oplysninger, som TET har modtaget fra PET, FE, CFCS og PPNR vedrørende disses it-infrastruktur er korrekte (se afsnit 3.4). TETs verificeringskontroller kategoriseres som kontroltype B, jf. afsnit 3.2.

Processen for TETs valg af metode, gennemførelse af kontrol og verificering af oplysninger følger af årshjulet.

Årshjul for TETs valg af metode, gennemførelse af kontrol og verificering af oplysninger



3.2 Kontroltype

Når TET har godkendt kontrolplanerne for det kommende års kontroller af henholdsvis PET, FE, CFCS og PPNR (se afsnit 2), skal der indledningsvist foretages en vurdering af, hvorvidt de enkelte kontroller vedrører:

KONTROLTYPE A	Et nyt kontrolobjekt eller et objekt, hvor forudsætningerne for kontrollen er eller kan være ændret, og at der derfor er behov for afklaring af ramme og metode for kontrollen, herunder ved opstartsmøde med PET, FE, CFCS eller PPNR. Ved denne kontroltype foretages indledende høring af PET, FE, CFCS eller PPNR med henblik på afdækning af tekniske, faktuelle og juridiske forhold vedrørende kontrolobjektet (se bilag 5). Endvidere afholdes opstartsmøde med PET, FE, CFCS eller PPNR, forinden TET fastlægger metode for kontrollen.
KONTROLTYPE B	Et kendt kontrolobjekt med en relativ fast ramme for kontrollen, der kan gennemføres efter en allerede fastlagt metode uden opstartsmøde med PET, FE, CFCS eller PPNR.

Beslutning om kontroltype angives i TETs kontrolplaner vedrørende PET, FE, CFCS og PPNR ud for de enkelte kontroller.

Det er TETs ansvarlige sagsbehandler, der har ansvaret for eventuelle ændringer af vurderingen af kontroltype ved ad hoc inddragelse af nye kontrolemner, eller hvis det viser sig, at en given kontrol alligevel ikke kan gennemføres efter en allerede kendt metode.

En ændring af vurderingen skal godkendes af TETs souschef og ajourføres i kontrolplanen.

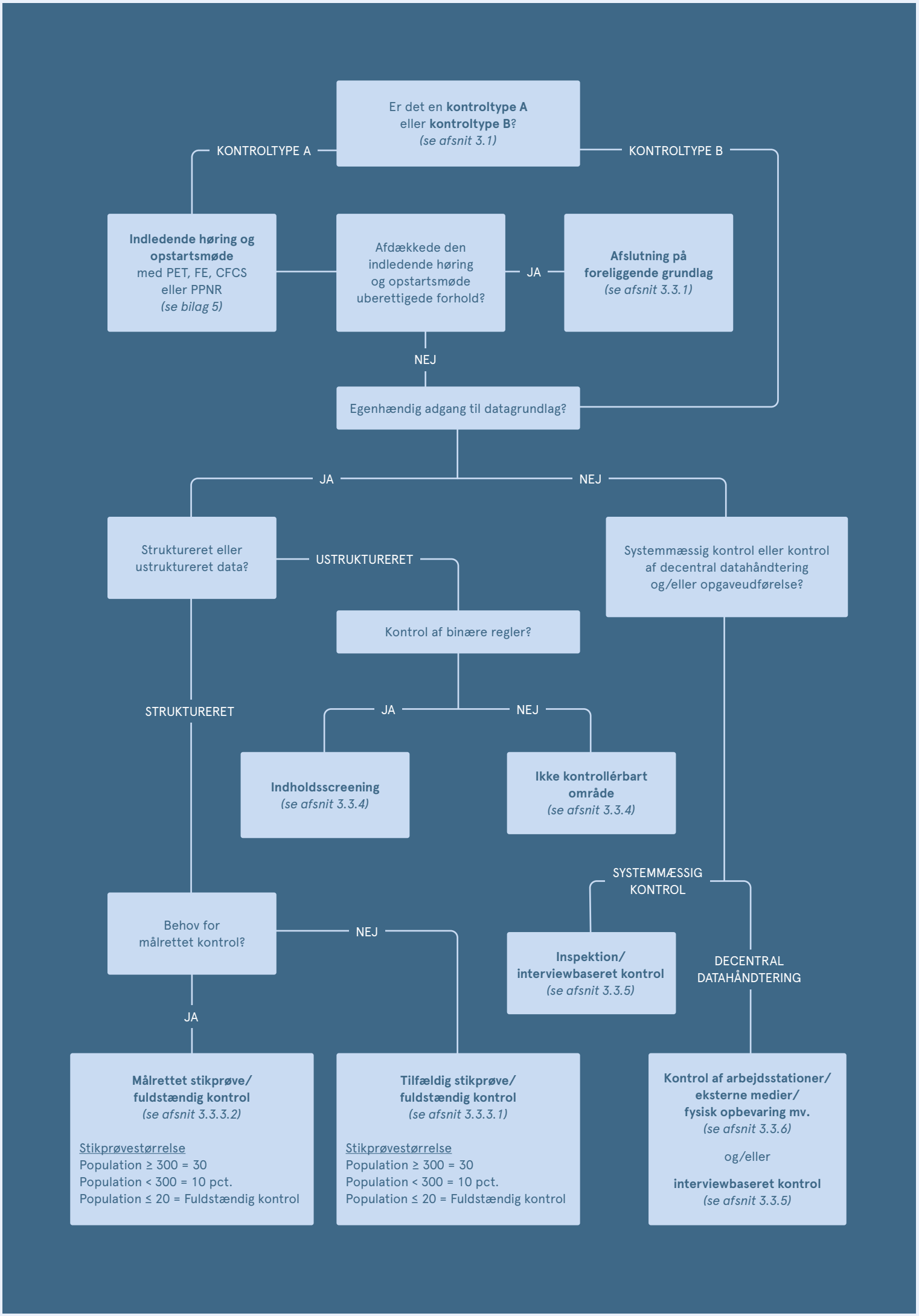
3.3 Kontrolmetoder

Når kontroltypen for et givent kontrolobjekt er afklaret, skal metoden for kontrollen besluttes. Valg af metode sker på baggrund af erfaringer fra tidligere kontroller, den konkrete risikovurdering af kontrolobjektet på baggrund af den tekniske og juridiske afdækning ved opstartsmøder med PET, FE, CFCS eller PPNR samt de faktiske forhold, som TET konstaterer i forbindelse med den specifikke kontrol.

Ved valg af kontrolmetode er det afgørende forinden at afdække, hvorvidt TET egenhændigt har adgang til datagrundlaget, og hvorvidt data består af struktureret eller ustruktureret data.

Nedenfor følger en gennemgang af de forskellige metoder til kontrol, som TET anvender. Den ansvarlige sagsbehandler har til opgave at foranledige en intern drøftelse af egnede kontrolmetoder for et givent kontrolobjekt i tæt dialog med den relevante sektionsleder og øvrige relevante medarbejdere i sektionen. På den baggrund udarbejdes en indstilling til kontrolmetode, der i alle tilfælde skal godkendes af TETs souschef.

Overordnet følger TETs beslutning om kontrolmetode følgende proces:


Er det en **kontroltype A** eller **kontroltype B**? *(se afsnit 3.1)*
KONTROLTYPE A
KONTROLTYPE B
Indledende høring og opstartsmøde med PET, FE, CFCS eller PPNR *(se bilag 5)*
Afdækkede den indledende høring og opstartsmøde uberettigede forhold?
JA
Afslutning på foreliggende grundlag *(se afsnit 3.3.1)*
NEJ
Egenhændig adgang til datagrundlag?
JA
NEJ
Struktureret eller ustruktureret data?
USTRUKTURERET
Systemmæssig kontrol eller kontrol af decentral datahåndtering og/eller opgaveudførelse?
Kontrol af binære regler?
STRUKTURERET
JA
NEJ
Indholdsscreening *(se afsnit 3.3.4)*
Ikke kontrollérbart område *(se afsnit 3.3.4)*
SYSTEMMÆSSIG KONTROL
Behov for målrettet kontrol?
NEJ
Inspektion/ interviewbaseret kontrol *(se afsnit 3.3.5)*
DECENTRAL DATAHÅNDTERING
JA
Målrettet stikprøve/ fuldstændig kontrol *(se afsnit 3.3.3.2)*
Stikprøvestørrelse
Population ≥ 300 = 30
Population < 300 = 10 pct.
Population ≤ 20 = Fuldstændig kontrol
Tilfældig stikprøve/ fuldstændig kontrol *(se afsnit 3.3.3.1)*
Stikprøvestørrelse
Population ≥ 300 = 30
Population < 300 = 10 pct.
Population ≤ 20 = Fuldstændig kontrol
Kontrol af arbejdsstationer/ eksterne medier/ fysisk opbevaring mv. *(se afsnit 3.3.6)*
og/eller
interviewbaseret kontrol *(se afsnit 3.3.5)*

3.3.1 Afslutning på foreliggende grundlag

Såfremt TETs opstartsmøde med PET, FE, CFCS eller PPNR afdækker forhold, som ved en umiddelbar vurdering ikke findes at være i overensstemmelse med gældende lovgivning, foretages høring med henblik på at indhente tjenestens, centrets eller enhedens bemærkninger.

Hvis TET på baggrund af høringssvaret fortsat vurderer, at de pågældende forhold ikke er i overensstemmelse med lovgivningen, afslutter tilsynet kontrollen på det foreliggende grundlag. TET vil i den sammenhæng bemærke over for PET, FE, CFCS eller PPNR, at tilsynet ikke vil foretage nærmere datanær kontrol af objektet førend de pågældende forhold er bragt i overensstemmelse med lovgivningen.

Hvis TET på baggrund af høringssvaret derimod vurderer, at de pågældende forhold er i overensstemmelse med lovgivningen eller i øvrigt ikke er en hindring for at foretage en nærmere datanær kontrol af objektet skal der tages beslutning om kontrolmetode, jf. afsnit 3.3.2-3.3.6.

3.3.2 Fuldstændig kontrol

Fuldstændig kontrol af et givent kontrolobjekt kan være en meget ressourcekrævende metode at anvende. Fuldstændige kontroller er således forbeholdt meget små populationer (poster/sager/individer mv. ≤ 20) eller helt særlige sager, hvor det vurderes af afgørende betydning at gennemgå det fuldstændige datagrundlag.

Et tænkt eksempel på små populationer kunne være en kontrol af FEs søgning i rådata, hvor gennemgang af et specifikt logudtræk – på baggrund af en forudgående frasortering af falske positiver – viser, at tjenesten inden for en given kontrolperiode alene har foretaget 20 eller færre søgninger i rådata vedrørende i Danmark hjemmehørende personer. Heraf skal der foretages en fuldstændig kontrol.

I kategorien "helt særlige sager" findes TETs særlige undersøgelse af FE i 2019/2020 samt tilfælde, hvor det vurderes nødvendigt at afdække den totale mængde af lovbrud eller behandling af oplysninger i strid med lovgivningen.

Ved populationer ≥ 21 skal der som udgangspunkt foretages stikprøvekontrol (se afsnit 3.3.3), medmindre særlige forhold gør sig gældende for fortsat at foretage en fuldstændig kontrol.

3.3.3 Stikprøve

Ved en stikprøvekontrol udvælges et mindre antal poster/sager/individer mv. fra en større population af data. En stikprøve er således en delmængde af en population, og giver TET et estimat over egenskaberne i populationen.

Stikprøver er en effektiv metode til kontrol af større mængder data. Det er imidlertid vigtigt, at gøre sig klart, hvorledes stikprøven er udvalgt, og dermed i hvor høj grad et kontrolresultat kan ekstrapoleres til det fulde datagrundlag. Ved brug af simpel tilfældig udvælgelse, dvs. en *tilfældig stikprøve* (se afsnit 3.3.3.1), er det muligt at generalisere forhold i stikprøven til den samlede population (ekstrapolering).

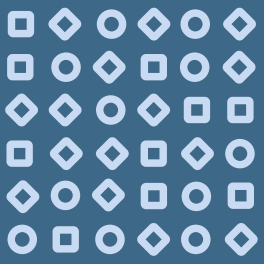
Hvor retvisende er TETs stikprøver?

Fordelen ved at kontrollere ved stikprøve er, at det både er hurtigere og mindre ressourcekrævende end at undersøge en hel population af poster/sager/oplysninger om individer mv. Men hvad er egenskaberne af en stikprøve?

STIKPRØVE

- Gennemsnit kan beregnes
- Andel af personoplysninger, der ikke er indhentet, behandlet eller videregivet i overensstemmelse med lovgivningen, kan beregnes

POPULATION

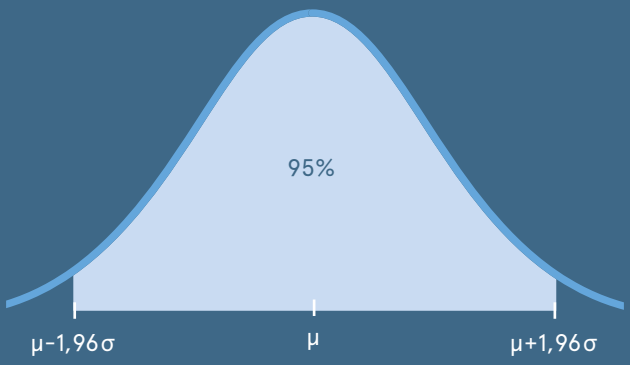


- Gennemsnit er ukendt
- Andel af personoplysninger, der ikke er indhentet, behandlet eller videregivet i overensstemmelse med lovgivningen, er ukendt (medmindre der foretages en fuldstændig kontrol heraf)

Undersøgelse af poster/sager/oplysninger om individer i en stikprøve gør det altså muligt at udtale sig om den fulde population. Det vil sige, at stikprøven giver et estimat over egenskaberne i populationen.

Hvis en population af poster/sager/oplysninger om individer er større end 10.000, kan det i henhold til den centrale grænseværdisætning antages, at fordelingen af værdier i populationen er som en normalfordeling.

NORMALFORDELING er i statistik den vigtigste og oftest forekommende af alle sandsynlighedsfordelinger. Den beskriver eksempelvis fordelingen af måleresultater, når disse er behæftet med en vis usikkerhed. Normalfordelingen har form som en klokkekurve, hvor toppunktet af kurven angiver middelværdien (μ) af det statistiske materiale, og bredden af kurven er et mål for spredningen (σ) eller standardafvigelsen.



Et **KONFIDENSINTERVAL** er en statistisk metode til at angive – udtrykt som et interval – hvor præcis en måling eller stikprøve er. Eksempelvis kan et 95 procent-konfidensinterval omkring en middelværdi angive, at man med 95 procent sikkerhed forventer, at det sande mål vil ligge inden for dette interval.

Men hvorfra kommer konstanten 1,96 i figuren? Hvis man kigger på fordelingsfunktionen for en normalfordeling med middelværdi 0 og varians 1, så er det samlede areal under kurven 1. Hvis man er interesseret i at finde det område under grafen, som dækker 95 procent af arealet, skal man fjerne 2,5 procent af arealet i begge ender. De ±1,96 svarer til det område under kurven, som giver et areal på 95 procent.

KONFIDENSNIVEAUET refererer til den procentdel af gange, hvor det konfidensinterval, man beregner, vil indeholde det sande mål i gentagne stikprøver. Et konfidensniveau på 95 procent er almindeligt og betyder, at hvis man gentog stikprøvetagningen mange gange, så ville 95 procent af de resulterede konfidensintervaller indeholde det sande mål.

Med andre ord, normalfordelingen beskriver fordelingen af data, konfidensintervallet er et interval, der estimerer det sande mål og konfidensniveauet er den procentdel af gange, man forventer, at dette interval vil indeholde det sande mål baseret på gentagne stikprøver.

Effekten af stikprøvestørrelser er at indsnævre konfidensintervallet – det vil sige båndet af gæt omkring estimatets middelværdi – ved samme konfidensniveau. Med en større stikprøve kan man dermed med samme sikkerhed sige noget mere præcist om populationen, end man kan med en mindre stikprøve. I små populationer er fordelingen lidt anderledes, hvilket gør, at en stikprøve kan være mindre ved samme usikkerhedsmargen.

Ved en tilfældig stikprøve anvender TET det, der kaldes en simpel randomiseret stikprøve. Dette opfylder kravene til at kunne anvende sandsynlighedsteori.

TETs **STIKPRØVESTØRRELSER** anvender et 95 procent-konfidensinterval. Mindst 95 procent af stikprøvernes resultater, hvis man udtog dem igen og igen, vil således indeholde det sande mål for populationen – i dette tilfælde den procentvise andel data/sager/poster/personoplysninger som ikke er indhentet, behandlet eller videregivet i overensstemmelse med lovgivningen.

Hvis TET ved en tilfældig stikprøve eksempelvis finder, at 16 procent af de udtrukne personoplysninger ikke er indhentet, behandlet eller videregivet i overensstemmelse med lovgivningen, så kan tilsynet med 95 procent sikkerhed udtale sig om, at tilsvarende gælder for den fulde population.

Det vil i TETs kontrol imidlertid være nødvendigt til tider at foretage en stikprøve baseret på en forudgående modellering/opdeling af datagrundlaget (populationen) ved metoder anvendt i relation til stratifikation, dvs. inddeling af populationen i gensidigt udelukkende dele (strata), eller klyngeudvælgelse. Disse metodiske begreber anvendes i denne procesvejledning bredt under betegnelsen *målrettet stikprøve* (se afsnit 3.3.3.2).

3.3.3.1

Tilfældig stikprøve

Ved simpel tilfældig udvælgelse, dvs. en tilfældig stikprøve, udtrækkes poster/sager/individer mv. til kontrol ved brug af en tilfældighedsgenerator uden forudgående bearbejdning af datagrundlaget (populationen).

TET anvender en tilfældighedsgenerator til udtrækning af tilfældige stikprøver ved indtastning af størrelse på population samt det ønskede antal poster til udtrækning.

Størrelsen på stikprøven afhænger af populationens størrelse:

- Population ≥ 300 = 30 poster/sager/individer mv.
- Population < 300 = 10 pct. af poster/sager/individer mv.
- Population ≤ 20 = Fuldstændig kontrol

Såfremt TETs standarder for stikprøvestørrelse følges, er det ved en tilfældig stikprøve muligt at ekstrapolere resultatet af en stikprøve til den samlede population.

3.3.3.2

Målrettet stikprøve

Ved målrettet udvælgelse, dvs. målrettet stikprøve, udtrækkes poster/sager/individer mv. til kontrol på baggrund af en forudgående bearbejdning af datagrundlaget (populationen).

Bearbejdning af datagrundlaget omfatter al form for målretning i TETs dataindsamling, herunder ved brug af søgestrenge til fremsøgning af en specifik gruppe af sager eller frasortering af falske positiver i forbindelse med gennemgang af logudtræk.

Ved en målrettet stikprøve udtrækkes poster/sager/individer mv. som udgangspunkt tillige ved brug af TETs tilfældighedsgenerator på baggrund af det bearbejdede datagrundlag. Afhængigt af behovet for målretning af stikprøven kan det imidlertid være en fordel at udtrække stikprøven på baggrund af en screening af det bearbejdede datagrundlag, dvs. manuel udvælgelse af de mest egnede poster/sager/individer mv. til kontrol.

Som ved en tilfældig stikprøve afhænger størrelsen på stikprøven af populationens størrelse:

- Population ≥ 300 = 30 poster/sager/individer mv.
- Population < 300 = 10 pct. af poster/sager/individer mv.
- Population ≤ 20 = Fuldstændig kontrol

Såfremt TETs standarder for stikprøvestørrelse følges, er det ved en målrettet stikprøve muligt at ekstrapolere resultatet af en stikprøve til den bearbejdede population.

3.3.4 Indholdsscreening/ikke kontrollérbart område

Såfremt datagrundlaget for en kontrol er kendetegnet ved ustruktureret data – dvs. data uden fikseret metadata, manglende mulighed for effektiv fremsøgning og/eller fravær af brugerhændelseslogning – er TETs muligheder for kontrol væsentligt indskrænket.

I sådanne tilfælde er TETs eneste mulighed at foretage kontrol på baggrund af binære regler, dvs. bestemmelser der ikke danner grundlag for en skønsmæssig vurdering – eksempelvis slettefristbestemmelser, der kan kontrolleres ved indholdsscreening/opslag.

Indholdsscreening er i relation til ustruktureret data ikke en anvendelig metode til afdækning af det komplette omfang af brud på eksempelvis slettefristbestemmelserne, men kan anvendes i en overordnet undersøgelse af, hvorvidt en given population indeholder brud på bestemmelserne. Indholdsscreening anvendes primært i kombination med inspektion af PETs, FEs, CFCS' eller PPNRs sletning af oplysninger i decentrale systemer, hvor det ikke er muligt at anvende funktioner i systemerne til at fremsøge oplysninger, som er ældre end slettefristen.

I tilfælde hvor TETs kontrol ikke er fokuseret på binære regler, og hvor datagrundlaget er kendetegnet ved ustruktureret data, klassificeres kontrolobjektet som et "ikke kontrollérbart område", og forelægges herefter for tilsynet til drøftelse og godkendelse (se afsnit 3.5).

Såfremt et kontrolobjekt klassificeres som et "ikke kontrollérbart område", modtager PET, FE, CFCS eller PPNR meddelelse herom efter gældende proces (se afsnit 3.6). I den sammenhæng opfordres PET, FE, CFCS eller PPNR til snarest muligt at etablere muligheder for at kunne foretage en effektiv kontrol, ligesom offentligheden vil blive gjort opmærksom herpå i TETs årlige redegørelser.

3.3.5 Inspektion/interviewbaseret kontrol

Såfremt TET ikke egenhændigt har adgang til et datagrundlag i relation til et givent kontrolobjekt, skal det afklares hvorvidt der skal foretages en systemmæssig kontrol eller kontrol af en decentral datahåndtering og/eller opgaveudførsel (se afsnit 3.3.6) – eller en kombination heraf.

En systemmæssig kontrol omfatter undersøgelse af det tekniske og processuelle setup af et givent indhentnings-, behandlings-, videregivelsessystem mv., herunder om muligt efterprøvelse af systemets efterlevelse af binære regler som eksempelvis håndtering af automatisk sletning af oplysninger.

En systemmæssig kontrol vil som udgangspunkt foregå i en kombination af en systemnær inspektion og en interviewbaseret kontrol, der samlet – foruden efterprøvelse af, hvorvidt kontrolobjektets datahåndtering finder sted i overensstemmelse med relevante binære regler – skal afdække risici for lovbrud.

Ved interviewbaseret kontrol er det afgørende, at forberede en klar spørgeramme for kontrollen, herunder eventuelt varsle PET, FE, CFCS eller PPNR om de overordnede emner for kontrollen med henblik på at sikre, at TET kan interviewe relevante teknikere/brugere af systemet under inspektionen.

I udfærdigelsen af en spørgeramme for den interviewbaserede kontrol skal fokus være på at sikre en effektiv kommunikation mellem TET og PET, FE, CFCS eller PPNR. Det er i den sammenhæng vigtigt at forberede klare og utvetydige spørgsmål, hvor formålet er at afdække

de faktiske forhold, ligesom det er vigtigt at anvende kontrolspørgsmål, hvor et kompliceret emne søges afdækket ved brug af samme spørgsmål i en ny formulering (tillægsspørgsmål).

Dataindsamlingen fra inspektionen/den interviewbaserede kontrol skal herefter sammenholdes med den forudgående dataindsamling i form af den tekniske afdækning af kontrolobjektet og/eller data fra tidligere års kontroller.

3.3.6 Kontrol af decentral datahåndtering

Kontrol af decentrale systemer omfatter arbejdsstationer, transitmedier og lignende, hvor det kan være vanskeligt at sikre dokumentation for kontrolresultatet. Kontrol af decentrale systemer sker ved brug af alle ovennævnte metoder (afsnit 3.3.2-3.3.5), men et særligt fokus i denne type kontrol er at sikre den rette dokumentation. Derfor suppleres den valgte kontrolmetode med følgende værktøjer til dokumentation:

- Kontrolskema
- Skærmbillede
- Kamera
- Skriftlig bekræftelse

Inden kontrollen påbegyndes, afholdes et formøde mellem de af TETs medarbejdere, som skal udføre kontrollen. Under mødet diskuteres

- de enkelte spørgsmål i kontrolskemaet, herunder hvad der anses for at være fyldestgørende svar, og
- hvilke forhold medarbejderne skal være særligt opmærksomme på i forbindelse med den pågældende kontrol.

3.3.6.1 Skærmbillede

Såfremt der i forbindelse med kontrollen er behov for at dokumentere fund, som opbevares elektronisk (eksempelvis på fildrev mv.), sikres dokumentation af fundet efter følgende fremgangsmåde:

1) PETs, FEs, CFCS' eller PPNRs medarbejder anmodes om at tage et skærmbillede af fundet.
    a. Ved dokumentation af filer på fildrev skal skærmbilledet tydeligt vise filtype, filnavn, ændringsdato, oprettelsesdato, størrelse og placering.
    b. Ved dokumentation af mails i postkasser tages et skærmbillede af indholdet af den mappe, som mailen findes i, som tydeligt viser afsender, emnefelt og modtagelsesdato/afsendelsesdato. Hvis det er nødvendigt for kontrollen, dokumenteres tillige mailens indhold. Såfremt der er fundet personoplysninger i flere af de mails, som fremgår af skærmbilledet, skal dette noteres i skemaet, således at det er muligt at identificere de mails, som indeholder personoplysninger.
    c. Ved dokumentation af filer og e-mails skal uret i nederste højre hjørne fremgå af skærmbilledet.

2) Skærmbilledet påføres bilagsnummer. Bilagsnummeret noteres i kontrolskemaet sammen med en kort beskrivelse af fundet.

3) PETs, FEs, CFCS' eller PPNRs juridiske afdeling fremsender dokumentet til TET. Mailen forsynes med den pågældende medarbejders medarbejdernummer i emnefeltet.

4) To af TETs medarbejdere kontrollerer, at skærmbilledet opfylder de ovenfor beskrevne krav, inden mailen sendes.

5) Umiddelbart efter kontrollen er gennemført, kontrolleres det, at TET har modtaget de korrekte skærmbilleder.

Dokumentation bør tillige sikres i tilfælde, hvor der er tvivl om, hvorvidt der er tale om et relevant fund. TETs medarbejdere kan om nødvendigt oplyse den pågældende medarbejder om, at dokumentationen ikke nødvendigvis betyder, at der er tale om behandling i strid med lovgivningen.

3.3.6.2

Kamera

Såfremt det er aftalt med PET, FE, CFCS eller PPNR og at der i forbindelse med kontrol af en decentral datahåndtering er behov for at dokumentere fund, som *ikke* opbevares elektronisk (eksempelvis i sikkerhedsskabe), sikres dokumentation for det fundne materiale efter følgende fremgangsmåde:

1) TETs medarbejder tager – ved brug af særligt sikret udstyr hertil – et billede af det fundne materiale.

   a. Billedet skal tydeligt vise overskrift, dokumentdato, sagsnummer, serienummer og lignende af betydning for kontrollen.

   b. Billedet skal tillige vise den placering, hvor materialet er fundet. Om nødvendigt kan der tages to separate billeder af materiale og placering.

2) PETs, FEs, CFCS' eller PPNRs medarbejder anmodes om at estimere, hvor længe dokumentet har været opbevaret på den givne placering, og svaret noteres i kontrolskemaet.

3) I kontrolskemaet noteres endvidere billedets bilagsnummer med tilhørende billednummer sammen med en kort beskrivelse af, hvad billedet viser.

4) Umiddelbart efter kontrollen overføres billederne til TETs klassificerede system, og hvert billede påføres bilagsnummer. Afslutningsvist slettes indholdet på kameraets hukommelseskort ved at formatere kortet, hvorefter det makuleres, så der ikke efter endt kontrol efterlades eventuelt klassificeret billedmateriale i kameraet.

Dokumentation bør tillige sikres i tilfælde, hvor der er tvivl om, hvorvidt der er tale om et relevant fund. TETs medarbejdere kan om nødvendigt oplyse den pågældende medarbejder om, at dokumentationen ikke nødvendigvis betyder, at der er tale om behandling i strid med lovgivningen.

3.3.6.3

Skriftlig bekræftelse

Såfremt det ikke er muligt at dokumentere fundet ved brug af skærmbilleder eller kamera, hvilket blandt andet kan skyldes sikkerhedsmæssige forhold, udfyldes en medbragt blanket.

Med henblik på at sikre, at der er enighed om beskrivelsen af fundet, underskrives blanketten af såvel TETs medarbejder som en repræsentant fra PETs, FEs, CFCS' eller PPNRs juridiske afdeling.

3.4 Verificeringskontrol

På baggrund af TETs kortlægning af it-infrastrukturen i henholdsvis PET, FE, CFCS og PPNR foretager tilsynet årlige verificeringskontroller af de oplysninger, som tilsynet har modtaget fra tjenesterne, centret og enheden.

TET krydsvaliderer således, om servere, der er kortlagt i PET, FE, CFCS og PPNR, svarer til de servere, som i praksis kører i de pågældende it-miljøer. Endvidere verificeres indholdet af udvalgte servertyper, herunder filservere og databaseservere. Dette kontrolleres dels ved årlige inspektioner af PETs, FEs, CFCS' og PPNRs virtualiseringslag (hypervisor-administrationsværktøjer) samt af fysiske servere i serverrum. Samtidig kontrolleres det, hvorvidt der findes slukkede servere eller servere, der er taget ud af produktion.

Verificering af de af PET, FE, CFCS og PPNRs indtastede oplysninger i infrastrukturoversigterne, som udarbejdes i forbindelse med TETs kortlægning af it-infrastruktur (se afsnit 1), i forhold til eksisterende servere udføres ved at krydstjekke servernavne på infrastrukturoversigten med de aktuelle servere, som optræder i tjenesternes, centrets og enhedens bruger- og objekt-directory og/eller server-administrationskonsoller (eksempelvis hypervisor-administrationsmoduler). Dette kræver læseadgang til de nævnte administrationsmoduler eller udskrifter fra PET, FE, CFCS og PPNR, der kan udskrives under en inspektion.

Verificering af kontekst- og netværksinddelinger krydstjekkes mod konfigurationsoversigter fra netværksudstyr og firewalls, herunder lister over hvilke netværk (herunder VLAN), der er oprettet.

3.5 Afrapportering til TET

Forinden forelæggelse af en kontrol for TETs medlemmer skal det fornødne beslutningsgrundlag være til stede. Dette sikres ved udførlig dokumentation og journalisering af

- TETs møder med PET, FE, CFCS eller PPNR,
- TETs specifikke risikovurdering af kontrolområdet,
- TETs valg af kontrolmetode,
- TETs gennemførelse af kontrol, herunder loglister, kontrolskemaer mv.,
- TETs høringer og høringssvar samt
- TETs kontrolnotat (se afsnit 3.5.1).

Før ovenstående er sikret, kan en kontrol ikke forelægges TETs medlemmer til drøftelse og/eller godkendelse.

3.5.1 Kontrolnotat

Kontrolnotater er en konsolidering af alle væsentlige oplysninger vedrørende et kontrolobjekt, herunder

- baggrund og formål med kontrollen samt TETs overordnede risikovurdering af objektet,
- en objektiv beskrivelse af kontrolobjektet, herunder på baggrund oplysninger modtaget fra PET, FE, CFCS eller PPNR på møder mv.,
- TETs specifikke risikovurdering af kontrolobjektet på baggrund af eventuelt opstartsmøde med tjenesten, centret eller enheden,
- TETs valg af kontrolmetode,
- resultaterne af TETs kontrol og
- erfaringer på baggrund af gennemførelse af kontrollen, herunder en vurdering af behovet for at gennemføre en lignende kontrol og/eller at foretage en fremtidig justering kontrolmetode mv.

Til udarbejdelse af kontrolnotater anvendes skabelonen i bilag 6.

Forinden forelæggelse af en kontrol for TETs medlemmer skal relevant dokumentation journaliseres på kontrolsagen. Endvidere skal kontrolnotatet være endeligt godkendt af TETs souschef.

Herefter kan kontrollen forelægges til drøftelse og/eller godkendelse for TETs medlemmer, herunder indgå i tilsynets interne kontrol (se afsnit 3.5.2.3).

3.5.2 Forelæggelse af kontrol på tilsynsmøde

Når en kontrol er klar til at blive forelagt TETs medlemmer, udarbejdes indstilling herom i den kommenterede dagsorden (KDO) til førstkommende tilsynsmøde. KDO og tilhørende bilag gennemgås af TETs formand og medlemmer i forbindelse med deres forberedelse af tilsynsmødet.

Forinden udarbejdelse af indstilling til KDO skal det afklares, hvorvidt et kontrolresultat skal indstilles til drøftelse i TET eller godkendelse uden yderligere behandling på mødet (se afsnit 3.5.2.1).

Ved udarbejdelse af indstillinger til TET er det væsentligt at sikre, at kun relevante beskrivelser/informationer medtages i KDO. Herved sikres, at TET forelægges klare, tydelige og ensrettede indstillinger.

Såfremt TET forelægges et teknisk og/eller juridisk kompliceret emne, er det afgørende at anvende faktabokse i KDO og/eller vedlægge detaljerede bilag.

3.5.2.1 *Kontrolresultater til drøftelse og/eller godkendelse*

Som udgangspunkt skal en kontrol alene indstilles til drøftelse i TET såfremt resultaterne giver anledning til principielle spørgsmål, der påkræver tilsynsmedlemmernes stillingtagen. I tvivlstilfælde afklarer TETs sagsbehandler dette med pågældendes sektionsleder samt tilsynets sekretariatschef eller souschef.

Hvis en kontrol indstilles til drøftelse i TET markeres dette i KDOen ud for indstillingen med angivelsen *"behandles på mødet"*.

3.5.2.2 *Forelæggelse af bilag*

Bilag (tekniske kortlægninger, kontrolskemaer, høringer, høringssvar mv.) forelægges som udgangspunkt alene for TETs medlemmer, når der ved kontrollen er konstateret brud på reglerne eller kontrollen på anden måde giver anledning til bemærkninger til PET, FE, CFCS eller PPNR, som efterfølgende skal behandles i et opfølgningsbrev (se afsnit 3.6).

3.5.2.3 *TETs interne kontrol*

TETs kontroller forelægges for tilsynets medlemmer på tilsynsmøder med henblik på drøftelse og afslutning af disse, og i den forbindelse forelægges der som udgangspunkt kun kontrolmateriale, der har givet anledning til høring af PET, FE, CFCS eller PPNR (se afsnit 3.5.2.2).

TETs medlemmer foretager intern kontrol af tilsynets kontrolvirksomhed. Det skyldes, at en omfattende mængde af TETs kontrolmateriale ikke forelægges tilsynets medlemmer, idet materialet ikke dokumenterer behandling i strid med lovgivningen og derfor ikke giver anledning til høring af PET, FE, CFCS eller PPNR.

Fremgangsmåden for TETs interne kontrol er som følger:

- TETs interne kontrol foretages af kontrolmateriale, som vedrører de kontroller, der forventes afsluttet på det kommende tilsynsmøde.
- Kontrolmaterialet, der er omfattet af den interne kontrol, har ikke givet anledning til høring af PET, FE, CFCS eller PPNR, hvorfor det ikke er vedlagt som bilag til mødematerialet.
- Kontrollerne af PET, FE, CFCS eller PPNR, der er omfattet af TETs interne kontrol, bliver inddelt i individuelle talgrupper, og hver enkelt kontrol får tildelt ét tal (eksempelvis PET-1, FE-3, CFCS-2, PPNR-2).
- Tilsynsmedlemmet vælger én kontrol fra hver af de kontrollerede myndigheder ved tilfældigt at vælge et tal uden at vide hvilken kontrol, tallet vedrører.
- Tilsynsmedlemmet får fra hver tilfældigt udvalgt kontrol udleveret kontrolskemaer.
- Tilsynsmedlemmet får ligeledes udleveret kontrolnotat samt øvrigt relevant dokumentation for hver tilfældigt udvalgt kontrol, således at tilsynsmedlemmet opnår baggrundsviden for kontrollerne, herunder om valg af metode og evaluering af resultat. Tilsynsmedlemmerne vil herved opnå en mere detaljeret viden om TETs overvejelser vedrørende den konkrete kontrol, såvel som de konsekvenser resultatet af kontrollen skal have for fremtidige kontroller.
- Tilsynsmedlemmet vil endelig få udleveret et kontrolskema, hvoraf det vil fremgå, hvilke kontroller, herunder hvilke kontrolskemaer, som tilsynsmedlemmet har

kontrolleret. Medlemmet vil have mulighed for at notere bemærkninger til kontrollerne heri. Kontrolskemaet underskrives af medlemmet, når den interne kontrol afsluttes.

- Tilsynsmedlemmet fremlægger på næstkommende tilsynsmøde resultaterne af den interne kontrol for de øvrige tilsynsmedlemmer.

3.6 Afrapportering til PET, FE, CFCS og PPNR

Når TETs medlemmer på møde har godkendt en kontrol fremsendes et opfølgningsbrev til PET, FE, CFCS eller PPNR. Til udarbejdelse af opfølgningsbrev anvendes skabelon i bilag 7.

Når TETs medlemmer har godkendt opfølgningsbrevet sendes det med formandens underskrift uden unødigt ophold til PET, FE, CFCS eller PPNR.

3.7 Afrapportering til justitsministeren og forsvarsministeren samt offentliggørelse af TETs årlige redegørelser

På baggrund af de af TET fremsendte opfølgningsbreve til PET, FE, CFCS og PPNR inden for et givent kontrolår udarbejder tilsynet årlige redegørelser, som fremsendes til henholdsvis justitsministeren (PET og PPNR) og forsvarsministeren (FE og CFCS).

TETs udkast til redegørelser godkendes som udgangspunkt på tilsynsmøde ultimo februar, hvorefter tilsynet fremsender disse til henholdsvis PET, FE, CFCS og PPNR med henblik på afklaring af, om redegørelserne indeholder klassificerede eller urigtige oplysninger.

Efter afrapportering til justitsministeren og forsvarsministeren afventer TET besked om, hvornår redegørelserne har været forelagt Folketingets Udvalg vedrørende Efterretningstjenesterne (Kontroludvalget), hvorefter redegørelserne kan offentliggøres.

3.8 Detaljeret procesbeskrivelse

I det følgende gennemgås processen for gennemførelse af TETs kontroller:

PROCES	DEADLINE

1. Praktisk forberedelse af kontroller

December

a. *Oprettelse af journalsager* for alle kontroller på kontrolplanen

b. *Kategorisering* af alle kontroller som enten kontroltype A eller B

c. *Tildeling af ansvarlig sagsbehandler* for hver kontrol

d. *Orientering af og eventuelt møde* med PET, FE, CFCS og PPNR om det kommende års kontrolplan

1.A AFSENDELSE AF INDLEDENDE HØRING (GÆLDER ALENE KONTROLTYPE A)

Ultimo december

a. *Afsendelse* af indledende høring indeholdende informationsark for samtlige kontroller (kontroltype A) inklusiv indkaldelse til opstartsmøde (se bilag 5)

   Indkaldelse til opstartsmøde sker med et ugenummer, og mødet kan tidligst afholdes fra uge 8

   Høringsfristen fastsættes til mandag ved arbejdstidsophør to uger før ugen for opstartsmødet

   Eksempel på fastsættelse af høringsfrist:
   Afsendelse af høring med tilhørende informationsark samt indkaldelse til opstartsmøde i uge 8.
   Svarfristen for anmodningen vil være mandag i uge 6 ved arbejdstids ophør

b. *Tilføjelse af datoer* for høring og høringsfrist på sagen

1.B FORBEREDELSE AF OPSTARTSMØDE (GÆLDER ALENE KONTROLTYPE A)

Inden afholdelse af opstartsmøde

a. *Gennemlæsning* af høringssvar med tilhørende informationsark

b. *Udarbejdelse af spørgeramme* i informationsarket til brug for opstartsmøde

c. *Inddragelse af infrastrukturoversigt* i relevant omfang

1.C OPSTARTSMØDE (GÆLDER ALENE KONTROLTYPE A)

Forberedelse

N/A

a. *Print* af relevant materiale til samtlige mødedeltagere forud for mødet

b. *Intern drøftelse i sektionen* af materiale og spørgeramme forud for mødet

Opsamling

a. *Gennemgang* af resultaterne af mødet med øvrige deltagere fra TET

b. *Notering* af svar på spørgeramme i informationsark til brug for opstartsmøde

c. *Fremsendelse* af eventuelle uafklarede spørgsmål og forespørgsler til PET, FE, CFCS eller PPNR

2. Fastlæggelse af kontrolmetode

Egne undersøgelser

Kontroltype A
Senest 1 uge efter afholdt opstartsmøde

a. *Efterprøvelse* af om TET har adgang og relevante brugerrettigheder til kontrolobjektet

b. *Undersøgelse* af hvorledes kontrolobjektet tilgås (applikation, web, e.l.) og fungerer (klient og system), herunder funktioner, typer af data og snitflader

Kontroltype B
Senest i uge 6

c. *Anmodning om brugerrettigheder* såfremt TET ikke har de relevante adgange til kontrolobjektet

PROCES	DEADLINE
d. *Fremsøgning af eksisterende information* om kontrolobjektet, herunder for eksempel tidligere kontrolnotater, it-landskab, detailskema, egne noter og dokumentation fra PET, FE, CFCS eller PPNR mv.	
e. *Journalisering* af al relevant dokumentation	
Fastlæggelse af kontrolmetode	
a. *Udarbejdelse* af indstilling til kontrolmetode (se afsnit 3.3) ved udfyldelse af afsnit 1-4 i kontrolnotat (se bilag 6) under inddragelse af sektionsleder	
b. *Journalisering* af kontrolnotat, informationsark og eventuelt yderligere relevant materiale	
c. *Afsendelse af udkast til kontrolnotat til bemærkninger* hos relevante medarbejdere, som deltog i opstartsmødet	
d. *Indarbejdelse* af eventuelle bemærkninger	
e. *Godkendelse af kontrolnotat* (afsnit 1-4) hos TETs souschef	

3. Gennemførelse af kontrol

Gennemførelse	N/A
a. *Gennemførelse af kontrol* i overensstemmelse med den fastlagte kontrolmetode	
b. *Godkendelse af kontrolskema* hos sektionsleder	
Ved mulige lovbrud foretages høring af PET, FE, CFCS eller PPNR	
a. *Godkendelse af udkast til høring* hos TETs sekretariatschef	
b. *Fastsættelse af høringsfrist* i overensstemmelse med TETs proces for høring af PET, FE, CFCS og PPNR (se appendiks)	
c. *Tilføjelse af datoer* for høring og høringsfrist på sagen	
Modtagelse af høringssvar	
a. *Journalisering* af høringssvar	
b. *Tilføjelse af dato* for høringssvar på sagen	

4. Afslutning af kontrollen

Godkendelse af kontrolnotat	Senest en uge inden tilsynsmøde
a. *Færdiggørelse* af udkast til kontrolnotat	
b. *Godkendelse* af kontrolnotat (afsnit 5) hos TETs souschef	
Godkendelse af opfølgningsbrev og punkt til kommenteret dagsorden (KDO) til tilsynsmøde	
a. *Udarbejdelse* af udkast til opfølgningsbrev og punkt til KDO til tilsynsmøde samt fremsendelse til godkendelse hos sektionsleder	
b. *Fremsendelse* til endelig godkendelse hos TETs sekretariatschef	
c. *Endelig godkendelse* af opfølgningsbrev på tilsynsmøde	
Fremsendelse af opfølgningsbrev til PET, FE, CFCS eller PPNR	Senest tre dage efter tilsynsmøde
a. *Fremsendelse* af opfølgningsbrev til PET, FE, CFCS eller PPNR	

PROCES	DEADLINE
b. *Færdiggørelse af journalisering* af sagen	
c. *Påfør kontrollen* i TETs skemaer vedrørende opfølgningskontrol i det kommende år	
Modtagelse af eventuelle bemærkninger a. *Modtagelse* af eventuelle bemærkninger fra PET, FE, CFCS eller PPNR b. *Beslutning* om hvorvidt bemærkninger giver anledning til at korrigere eller supplere tidligere fremsendte opfølgningsbrev	4 uger efter fremsendelse af TETs opfølgningsbrev

5. Gennemførelse af kontrol

Godkendelse af udkast til TETs årlige redegørelser a. *Godkendelse* af udkast til redegørelser på tilsynsmøde	Uge 8-13
Høring af PET, FE, CFCS og PPNR a. *Fremsendelse* af udkast til TETs årlige redegørelser til PET, FE, CFCS og PPNR med henblik på afklaring af, om udkastene indeholder klassificerede eller urigtige oplysninger. Høringsfrist sættes til 2 uger. b. *Indarbejdelse* af eventuelle bemærkninger fra PET, FE, CFCS og PPNR	Uge 9-14
Afgivelse af TETs årlige redegørelser om PET, herunder PPNR, FE og CFCS til henholdsvis justitsministeren og forsvarsministeren	N/A
Offentliggørelse af TETs årlige redegørelser om PET, herunder PPNR, FE og CFCS	Når TET har modtaget orientering fra Justitsministeriet og Forsvarsministeriet om, at redegørelserne har været forelagt Udvalget vedrørende Efterretningstjenesterne

Appendiks og bilag

APPENDIKS A

Ordforklaring

Denne ordliste forklarer de vigtigste begreber anvendt i TETs standarder.

BEGREB	FORKLARING
Binære regler	Bestemmelser der ikke danner grundlag for en skønsmæssig vurdering. Eksempelvis slettefristbestemmelser, der kan kontrolleres ved simpelt opslag.
Kontrolobjekt	Genstand for TETs kontrol, dvs. system/proces/område, som tilsynet har besluttet, at der skal foretages kontrol af.
Kontroltype A	Et nyt område eller et område, hvor forudsætningerne for kontrollen er eller kan være ændret, og der derfor er behov for afklaring af ramme og metode for kontrollen, herunder ved opstartsmøde med PET, FE, CFCS eller PPNR.
Kontroltype B	Et kendt kontrolemne med en (nogenlunde) fast ramme for kontrollen, der kan gennemføres efter en allerede fastlagt metode uden opstartsmøde med PET, FE, CFCS eller PPNR.
Population	Det samlede datagrundlag, der er genstand for en specifik kontrol.
Stikprøve	Et begrænset udsnit af det fulde datagrundlag (population). En stikprøve kan være udtrukket tilfældigt eller på baggrund af målrettede parametre (se afsnit 3.3.3).
Ustruktureret data	Data uden fikseret metadata, manglende mulighed for effektiv fremsøgning og/eller fravær af brugerhændelseslogning.

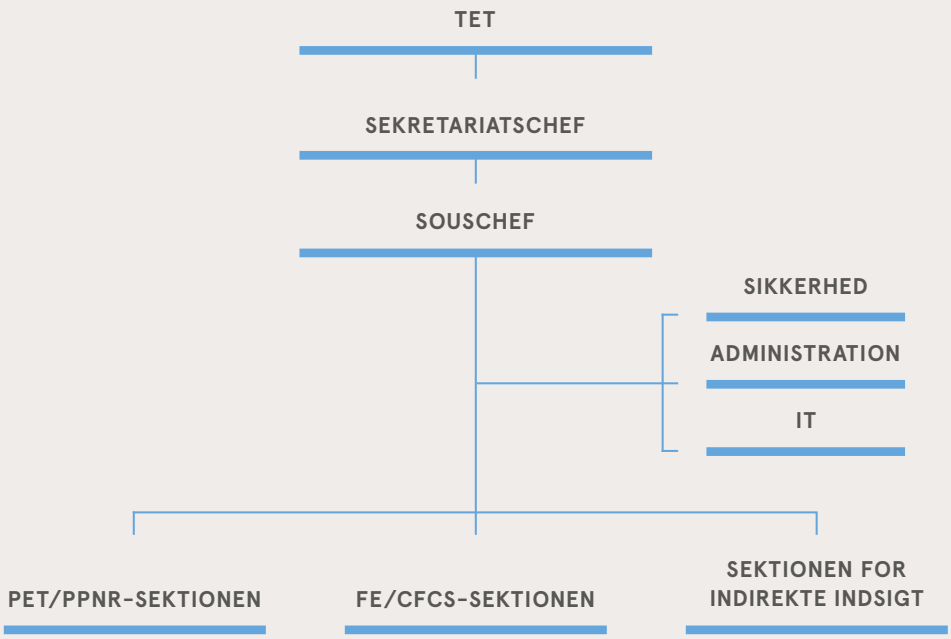
APPENDIKS B

TETs organisation

TET består af fem medlemmer, der er udpeget af justitsministeren efter forhandling med forsvarsministeren. Formanden, der skal være landsdommer, er udpeget efter indstilling fra præsidenterne for Østre Landsret og Vestre Landsret, mens de øvrige medlemmer er udpeget efter drøftelser med Folketingets Udvalg vedrørende Efterretningstjenesterne.

TET bistås af et sekretariat, der alene er undergivet tilsynets instruktion. TET bestemmer selv, hvem der skal ansættes til sekretariatet, herunder hvilken uddannelsesmæssig baggrund og øvrige kvalifikationer de pågældende skal have. De primære faggrupper i TETs sekretariat er jurister, politologer og it-specialister.

Sekretariatet er opdelt i sektioner, der beskæftiger sig med henholdsvis PET/PPNR, FE/CFCS og anmodninger om indirekte indsigt. Med henblik på at sikre faglig koordinering og erfaringsudveksling arbejder TETs medarbejdere på tværs af sektionerne.



APPENDIKS C

Generelle forudsætninger for TETs kontrol og tilsynets forventninger til PET, FE, CFCS og PPNR

TETs kontrolvirksomhed bidrager til legitimeringen af PETs, FEs, CFCS' og PPNRs aktiviteter ved at styrke offentlighedens tillid til, at disse aktiviteter er lovmedholdelige.

TETs virke er bestemt ved lov, herunder

- at tilsynet efter klage eller af egen drift påser, at PET, FE, CFCS og PPNR behandler personoplysninger i overensstemmelse med lovgivningen,
- at tilsynet hos PET, FE, CFCS og PPNR kan kræve enhver oplysning og alt materiale, der er af betydning for tilsynets virksomhed,
- at tilsynet til enhver tid har adgang til alle lokaler, hvorfra der er adgang til de oplysninger som behandles, eller hvor tekniske hjælpemidler anvendes,
- at tilsynet kan afkræve PET, FE, CFCS og PPNR skriftlige udtalelser om faktiske og retlige forhold af betydning for tilsynets kontrolvirksomhed,
- at PET, FE, CFCS eller PPNR – såfremt disse undtagelsesvist beslutter ikke at følge en henstilling i en udtalelse fra tilsynet – uden unødigt ophold skal forelægge sagen for henholdsvis justitsministeren eller forsvarsministeren til afgørelse,
- at tilsynet underretter henholdsvis justitsministeren og forsvarsministeren om forhold, som ministrene efter tilsynets opfattelse bør have kendskab til, og
- at tilsynet årligt skal afgive redegørelser om sin virksomhed, som skal offentliggøres.

Hvis PET, FE, CFCS eller PPNR undlader til fulde at efterleve disse grundlæggende forudsætninger for en effektiv og retvisende kontrol, vil det i væsentlig grad svække TETs muligheder for at kontrollere tjenesternes, centrets og enhedens lovmedholdelighed og herved sikre myndighedernes legitimitet over for offentligheden.

TET har følgende forventninger til PET, FE, CFCS og PPNR i opfyldelsen af disse krav:

TETs adgang til oplysninger

TET forventer, at PET, FE, CFCS og PPNR giver tilsynet uhindret, fuldstændig og rettidig adgang til alt materiale, som er relevant for at tilsynet kan gennemføre en korrekt og effektiv kontrol.

TET forventer, at PET, FE, CFCS og PPNR sikrer, at tilsynet har de rette brugeradgange til tjenesternes, centrets og enhedens it-infrastruktur, som sikrer direkte og uhindret adgang til relevante oplysninger for tilsynets kontrol.

TET forventer i de tilfælde, hvor der af tekniske årsager ikke kan gives fulde brugerrettigheder til udvalgte dele af PETs, FEs, CFCS' eller PPNRs it-infrastruktur, at tilsynet oplyses om

- karakteren og omfanget af den del af it-infrastrukturen, som tilsynet ikke egenhændigt har adgang til, og
- karakteren og omfanget af data, som behandles i den del af it-infrastrukturen, som tilsynet ikke egenhændigt har adgang til.

Uhindret, fuldstændig og rettidig adgang til materiale af betydning for TETs virksomhed er afgørende for en effektiv og retvisende kontrol.

PET, FE, CFCS eller PPNR vil undtagelsesvist kunne afgive udtalelse omkring undladelse af kontrol af udvalgte oplysninger. For at TETs lovbestemte adgang til oplysninger iagttages, er det imidlertid alene tilsynet, der har beslutningskompetencen om, hvorvidt udvalgte oplysninger kan undlades i forbindelse med en kontrol.

Såfremt TET ikke har mulighed for at verificere, at de pågældende oplysninger, som PET, FE, CFCS eller PPNR ønsker undladt i forbindelse med en kontrol, ikke er relevante for tilsynets kontrol vil dette udgøre en væsentlig risiko for omgåelse af loven.

Besvarelse af TETs høringer

TET forventer, at PETs, FEs, CFCS' og PPNRs høringssvar er fuldstændige, gennemsigtige og uforbeholdne.

TET forventer, at PET, FE, CFCS og PPNR oplyser tilsynet om eksistensen af øvrigt relevante oplysninger eller materiale af betydning for kontrollen, som tjenesterne, centret eller enheden måtte erkende, at tilsynet ikke har indsigt i.

TET forventer, at PETs, FEs, CFCS' og PPNRs høringssvar afgives rettidigt og inden for de tidsrammer, som fremgår af tilsynets proces for høring af tjenesterne, centret og enheden (se TETs proces for høring af PET, FE, CFCS og PPNR).

Med henblik på at sikre en effektiv og retvisende kontrol fremsender TET målrettede anmodninger om udtalelser om faktiske og retlige forhold af betydning for tilsynets kontrolvirksomhed.

TET har beslutningskompetencen i afgørelsen af, om udvalgte oplysninger er relevante for kontrollen, hvorfor PETs, FEs, CFCS' og PPNRs høringssvar skal være fuldstændige, gennemsigtige og uforbeholdne.

PET, FE, CFCS eller PPNR må således ved besvarelse af TETs høringer ikke selvstændigt foretage en vurdering af, om udvalgte anmodninger om oplysninger er relevante for tilsynets kontrol.

Opfølgning på TETs kontrol

TET forventer – såfremt PET, FE, CFCS eller PPNR måtte have bemærkninger til resultatet af tilsynets enkeltvise kontroller – at disse fremsendes til tilsynet inden for den frist, som er angivet i tilsynets opfølgningsbrev.

TET forventer – såfremt PET, FE, CFCS eller PPNR undtagelsesvist måtte beslutte ikke at følge en henstilling fra tilsynet – at tjenesten, centret eller enheden opfylder deres oplysningspligt og uden unødigt ophold forelægger sagen for henholdsvis justitsministeren eller forsvarsministeren til afgørelse.

Praksis, som TET har vurderet ikke er lovmedholdelig, og hvor PET, FE, CFCS eller PPNR er enige heri, skal indstilles straks, og uenighed om fortolkningen af lovgrundlaget bør afklares uden unødigt ophold. Det er derfor afgørende, at PET, FE, CFCS eller PPNR rettidigt responderer på tilsynets henstillinger, herunder om nødvendigt ved at forelægge en given sag for henholdsvis justitsministeren og forsvarsministeren til afgørelse.

APPENDIKS D

Skala for bemærkninger til PET, FE, CFCS og PPNR

TETs bemærkninger til PET, FE, CFCS og PPNR, der fremsendes til tjenesten, centret og enheden i et klassificeret opfølgningsbrev (se bilag 7) og efterfølgende offentliggøres i tilsynets årlige redegørelser om sin virksomhed i en ikke-klassificeret version, tager udgangspunkt i følgende skala:

BEMÆRKNINGER	BAGGRUND FOR BEMÆRKNINGER
[…] ***giver ikke anledning til bemærkninger***	Anvendes når TET er enig med myndigheden i, hvordan loven generelt eller konkret administreres.
TET finder ***ikke*** *på det foreliggende grundlag, at* ***det er muligt at vurdere*** […]	Anvendes når TETs prøvelsesmuligheder er begrænset enten af faktiske eller juridiske forhold.
TET finder det ***bemærkelsesværdigt*** […]	Anvendes om forhold i myndigheden eller lovgivningen, som ikke stemmer overens med det almindelige eller umiddelbare indtryk, som en udenforstående har.
TET finder det ***problematisk*** […]	Anvendes om forhold, hvor der ikke er konstateret egentlige lovbrud, men hvor der vurderes at være en stor risiko for, at forholdene kan føre til lovbrud eller hvor TET har været forhindret i at udøve sin virksomhed i en periode af en vis varighed.
TET kan ***konstatere*** […]	Anvendes om forhold, hvor der er konstateret egentlige lovbrud af enkeltstående karakter eller brud på interne retningslinjer.
TET finder det ***kritisabelt*** […]	Anvendes om forhold, hvor der er konstateret ikke uvæsentlige lovbrud eller hvor TET har været forhindret i at udøve sin virksomhed i en længere periode.
TET finder det ***overordentligt kritisabelt*** […]	Anvendes om forhold, hvor der er konstateret alvorlige lovbrud eller hvor TET har været forhindret i at udøve sin virksomhed i en længere periode, uden at myndigheden har udvist vilje til at sikre den fornødne afhjælpning heraf.

APPENDIKS E

TETs proces for høring af PET, FE, CFCS og PPNR

Følgende proces gælder for TETs høring af henholdsvis PET, FE, CFCS eller PPNR:

1) Ved fremsendelse af en høring fastsætter TET en høringsfrist på 25 arbejdsdage. Høringsfristen regnes fra den første arbejdsdag efter modtagelsen af høringen. Følgende uger medregnes ikke i forbindelse med fastsættelsen afhøringsfrister:

   - Uge 7
   - Uge 28, 29 og 30
   - Uge 42
   - Uge 52

2) Såfremt høringens omfang eller kompleksitet gør, at TET vurderer, at besvarelse heraf ikke er mulig inden for 25 arbejdsdage, fastsætter tilsynet en høringsfrist på 60 arbejdsdage.

3) Såfremt PET, FE, CFCS eller PPNR efter modtagelse af en høring fra TET vurderer, at høringen ikke kan besvares inden for den angivne frist har tjenesten, centret eller enheden følgende muligheder:

   Ved modtagelse af høring med frist på *25 arbejdsdage*

   i. PET, FE, CFCS eller PPNR kan undtagelsesvist skriftligt anmode TET om forlængelse af svarfristen fra 25 arbejdsdage til 60 arbejdsdage. Det forudsættes, at anmodningen som udgangspunkt fremsættes senest *15 arbejdsdage* efter modtagelsen af høringen og indeholder en konkret begrundelse.

   Ved modtagelse af høring med frist på *60 arbejdsdage*

   ii. PET, FE, CFCS eller PPNR kan undtagelsesvist senest 15 arbejdsdage efter modtagelsen af høringen skriftligt tilkendegive over for TET, at det ikke vurderes muligt at besvare høringen inden for den angivne frist. Det forudsættes, at anmodningen indeholder en konkret begrundelse.

      I tilfælde heraf vil TET indstille kontrollen af det pågældende område, hvorefter tilsynet vil gå i dialog med PET, FE, CFCS eller PPNR om, hvornår området forventes klar til kontrol.

      Det vil herefter fremgå af TETs årlige redegørelse, at den planlagte kontrol ikke kunne gennemføres i indeværende år, men at tilsynet og PET, FE, CFCS eller PPNR er i dialog om klargøring af området til kontrol.

[Politiets Efterretningstjeneste/
Forsvarets Efterretningstjeneste/
Center for Cybersikkerhed/
Politiets PNR-enhed]

Tilsynet med Efterretningstjenesterne

Dato:
Sagsbeh.: [Navn 1] [Navn 2]
Sagsnr.: [Sagsnr.]
Dok.: [Dokumentnr.]

Anmodning vedrørende [PETs / FEs / CFCS' / PPNRs] it-infrastruktur

TET planlægger, tilpasser og gennemfører sine kontroller af [PET / FE / CFCS / PPNR] på baggrund af løbende, årlige risiko- og væsentlighedsvurderinger af [tjenestens / centrets / enhedens] arbejdsprocesser og it-systemer.

TETs viden om [PETs / FEs / CFCS' / PPNRs] it-infrastruktur, herunder systemer, er afgørende for fuldstændigheden af tilsynets kontrol samt for tilsynets muligheder for at vurdere risici i forhold til [tjenestens / centrets / enhedens] tilvejebringelse, behandling, herunder sletning, og videregivelse af oplysninger.

TET har af hensyn til sin efterfølgende bearbejdning og samstilling af data behov for at indsamle oplysningerne via udfyldelse af den vedlagte Excel-skabelon, som i tilsynets regi benævnes "Infrastrukturoversigten". Skabelonen omfatter det minimum af information, som TET finder tilstrækkeligt til at opnå et overordnet overblik over, hvad der aktuelt findes af netværk, domæner og servere samt hvilke it-systemer, der afvikles på disse.

TET skal på den baggrund anmode [PET / FE / CFCS / PPNR] om at udfylde vedlagte Infrastrukturoversigt (se vedhæftede bilag A) med oplysninger om samtlige netværk og samtlige servere, både virtuelle og fysiske, der findes i alle tjenestens it-miljøer, samt fremsende disse til tilsynet senest den 1. maj [år], [PET-lovens § 20, stk. 3 / FE-lovens § 17, stk. 3 / CFCS-lovens § 22, stk. 3].

Med venlig hilsen
Tilsynet med Efterretningstjenesterne

v/[Navn]
[Titel]

Borgergade 28, 1
DK-1300 København K
t 25 50 10 34
www.tet.dk

Vejledning til udfyldelse af TETs infrastrukturoversigt

INDLEDNING OG FORMÅL

TETs infrastrukturoversigt er opdelt i to separate faneblade indeholdende en netværksliste og en serverliste, som samlet har til formål at kortlægge den fulde it-infrastruktur i henholdsvis PET, FE, CFCS og PPNR. Sammenstilling og vurdering af informationerne fra netværkslisten (se fanen A. Netværkslisten) og serverlisten (se fanen B. Serverlisten) giver TET en grundlæggende forståelse for opbygningen og sammenhængen af it-infrastrukturen i PET, FE, CFCS og PPNR. TET udarbejder årligt på baggrund af bland andet infrastruktuoversigten en liste over systemer i PET, FE, CFCS og PPNR, som danner grundlag for tilsynets årlige risiko- og væsentlighedsvurderinger af tjenesterne, centret og enheden. På baggrund af risiko- og væsentlighedsvurderingerne fastlægger TET sine årlige kontrolplaner.

Netværkslisten kan sammen med serverlisten anvendes til krydstjek og validering af, hvorvidt der findes

- netværk, miljøer eller VLANs, som TET ikke allerede er bekendt med,
- netværk, miljøer eller VLANs, hvortil der ikke er oplyst om tilknyttede servere eller systemer,
- systemer eller servere der er tilknyttet netværk, miljøer eller VLANs, der ikke figurerer på netværkslisten,
- servere, som ikke er en del af et it-system,
- systemer og/eller servere, som tilsynet endnu ikke har kendskab til, og
- systemer og/eller servere der er tilkommet eller bortfaldet siden seneste opdatering.

Infrastrukturoversigten giver endvidere TET mulighed for at krydstjekke og validere, om de servere, der fremgår af serverlisten, svarer til de servere, som i praksis kører i PET, FE, CFCS og PPNRs it-miljøer.

TET har valgt årligt at kortlægge PET, FE, CFCS og PPNRs it-infrastrukturer i denne Excel-skabelon, som omfatter de oplysninger, som tilsynet aktuelt skønner nødvendige for at opnå et overblik over, hvad der aktuelt findes af netværk og domæner samt hvilke systemer, der findes på disse.

TETs proces for it-kortlægning er nærmere beskrevet i tilsynets standarder, som findes her www.tet.dk.

VEJLEDNING TIL DE ENKELTE KOLONNER PÅ FANEBLADET A. NETVÆRKSLISTEN

Kaldenavn for it-miljø/ sikkerhedskontekst	I denne kolonne angives det/de kaldenavn(e), det enkelte it-miljø/sikkerhedskontekst i det daglige benævnes med. Et it-miljø/sikkerhedskontekst er i denne sammenhæng defineret som en gruppering af et eller flere VLANs på et fysisk netværk, der tilsammen udgør et separat it-miljø, f.eks. et produktions-, test-, indhentnings-, behandlings- eller udviklingsmiljø.
Navn på fysisk netværk	I denne kolonne angives navnet på det fysiske netværk. Et fysisk netværk er i denne sammenhæng defineret som lokalnetværk (LAN) bestående af netværkskomponenter forbundet med kabler (fiber, UTP, STP eller lignende) afgrænset af f.eks "airgaps" eller dioder.
VLANs i it-miljø/netværkskontekst	I denne kolonne angives, hvilke VLANs der indgår i det enkelte it-miljø/sikkerhedskontekst.
Netværkets klassifikation	I denne kolonne angives den højeste klassifikation, som det aktuelle netværk er godkendt til.
Kort beskrivelse at it-miljøets/ sikkerhedskontekstens anvendelse/ funktion/rolle	I denne kolonne angives en kort beskrivelse af, hvad it-miljøet/sikkerhedskonteksten anvendes til, f.eks. testmiljø for intern IT eller anvendes til at teste nye systemer, der anvendes udelukkende anonymiserede oplysninger i forbindelse med test.

VEJLEDNING TIL DE ENKELTE KOLONNER PÅ FANEBLADET B. SERVERLISTEN

Navn	I denne kolonne angives navnet på serveren. Alle fysiske og virtuelle servere på alle netværk skal angives i denne kolonne. Findes en server med det samme navn i tre forskellige it-miljøer/sikkerhedskontekster, skal serverens navn optræde tre gange i denne kolonne. Navnet på serveren angives enten som NETBIOS-navn eller DNS-navn.
Systemnavn	I denne kolonne angives det eller de forretningssystemer, som serveren udgør en del af. Systemnavne indført i denne kolonne kommer til at danne grundlaget for TETs årlige risiko- og væsentlighedsvurdering samt kontrolplan for det kommende år. Det er derfor vigtigt, at systemnavnene, der anvendes, er konsistente med de systemnavne, som anvendes i f.eks. en retentionsplan, lister over aktiver, dokumentationssystemer

	eller generelt i forretningen. Det er ligeledes vigtigt, at alle systemer, som serveren er en del af, påføres listen. Anvendes en database- og en filserver f.eks. i system A og system B, anføres begge systemer ud for begge servere. Servere, der håndterer f.eks. print, shares for installationssoftware, Active Directory, terminalservere, Citrix-infrastruktur, antivirus, DHCP, DNS, VCenter, certifikatinfrastruktur, jumpservere, loadbalancing, administrationservere til netværkskomponenter SAN eller lignende, anføres i denne kolonne som "Infrastruktur", og en kort beskrivelse af serverens funktion angives i kolonnen "Kort beskrivelse af serverens funktion/rolle". Kan serveren ikke tilknyttes til et system eller kategoriseres som infrastruktur, noteres N/A og en forklarende beskrivelse tilføjes under "Kort beskrivelse af serverens funktion/rolle".
Kaldenavn for it-miljø/ sikkerhedskontekst	I denne kolonne angives, hvilket it-miljø/sikkerhedskontekst serveren er tilsluttet. Det er vigtigt, at de kaldenavne, der anvendes i denne kolonne, er entydige igennem hele dette skema og konsistente med netværkslisten (i vejledning til Netværksoversigten findes yderligere beskrivelse af begrebet it-miljø/ sikkerhedkontekst), således at TET kan danne sig et overblik over hvilke servere/systemer, der findes i de enkelte it-miljøer/sikkerhedskontekster. Er én server tilsluttet flere it-miljøer/sikkerhedskontekster, angives de alle.
VLAN ID	I denne kolonne angives ID på det VLAN, som serveren er tilsluttet i det aktuelle it-miljø/sikkerhedskontekst. Er der ikke anvendt VLAN-teknologi i det it-miljø/sikkerhedskontekst, som serveren er tilsluttet, angives dette som "VLAN ikke anvendt".
DNS-domæne	I denne kolonne angives, om serveren er en del af et DNS-domæne. Er det tilfældet, skal det angives med DNS-navnet (f.eks. statens-it.local) som N/A eller workgroup-navnet.
Primær software	I denne kolonne angives serverens primære software-produkt. Hvis serveren er en databaseserver, kan det primære software produkt f.eks. være MSSQL, Oracle, MySql, MongoDB eller lignende. Hvis serverens primære funktion er baseret på en funktion, der er indbygget i operativsystemet, kan der f.eks, anføres DNS, print, fildeling, DFS eller lignende, afhængig af hvilken service serveren udbyder.
Kort beskrivelse af serverens funktion/rolle	I denne kolonne angives en forklaring og/eller en bemærkninger vedrørende serverens funktion, data eller andre relevante forhold, der kan bidrage til forståelsen af serverens rolle i tjenestens it-miljø.

A. Netværksliste

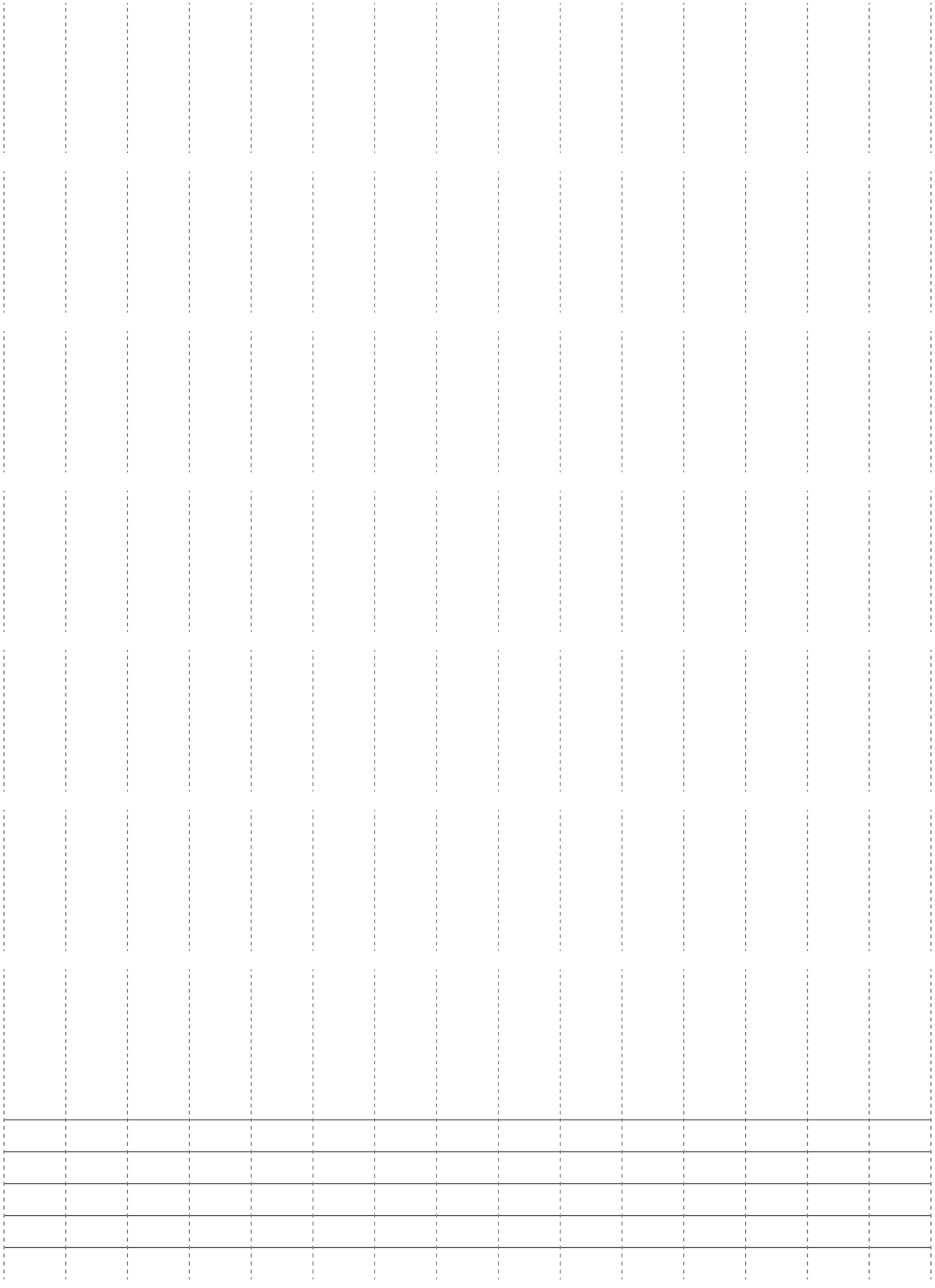
KALDENAVN FOR IT-MILJØ/SIKKERHEDS-KONTEKST	NAVN PÅ FYSISK NETVÆRK	VLANS I IT-MILJØ/ SIKKERHEDS-KONTEKST	NETVÆRKETS KLASSIFIKATION	KORT BESKRIVELSE AT IT-MILJØETS/ SIKKERHEDSKONTEKSTENS ANVENDELSE/ FUNKTION/ROLLE
***Eksempel** - DMZ*	*DMZ-net*	*242*	*IKL*	*Udstiller eksterne services som authentikering og mailservices*
***Eksempel** - Lukket net, HEM-NET*	*HEM-FiberNet*	*36, 42, 43, 46, 47, 48, 49*	*HEM*	*Anvendes til afsluttende analyse af sager samt generel administration*
***Eksempel** - DEV-net, sandkassen, udviklernet*	*HEM-FiberNet*	*568,570, 599*	*HEM*	*Anvendes i forbindelse med udvikling og indledende funktionstest af egenudviklet software, samt indledende test af kommecielle systemer*
***Eksempel** - STAG-net, Staging*	*HEM-FiberNet*	*663, 664, 665*	*HEM*	*Anvendes til afsluttende installationstest, der testes udelukkende med anonymiseret testdata.*
***Eksempel** - Åbent net*	*IKL-UTPNet*	*250, 251, 260*	*IKL*	*Anvendes af brugere til ikke operativ mailkommunikation med eksterne aktører.*
***Eksempel** - Opdateringsnet, Gæstenet*	*WLAN-internet*	*128-136*	*IKL*	*Anvendes til gæster der ønsker at tilslutte et medbragt device, eller medarbejdere der vil opdatere telefoner eller tablets, netværket giver kun adgang til internet*

B. Serverliste

NAVN	SYSTEMNAVN	KALDENAVN FOR IT-MILJØ/SIKKER-HEDSKONTEKST	VLAN ID	DNS-DOMÆNE	PRIMÆR SOFT-WARE	KORT BESKRIVELSE AF SERVERENS FUNKTION/ ROLLE
Servernavn (NETBIOS eller DNS)	**Forretnings-system(er) som serveren udgør en del af.**	**Angiv kaldenavn på det it-miljø/ sikkerhedkontekst serveren er en del af**	**Angiv ID på det VLAN serveren er tilsluttet**	**Er serveren en del af et DNS-domæne, angiv dette, ellers angives N/A eller workgroup**	**Serverens primære software-produkt.**	**Forklaringer og/ eller bemærkninger vedrørende serverens funktion, data eller andre relevante forhold, der kan bidrage til forståelsen af serverens rolle**
***Eksempel** - ServerX*	*Infrastruktur*	*HEM-NET*	*42*	*HEMDOM.local*	*Windows AD*	*Brugerdatabase i form af Microsoft Active Directory, anvendes i forbindelse med validering af brugere.*
***Eksempel** - ServerY*	*Hobbit / ComBIT*	*HEM-NET*		*N/A*	*Datadiode Modtager*	*Modtager beskeder via mail fra IKL-NET til HEM-NET netværk.*
***Eksempel** - ServerZ*	*Historisk-arkiv*	*HEM-NET*	*36*	*HEMDOM.local*	*ScanArkiv 4.0*	*Indeholder alle scannede dokumenter, og OCR genkender alle PDF filer.*
***Eksempel** - ServerQ*	*Infrastruktur og System E, D og G*	*HEM-NET*	*46*	*HEMDOM.local*	*Splunk 5.6*	*Splunk anvendes til at søge i logfiler leveret fra systemerne E, D og G.*
***Eksempel** - ServerR*	*Analysesystem*	*HEM-NET*	*43*	*HEMDOM.local*	*Linux*	*Filserver for Linux-baseret analysesystem*
***Eksempel** - ServerS*	*Hobbit / ComBIT*	*Åbent net*	*128*	*N/A*	*Datadiode Afsender*	*Afsender beskeder via mail fra IKL-NET til HEM-NET netværk.*
***Eksempel** - ServerT*	*Infrastruktur*	*HEM-NET*	*42*	*HEMDOM.local*	*Windows*	*Filserver på HEM-NET - Hoster alle afdelingsdrev.*
***Eksempel** - ServerU*	*System E, D og G*	*HEM-NET*	*46*	*HEMDOM.local*	*MS SQL 2019*	*Operative data, data ligger i 3 forskellige databaser og læses / redigeres via systemerne E, D og G*

Systemliste [år]

KILDE-ANGIVELSE					SYSTEMNAVN	BESKRIVELSE	NETVÆRK/ KONTEKST/MILJØ	PÅFØRT SYSTEMLISTE	RELEVANS SCORE	RELEVANS VURDERING	NAVNEÆNDRING
Infrastrukturoversigt (år)	Modtaget dokumentation (år)	Asset management (år)	Udfundet ESDH (år)	Ledelsessystem (år)	Her angives navn på systemet	Her angives en kort beskrivelse af systemet	Her angives hvilket miljø, kontekst eller netværk systemet afvikles på. Afvikles systemet på flere miljøer angiv hvilke	Her angives navn på hvilken systemliste, systemet første gang blev påført	Systemer inddeles i 3 kategorier: 3. Ikke relevante systemer 2. Relevante systemer 1. Relevante systemer der anbefales til kontrol	Eventuel skriftlig begrundelse eller kommentar til kategori indeling.	Her angives om et eksisterende system har fået nyt navn samt systemet seneste navne
				x	***Eksempel*** *- MAILMAN*	*Mailsystem* *- anvendes af alle brugere på HEM-NET til at sende mails internt*	*HEM-NET*		*2*		*Nej*
	x				***Eksempel*** *- GOLIAT*	*Anvendes til at registrere aflytninger, bla. formalia vedr. oprettelse og nedtagning*	*HEM-NET*		*1*	*Dette system er komplekst og indeholder manuelle arbejdsgange, desuden indeholder det tilsyneladende store mængder af ældre personoplysninger*	*Ja, DAVID*



BEMÆRKNINGER

RISIKOSCORE PER LOVHJEMMEL

0-5 = Lav risiko
6-12 = Begrænset risiko
13-19 = Middel risiko
20-26 = Høj risiko

TETS KONTROL GIVET ANLEDNING TIL BEMÆRKNINGER?

Nej eller *N/A* = 0
Ja, mindre væsentlige bemærkninger ved tidligere kontrol (≤ 3 år) = 1
Ja, mindre væsentlige bemærkninger ved seneste kontrol = 2
Ja, væsentlige bemærkninger ved tidligere kontrol (kritisabelt/overordentligt kritisabelt) (≤ 3 år) = 3
Ja, væsentlige bemærkninger ved seneste kontrol (kritisabelt/overordentligt kritisabelt) = 5

TETS KONTROL VIST FEJL?

Nej eller *N/A* = 0
Ja, mindre fejl ved tidligere kontrol (≤ 3 år) = 1
Ja, mindre fejl ved seneste kontrol = 2
Ja, lovbrud ved tidligere kontrol (≤ 3 år) = 3
Ja, lovbrud ved seneste kontrol = 5

TETS SENESTE KONTROL?

≤ 1 år eller *N/A* = 0
2 år = 1
3 år = 2
≥ 4 år = 3

TET FORETAGET KONTROL?

Ja eller *N/A* = 0
Nej = 2

HAR INTERNE KONTROL VIST FEJL?

Nej eller *N/A* = 0
Ja, mindre fejl = 1
Ja, lovbrud = 2

INTERN KONTROL?

Ja, tilfredsstillende eller *N/A* = 0
Ja, men ad hoc/decentralt/ikke tilfredsstillende = 1
Nej eller Ukendt = 3

INTERN LEGALITETSSIKRING?

Ja, inkl. fast praksis for juridisk godkendelse eller *N/A* = 0
Ja, dog ikke fast praksis for juridisk godkendelse = 1
Nej eller Ukendt = 3

LOGNING OG RETTIGHEDSSTYRING?

Ja, i relevant omfang eller *N/A* = 0
Ja, i mindre relevant omfang = 1
Nej = 2
Ukendt = 3

PLACERING AF BEHANDLING?

Central, og TET har egenhændig adgang eller *N/A* = 0
Central, men TET har ikke egenhændig adgang = 1
Decentral = 2
Ukendt = 3

PROCES FOR BEHANDLING?

Automatiseret eller *N/A* = 0
Delvist automatiseret = 1
Manuel = 2
Ukendt = 3

HAR INTERNE KONTROL VIST FEJL?

Nej eller *N/A* = 0
Ja, mindre fejl = 1
Ja, lovbrud = 2

DATAKVALITET?

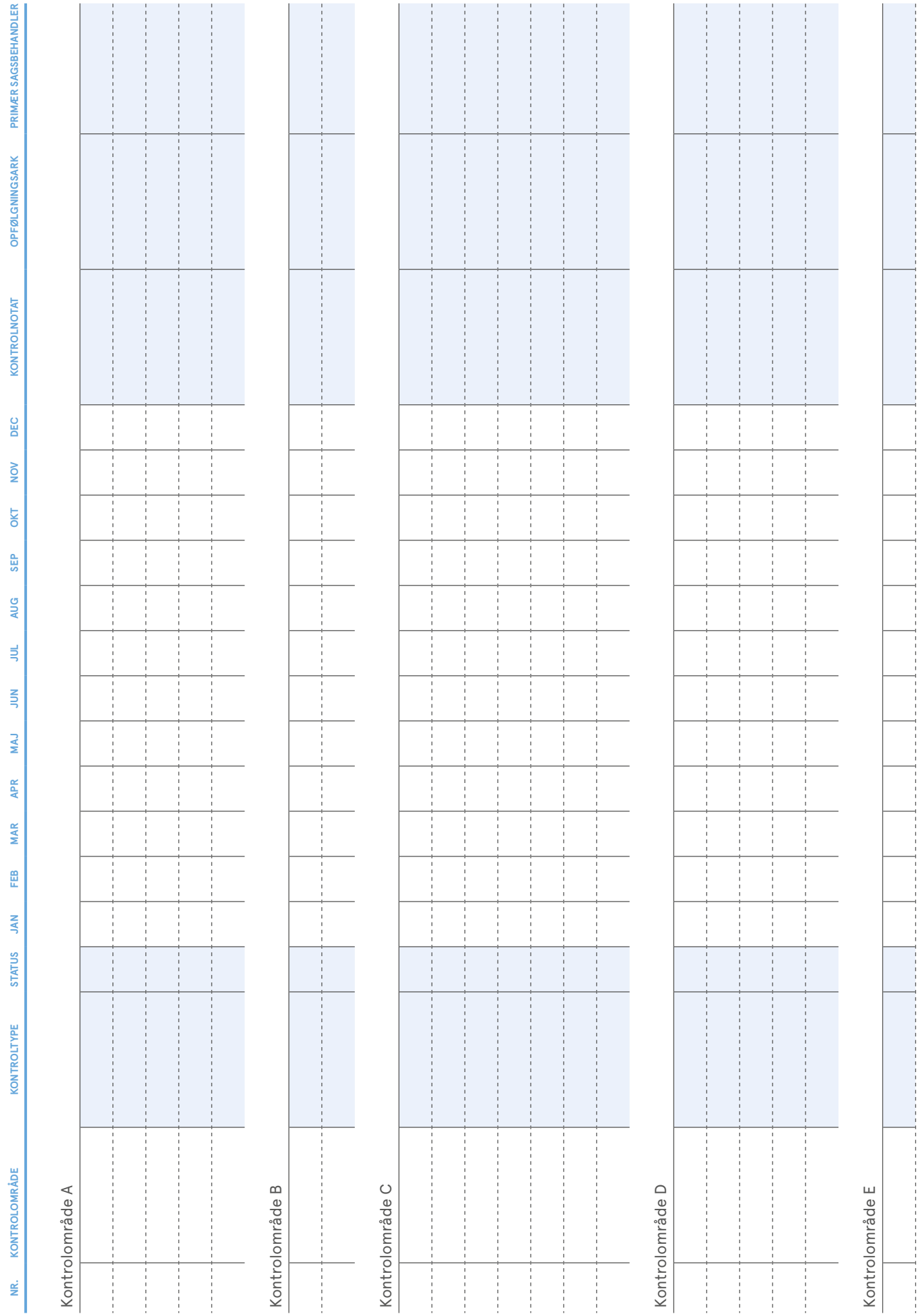
Struktureret eller *N/A* = 0
Ustruktureret = 2
Ukendt = 3

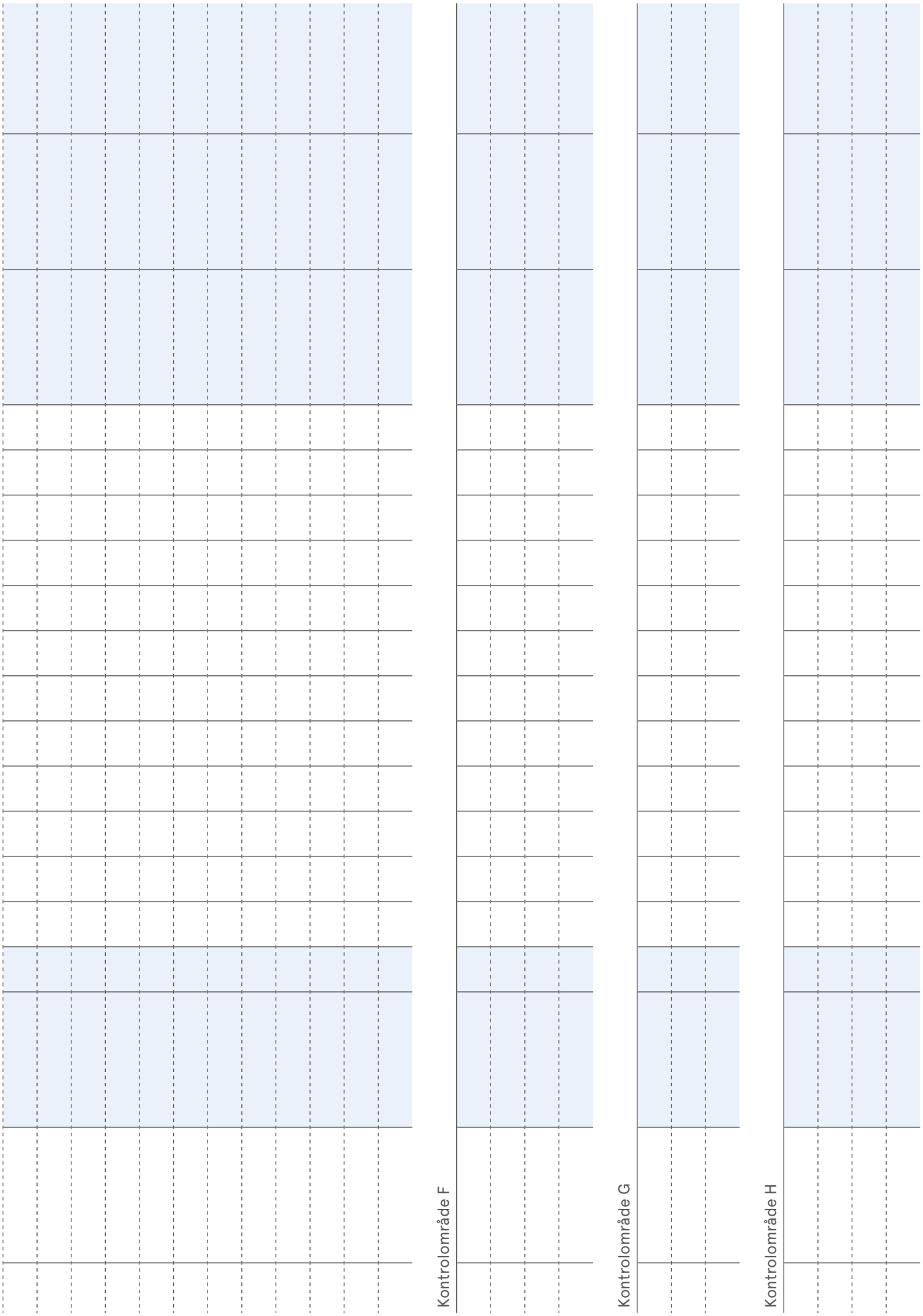
LOVREGLER	SYSTEM	KONTROLOMRÅDE
Lovbestemmelse A	System A	Kontrolområde A
Lovbestemmelse B		
Lovbestemmelse C		
Lovbestemmelse D		
Lovbestemmelse E		
Lovbestemmelse A	System B	
Lovbestemmelse B		
Lovbestemmelse C		
Lovbestemmelse D		
Lovbestemmelse E		
Lovbestemmelse A	System A	Kontrolområde B
Lovbestemmelse B		
Lovbestemmelse C		
Lovbestemmelse D		
Lovbestemmelse E		
Lovbestemmelse A	System B	
Lovbestemmelse B		
Lovbestemmelse C		
Lovbestemmelse D		
Lovbestemmelse E		

Kontrolområde C	System A	Lovbestemmelse A															
		Lovbestemmelse B															
		Lovbestemmelse C															
		Lovbestemmelse D															
		Lovbestemmelse E															
	System B	Lovbestemmelse A															
		Lovbestemmelse B															
		Lovbestemmelse C															
		Lovbestemmelse D															
		Lovbestemmelse E															
Kontrolområde D	System A	Lovbestemmelse A															
		Lovbestemmelse B															
		Lovbestemmelse C															
		Lovbestemmelse D															
		Lovbestemmelse E															
	System B	Lovbestemmelse A															
		Lovbestemmelse B															
		Lovbestemmelse C															
		Lovbestemmelse D															
		Lovbestemmelse E															

Øvrige systemer
(systemer/databaser der umiddelbart vurderes ikke at skulle være underlagt TETs almindelige kontrol, men alene være omfattet af TETs tekniske undersøgelser af adgangsrettigheder mv.)

SYSTEM	BESKRIVELSE	SENESTE INSPEKTION
System A		
System B		
System C		
System D		
System E		
System F		


NR.
KONTROLOMRÅDE
KONTROLTYPE
STATUS
JAN
FEB
MAR
APR
MAJ
JUN
JUL
AUG
SEP
OKT
NOV
DEC
KONTROLNOTAT
OPFØLGNINGSARK
PRIMÆR SAGSBEHANDLER
Kontrolområde A
Kontrolområde B
Kontrolområde C
Kontrolområde D
Kontrolområde E


Kontrolområde F
Kontrolområde G
Kontrolområde H

[Politiets Efterretningstjeneste/
Forsvarets Efterretningstjeneste/
Center for Cybersikkerhed/
Politiets PNR-enhed]

Tilsynet med Efterretningstjenesterne

Dato:
Sagsbeh.: [Navn 1] [Navn 2]
Sagsnr.: [Sagsnr.]
Dok.: [Dokumentnr.]

Indledende høring samt anmodning om opstartsmøde vedrørende kontrol af [kontrolobjekt] i [år (Pxx-xx / Fxx-xx / Cxx-xx / Rxx-xx)]

TET besluttede på møde den [dato], at der i [år] skal foretages kontrol af [kontrolobjekt].

I den forbindelse skal TET anmode om et opstartsmøde i **uge [ugenummer]**. TET skal endvidere anmode om, at [PET / FE / CFCS / PPNR] indleder opstartsmødet med en demonstration af systemet.

Til brug for forberedelsen heraf skal TET endvidere anmode om, at [PET / FE / CFCS / PPNR] udarbejder og fremsender det nedenfor beskrevne materiale, jf. [PET-lovens § 20, stk. 3 / FE-lovens § 17, stk. 3 / CFCS-lovens § 22, stk. 3], senest mandag **den [mandag to uger før opstartsmødet]** ved arbejdstids ophør:

a. Materiale til brug for opstartsmøde:

   TET planlægger, tilpasser og gennemfører sine kontroller af [PET / FE / CFCS / PPNR] på baggrund af løbende, årlige risiko- og væsentlighedsvurderinger af [tjenestens / centrets / enhedens] systemer og arbejdsprocesser. Det er en forudsætning for gennemførelsen af vurderingerne og den efterfølgende kontrol, at TET opnår et detaljeret kendskab til systemerne herunder deres tekniske opbygning og funktioner, data i systemet og de konkrete processer og arbejdsgange i forbindelse hermed.

   Med sigte på at opnå en effektiv og målrettet kontrol ønsker TET at opbygge teknisk viden om et system forud for en planlagt kontrolaktivitet. TET ønsker endvidere at ensarte og strukturere sin indsamling af teknisk viden for de enkelte systemer/databaser på en måde, som bedre kan danne grundlag for den løbende og oftest tilbagevendende tekniske dialog om systemerne.

Borgergade 28, 1
DK-1300 København K
t 25 50 10 34
www.tet.dk

TET ønsker på den baggrund at indsamle og dokumentere sin viden i henholdsvis et informationsark (se vedhæftede bilag A) og en teknisk, dataflow-orienteret systemtegning (se eksempler i vedhæftede bilag B) for hvert system, der indgår i tilsynets kontrol. Det er TETs erfaring, at begge produkter er nødvendige for at skabe det bedste fundament for forståelse af komplekse systemer og tilhørende arbejdsgange.

Det tilstræbes, at der kun udfyldes ét informationsark per system, men i tilfælde, hvor der er tale om komplekse systemer, som består af et antal selvstændige delsystemer, kan det give bedst mening at udfylde et informationsark per delsystem. Der udarbejdes dog stadig kun ét flow-baseret systemdiagram, hvor alle delsystemerne indgår.

TET skal således anmode om følgende:

- Udfyldt informationsark i Word-format vedrørende [kontrolobjekt] (se vedhæftede bilag A)
- Flow-baseret systemdiagram i Visio-format

For at illustrere den ønskede detaljegrad for systemtegningen har TET til inspiration udarbejdet fiktive eksempler på systemtegninger i et Visio-ark. (se vedhæftede bilag B).

TET skal endvidere anmode om følgende:

- Henvisning til relevant særlovgivning, der måtte finde anvendelse for kontrolområdet i form af bekendtgørelser og/eller cirkulærer
- Henvisning til [PETs / FEs / CFCS' / PPNRs] eventuelle interne retningslinjer, vejledninger mv., der finder anvendelse for kontrolområdet

Såfremt anmodningen, herunder de enkelte elementer i bilag A [og bilag B], giver anledning til spørgsmål, skal TET anmode [PET / FE / CFCS / PPNR] om snarest at kontakte tilsynet med henblik på afklaring heraf.

Endelig skal TET anmode [PET / FE / CFCS / PPNR] om at sikre, at samtlige mødedeltagere er godkendte til at kunne deltage i drøftelsen af ovenstående emne.

Såfremt TET ikke modtager svar eller anmodning om forlængelse fra [PET / FE / CFCS / PPNR] inden udløbet af svarfristen, vil kontroller blive afsluttet på det foreliggende grundlag.

Med venlig hilsen
Tilsynet med Efterretningstjenesterne

v/[navn]
[Titel]

Informationsark for PETs it-system [kontrolobjekt]

UDFYLDES AF TET

Dato for opstartsmøde	Mødedeltagere fra TET	Mødedeltagere fra PET
[DATO]	[NAVNE]	[NAVNE]

Vejledning til udfyldelse af skema (Word) og tilhørende flow-baseret systemdiagram (Visio)

Skemaet indeholder tekniske og juridiske spørgsmål. Teksten i firkantede parenteser i skemaet nedenfor tjener som vejledning og skal fjernes i forbindelse med udfyldelse. Felter udfyldes med N/A hvis de ikke er relevante for det pågældende system.

Såfremt systemet består af flere selvstændige delsystemer, hvor det skønnes at medføre uhensigtsmæssig kompleksitet eller uoverskuelighed at samle alle informationer i et enkelt skema, udfyldes i stedet ét skema pr. delsystem. Diagramtegningen bør imidlertid stadig udarbejdes som én samlet oversigt.

Formålet med diagramtegningen (Visio) er at skabe et overblik, der både beskriver selve systemet, men også samtidig illustrerer dataflow fra data skabes eller indsamles til det lagres eller overføres til andre systemer. Diagramtegningen skal derfor indeholde:

- Hvilke data, der tilflyder, behandles og forlader systemet
- Hovedkomponenter og datalagringspunkter (f.eks. databaser, filshares eller mailsystemer) i systemet
- Flow-pile, der viser, hvilke veje og retning data flyder gennem systemet

UDFYLDES AF PET (BOKS 1-9)

1. Overordnet beskrivelse af systemet

Formål med systemet	[Beskrivelse af hvad systemet anvendes til, herunder de primære funktioner og dets operative formål]

2. Stamdata for systemet

TEKNISKE SPØRGSMÅL

Systemnavn(e)	[Angiv systemets kaldenavn(e)]
Anvendte produkter/producenter	[F.eks. MS Exchange 2010, Apache Tomcat v7.0, udviklet af NNIT etc. samt det aktuelle versionsnummer]
Idriftsættelsesdato	[Alternativt angiv måned og år for idriftsættelse]
Driftsansvarlig	[Angiv hvilken afdeling, sektion eller f.eks. anden ekstern myndighed, der er ansvarlig for den daglige drift af systemet]
Erstatning/opgradering	[Hvis systemet erstatter eller er en versionsopgradering af et eksisterende system, angiv da det tidligere navn]
Dataejer	[Angiv dataejer for systemet]
Kopier i andre it-miljøer	[Findes der hele eller delvise kopier af systemet i andre it-miljøer end drifts-/produktionsmiljøet? F.eks. udviklings-, test- eller staging-miljøer?]
Planlagte ændringer	[Såfremt der er planlagt større ændringer for systemet eller brugen heraf i indeværende år, bedes disse beskrevet]

3. Systemets it-infrastruktur

TEKNISKE SPØRGSMÅL	
Netværk/kontekst og domæne	[Kaldenavn på netværket/konteksten, som systemet er tilsluttet]
Servere(navngivne) og deres primære roller	[F.eks. applikations-, database-, filserver-, share etc.]
Klienttype(r)	[Webbrowser eller applikation, anfør weblink eller forklar hvorledes systemet tilgås/klient opstartes]
Datakilder til systemet	[F.eks. system hos anden myndighed, indhentningssystem, ESDH etc.]
Dataformater, der overføres til systemet	[F.eks. PCAP, ZIP, XML, CSV etc.]
Datamængder, der overføres til systemet	[Estimat i relevant format f.eks. poster, MB, GB, antal dokumenter etc.]
Modtagere af data fra systemet	[F.eks. system hos anden myndighed, anden afdeling, ESDH, intern database etc.]
Dataformater, der overføres fra systemet	[F.eks. PCAP, ZIP, XML, CSV etc.]
Datamængder, der overføres fra systemet	[Estimat i relevant format f.eks. poster, MB, GB, antal dokumenter etc.]
Datalagringspunkter	[Alle databaser (navneliste), filsystemer, eksterne medier eller øvrige placeringer, hvor data lagres (evt. midlertidigt) af systemet eller daglig anvendelse af systemet]

4. Bruger- og rettighedsstyring

TEKNISKE SPØRGSMÅL	
Brugere af systemet	[Hvilke grupper af brugere anvender systemet, f.eks. afdelinger, sektioner, eksterne]
Antal brugere (læserettigheder)	[Brugere eller brugergrupper, der kun kan læse data]
Antal brugere (skriverettigheder)	[Brugere eller brugergrupper, der kan opdatere (skrive) data]
Rettighedsstyringssystem	[Hvilket system anvendes til styring af brugerrettigheder i systemet? F.eks. Active Directory, intern brugerdatabase, en kombination af flere systemer, etc.]

JURIDISKE SPØRGSMÅL	
Hvordan har PET sikret, at det kun er de personer, som autoriseres hertil, der har adgang til de oplysninger om fysiske og juridiske personer, der behandles i systemet, jf. PET-sikkerhedsbekendtgørelsens §§ 10 og 11?	[Spørgsmålet skal ses i sammenhæng med de tekniske spørgsmål ovenfor]
Foretager PET kontrol med afviste adgangsforsøg, jf. PET-sikkerhedsbekendtgørelsens § 16?	[Ja/Nej. Hvis ja, angiv supplerende oplysninger]

5. Sletning af data i praksis

TEKNISKE SPØRGSMÅL	
Initiering af sletning	[Hvem sikrer, at der sker en rutinemæssig sletning/oprydning i data i overensstemmelse med eventuelle slettefrister?]
Gennemførsel af sletning	[Sker sletningen af data i systemet manuelt eller automatisk f.eks. via scripts? Ved manuel sletning, hvem er da udførende?]

Hvordan angives det for sletning relevante indhentningstidspunkt/indførselstidspunkt/alder/e.l. på data i systemet?	[Sker angivelsen af alder på data eksempelvis ved felt med creation date i en database eller ved oprettelsestidspunkt i metadata på filer?]
Frekvens	[Hvor ofte foretages rutinemæssig sletning/oprydning af data i systemet?]

JURIDISKE SPØRGSMÅL

Er systemet en elektronisk journal, jf. PET-bekendtgørelsens § 1, stk. 1?	[Ja/Nej Spørgsmålet skal ses i sammenhæng med det tekniske spørgsmål "Hvordan angives det for sletning relevante indhentningstidspunkt/indførselstidspunkt/alder/e.l. på data i systemet?" ovenfor]
Er systemet en database, jf. PET-bekendtgørelsens § 2, stk. 1?	[Ja/Nej]
Såfremt systemet er en database, hvilken slettefrist har PET så fastsat herfor, jf. PET-bekendtgørelsens § 2, stk. 2?	[Angiv slettefristen, hvis der er tale om en database, jf. PET-bekendtgørelsens § 2, stk. 1. Spørgsmålet skal ses i sammenhæng med det tekniske spørgsmål "Hvordan angives det for sletning relevante indhentningstidspunkt/indførselstidspunkt/alder/e.l. på data i systemet?" ovenfor]
Er systemet et transitsystem, dvs. at systemet hverken er en elektronisk journal, jf. PET-bekendtgørelsens § 1, stk. 1, eller en database, jf. PET-bekendtgørelsens § 2, stk. 2?	[Ja/Nej Spørgsmålet skal ses i sammenhæng med det tekniske spørgsmål "Hvordan angives det for sletning relevante indhentningstidspunkt/indførselstidspunkt/alder/e.l. på data i systemet?" ovenfor]

6. Backup og restore

TEKNISKE SPØRGSMÅL

Backup af data	[Tages der backup af data i systemet?]
Data retention	[Hvor langt tilbage er det muligt at genskabe data?]
Restore af data	[Hvordan sikres det, at data, der er slettet som følge af revision ikke fejlagtigt genskabes?]

7. Logning af brugerhandlinger

TEKNISKE SPØRGSMÅL

Brugerhændelseslogning	[Sker der logning af de handlinger/transaktioner, som brugerne foretager?]
Hændelsestyper	[Hvilke typer af brugerhandlinger logges? F.eks. læsning, skrivning, ændring, sletning, søgning, søgeresultat etc.]
Adgang til hændelseslog	[Hvor og hvordan tilgås systemets brugerhændelseslogs]
Søgning i hændelseslogs	[Hvorledes kan søgning i hændelseslogs ske? Kan denne søgning tidsafgrænses?]

JURIDISKE SPØRGSMÅL

Har PET etableret en logning, som mindst indeholder oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium, jf. PET-sikkerhedsbekendtgørelsens § 17, stk. 1, 1. pkt.?	[Ja/Nej. Hvis ja, angiv supplerende oplysninger. Spørgsmålet skal ses i sammenhæng med det tekniske spørgsmål "Hændelsestyper" ovenfor]
Hvor længe opbevares loggen, jf. PET-sikkerhedsbekendtgørelsens § 17, stk. 1, 2. og 3. pkt.?	[Angiv periode for opbevaring af logdata]

8. Dokumentation og vejledninger

TEKNISKE SPØRGSMÅL	
Brugervejledning til søgning	[Vedlæg kopi eller angiv placeringen af eksisterende brugervejledninger vedrørende søgning i systemet]
Brugervejledning til systemet	[Vedlæg kopi eller angiv placeringen af eksisterende brugervejledninger vedrørende brug af systemet]
Anden systemdokumentation	[Vedlæg kopi eller angiv placeringen af eksisterende dokumentation vedrørende systemets opbygning og funktionalitet]
Detailskema, såfremt PET vurderer, at der er tale om et RM-system	[Vedlæg kopi eller angiv placeringen af eksisterende detailskema vedrørende systemet]

9. Generelle spørgsmål vedrørende behandlingssikkerhed

JURIDISKE SPØRGSMÅL	
Hvilke tekniske og organisatoriske foranstaltninger har PET truffet mod, at oplysninger om fysiske og juridiske personer hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med lov om PET, jf. PET-sikkerhedsbekendtgørelsens § 3?	[Angiv tekniske og organisatoriske foranstaltninger]
Har PET fastsat nærmere interne bestemmelser om sikkerhedsforanstaltninger, jf. PET-sikkerhedsbekendtgørelsens § 4, stk. 1? Og hvornår har PET i så fald senest gennemgået disse, jf. PET-sikkerhedsbekendtgørelsens § 4, stk. 2?	[Ja/Nej. Hvis ja, angiv supplerende oplysninger]
Har PET givet instruktion til de medarbejdere, som behandler oplysninger om fysiske og juridiske personer, jf. PET-sikkerhedsbekendtgørelsens § 5?	[Ja/Nej. Hvis ja, angiv supplerende oplysninger]
Har PET truffet forholdsregler på steder, hvor der foretages behandling af oplysninger om fysiske og juridiske personer, med henblik på at forhindre uvedkommendes adgang til oplysningerne, jf. PET-sikkerhedsbekendtgørelsens § 7?	[Ja/Nej. Hvis ja, angiv supplerende oplysninger]

Såfremt PET har udarbejdet dokumentation, som besvarer ovenstående spørgsmål vedrørende behandlingssikkerhed, anmodes tjenesten om tillige at fremsende dette.

UDFYLDES AF TET

Eventuelle opfølgende spørgsmål til opstartsmøde

NUMMER	SPØRGSMÅL	SVAR
1		
2		
3		

Informationsark for FEs it-system [kontrolobjekt]

UDFYLDES AF TET

Dato for opstartsmøde	Mødedeltagere fra TET	Mødedeltagere fra FE
[DATO]	[NAVNE]	[NAVNE]

Vejledning til udfyldelse af skema (Word) og tilhørende flow-baseret systemdiagram (Visio)

Skemaet indeholder tekniske og juridiske spørgsmål. Teksten i firkantede parenteser i skemaet nedenfor tjener som vejledning og skal fjernes i forbindelse med udfyldelse. Felter udfyldes med N/A hvis de ikke er relevante for det pågældende system.

Såfremt systemet består af flere selvstændige delsystemer, hvor det skønnes at medføre uhensigtsmæssig kompleksitet eller uoverskuelighed at samle alle informationer i et enkelt skema, udfyldes i stedet ét skema pr. delsystem. Diagramtegningen bør imidlertid stadig udarbejdes som én samlet oversigt.

Formålet med diagramtegningen (Visio) er at skabe et overblik, der både beskriver selve systemet, men også samtidig illustrerer dataflow fra data skabes eller indsamles til det lagres eller overføres til andre systemer. Diagramtegningen skal derfor indeholde:

- Hvilke data, der tilflyder, behandles og forlader systemet
- Hovedkomponenter og datalagringspunkter (f.eks. databaser, filshares eller mailsystemer) i systemet
- Flow-pile, der viser, hvilke veje og retning data flyder gennem systemet

UDFYLDES AF FE (BOKS 1-9)

1. Overordnet beskrivelse af systemet

Formål med systemet	[Beskrivelse af hvad systemet anvendes til, herunder de primære funktioner og dets operative formål]

2. Stamdata for systemet

TEKNISKE SPØRGSMÅL

Systemnavn(e)	[Angiv systemets kaldenavn(e)]
Tilknyttede FE-kodeord	[Angiv alle anvendte FE-kodeord (skrevet med versaler), som er knyttet til eller indgår i systemet, dets delsystemer eller applikationer]
Anvendte produkter/producenter	[F.eks. MS Exchange 2010, Apache Tomcat v7.0, udviklet af NNIT etc. samt det aktuelle versionsnummer]
Idriftsættelsesdato	[Alternativt angiv måned og år for idriftsættelse]
Driftsansvarlig	[Angiv hvilken afdeling, sektion eller f.eks. anden ekstern myndighed, der er ansvarlig for den daglige drift af systemet]
Erstatning/opgradering	[Hvis systemet erstatter eller er en versionsopgradering af et eksisterende system, angiv da det tidligere navn]
Dataejer	[Angiv dataejer for systemet]
Kopier i andre it-miljøer	[Findes der hele eller delvise kopier af systemet i andre it-miljøer end drifts-/produktionsmiljøet? F.eks. udviklings-, test- eller staging-miljøer?]
Planlagte ændringer	[Såfremt der er planlagt større ændringer for systemet eller brugen heraf i indeværende år, bedes disse beskrevet]

3. Systemets it-infrastruktur

TEKNISKE SPØRGSMÅL	
Netværk/kontekst og domæne	[Kaldenavn på netværket/konteksten, som systemet er tilsluttet]
Servere(navngivne) og deres primære roller	[F.eks. applikations-, database-, filserver-, share etc.]
Klienttype(r)	[Webbrowser eller applikation, anfør weblink eller forklar hvorledes systemet tilgås/klient opstartes]
Datakilder til systemet	[F.eks. system hos anden myndighed, indhentningssystem, ESDH etc.]
Dataformater, der overføres til systemet	[F.eks. PCAP, ZIP, XML, CSV etc.]
Datamængder, der overføres til systemet	[Estimat i relevant format f.eks. poster, MB, GB, antal dokumenter etc.]
Modtagere af data fra systemet	[F.eks. system hos anden myndighed, anden afdeling, ESDH, intern database etc.]
Dataformater, der overføres fra systemet	[F.eks. PCAP, ZIP, XML, CSV etc.]
Datamængder, der overføres fra systemet	[Estimat i relevant format f.eks. poster, MB, GB, antal dokumenter etc.]
Datalagringspunkter	[Alle databaser (navneliste), filsystemer, eksterne medier eller øvrige placeringer, hvor data lagres (evt. midlertidigt) af systemet eller daglig anvendelse af systemet]

4. Bruger- og rettighedsstyring

TEKNISKE SPØRGSMÅL	
Brugere af systemet	[Hvilke grupper af brugere anvender systemet, f.eks. afdelinger, sektioner, eksterne]
Antal brugere (læserettigheder)	[Brugere eller brugergrupper, der kun kan læse data]
Antal brugere (skriverettigheder)	[Brugere eller brugergrupper, der kan opdatere (skrive) data]
Rettighedsstyringssystem	[Hvilket system anvendes til styring af brugerrettigheder i systemet? F.eks. Active Directory, intern brugerdatabase, en kombination af flere systemer, etc.]

5. Sletning af data i praksis

TEKNISKE SPØRGSMÅL	
Initiering af sletning	[Hvem sikrer, at der sker en rutinemæssig sletning/oprydning i data i overensstemmelse med eventuelle slettefrister?]
Gennemførsel af sletning	[Sker sletningen af data i systemet manuelt eller automatisk f.eks. via scripts? Ved manuel sletning, hvem er da udførende?]
Hvordan angives det for sletning relevante indhentningstidspunkt/indførselstidspunkt/alder/e.l. på data i systemet?	[Sker angivelsen af alder på data eksempelvis ved felt med creation date i en database eller ved oprettelsestidspunkt i metadata på filer?]
Frekvens	[Hvor ofte foretages rutinemæssig sletning/oprydning af data i systemet?]

JURIDISKE SPØRGSMÅL	
Indeholder systemet erkendte oplysninger, som er tilvejebragt efter FE-lovens § 1, stk. 1, jf. § 6, stk. 1?	[Ja/Nej Spørgsmålet skal ses i sammenhæng med det tekniske spørgsmål "Hvordan angives det for sletning relevante indhentningstidspunkt/indførselstidspunkt/alder/e.l. på data i systemet?" ovenfor]

Indeholder systemet rådata, jf. FE-lovens § 6, stk. 2?	[Ja/Nej Spørgsmålet skal ses i sammenhæng med det tekniske spørgsmål "Hvordan angives det for sletning relevante indhentningstidspunkt/indførselstidspunkt/alder/e.l. på data i systemet?" ovenfor]

6. Backup og restore

TEKNISKE SPØRGSMÅL	
Backup af data	[Tages der backup af data i systemet?]
Data retention	[Hvor langt tilbage er det muligt at genskabe data?]
Restore af data	[Hvordan sikres det, at data, der er slettet som følge af revision ikke fejlagtigt genskabes?]

7. Logning af brugerhandlinger

TEKNISKE SPØRGSMÅL	
Brugerhændelseslogning	[Sker der logning af de handlinger/transaktioner, som brugerne foretager?]
Hændelsestyper	[Hvilke typer af brugerhandlinger logges? F.eks. læsning, skrivning, ændring, sletning, søgning, søgeresultat etc.]
Adgang til hændelseslog	[Hvor og hvordan tilgås systemets brugerhændelseslogs]
Søgning i hændelseslogs	[Hvorledes kan søgning i hændelseslogs ske? Og kan denne søgning tidsafgrænses?]

8. Dokumentation og vejledninger

TEKNISKE SPØRGSMÅL	
Brugervejledning til søgning	[Vedlæg kopi eller angiv placeringen af eksisterende brugervejledninger vedrørende søgning i systemet]
Brugervejledning til systemet	[Vedlæg kopi eller angiv placeringen af eksisterende brugervejledninger vedrørende brug af systemet]
Anden systemdokumentation	[Vedlæg kopi eller angiv placeringen af eksisterende dokumentation vedrørende systemets opbygning og funktionalitet]

9. Generelle spørgsmål vedrørende behandlingssikkerhed

JURIDISKE SPØRGSMÅL	
Hvilke tekniske og organisatoriske foranstaltninger har FE truffet mod, at oplysninger om i Danmark hjemmehørende fysiske og juridiske personer hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med lov om FE, jf. FE-sikkerhedsbekendtgørelsens § 3?	[Angiv tekniske og organisatoriske foranstaltninger]

Såfremt FE har udarbejdet dokumentation, som besvarer ovenstående spørgsmål vedrørende behandlingssikkerhed, anmodes tjenesten om tillige at fremsende dette.

UDFYLDES AF TET

Eventuelle opfølgende spørgsmål til opstartsmøde

NUMMER	SPØRGSMÅL	SVAR
1		
2		
3		

Informationsark for CFCS' it-system [kontrolobjekt]

UDFYLDES AF TET

Dato for opstartsmøde	Mødedeltagere fra TET	Mødedeltagere fra CFCS
[DATO]	[NAVNE]	[NAVNE]

Vejledning til udfyldelse af skema (Word) og tilhørende flow-baseret systemdiagram (Visio)

Skemaet indeholder tekniske og juridiske spørgsmål. Teksten i firkantede parenteser i skemaet nedenfor tjener som vejledning og skal fjernes i forbindelse med udfyldelse. Felter udfyldes med N/A hvis de ikke er relevante for det pågældende system.

Såfremt systemet består af flere selvstændige delsystemer, hvor det skønnes at medføre uhensigtsmæssig kompleksitet eller uoverskuelighed at samle alle informationer i et enkelt skema, udfyldes i stedet ét skema pr. delsystem. Diagramtegningen bør imidlertid stadig udarbejdes som én samlet oversigt.

Formålet med diagramtegningen (Visio) er at skabe et overblik, der både beskriver selve systemet, men også samtidig illustrerer dataflow fra data skabes eller indsamles til det lagres eller overføres til andre systemer. Diagramtegningen skal derfor indeholde:

- Hvilke data, der tilflyder, behandles og forlader systemet
- Hovedkomponenter og datalagringspunkter (f.eks. databaser, filshares eller mailsystemer) i systemet
- Flow-pile, der viser, hvilke veje og retning data flyder gennem systemet

UDFYLDES AF CFCS (BOKS 1-9)

1. Overordnet beskrivelse af systemet

Formål med systemet	[Beskrivelse af hvad systemet anvendes til, herunder de primære funktioner og dets operative formål]

2. Stamdata for systemet

TEKNISKE SPØRGSMÅL

Systemnavn(e)	[Angiv systemets kaldenavn(e)]
Tilknyttede FE-kodeord	[Angiv alle anvendte CFCS-kodeord (skrevet med versaler), som er knyttet til eller indgår i systemet, dets delsystemer eller applikationer]
Anvendte produkter/producenter	[F.eks. MS Exchange 2010, Apache Tomcat v7.0, udviklet af NNIT etc. samt det aktuelle versionsnummer]
Idriftsættelsesdato	[Alternativt angiv måned og år for idriftsættelse]
Driftsansvarlig	[Angiv hvilken afdeling, sektion eller f.eks. anden ekstern myndighed, der er ansvarlig for den daglige drift af systemet]
Erstatning/opgradering	[Hvis systemet erstatter eller er en versionsopgradering af et eksisterende system, angiv da det tidligere navn]
Dataejer	[Angiv dataejer for systemet]
Kopier i andre it-miljøer	[Findes der hele eller delvise kopier af systemet i andre it-miljøer end drifts-/produktionsmiljøet? F.eks. udviklings-, test- eller staging-miljøer?]
Planlagte ændringer	[Såfremt der er planlagt større ændringer for systemet eller brugen heraf i indeværende år, bedes disse beskrevet]

3. Systemets it-infrastruktur

TEKNISKE SPØRGSMÅL	
Netværk/kontekst og domæne	[Kaldenavn på netværket/konteksten, som systemet er tilsluttet]
Servere(navngivne) og deres primære roller	[F.eks. applikations-, database-, filserver-, share etc.]
Klienttype(r)	[Webbrowser eller applikation, anfør weblink eller forklar hvorledes systemet tilgås/klient opstartes]
Datakilder til systemet	[F.eks. system hos anden myndighed, indhentningssystem, ESDH etc.]
Dataformater, der overføres til systemet	[F.eks. PCAP, ZIP, XML, CSV etc.]
Datamængder, der overføres til systemet	[Estimat i relevant format f.eks. poster, MB, GB, antal dokumenter etc.]
Modtagere af data fra systemet	[F.eks. system hos anden myndighed, anden afdeling, ESDH, intern database etc.]
Dataformater, der overføres fra systemet	[F.eks. PCAP, ZIP, XML, CSV etc.]
Datamængder, der overføres fra systemet	[Estimat i relevant format f.eks. poster, MB, GB, antal dokumenter etc.]
Datalagringspunkter	[Alle databaser (navneliste), filsystemer, eksterne medier eller øvrige placeringer, hvor data lagres (evt. midlertidigt) af systemet eller daglig anvendelse af systemet]

4. Bruger- og rettighedsstyring

TEKNISKE SPØRGSMÅL	
Brugere af systemet	[Hvilke grupper af brugere anvender systemet, f.eks. afdelinger, sektioner, eksterne]
Antal brugere (læserettigheder)	[Brugere eller brugergrupper, der kun kan læse data]
Antal brugere (skriverettigheder)	[Brugere eller brugergrupper, der kan opdatere (skrive) data]
Rettighedsstyringssystem	[Hvilket system anvendes til styring af brugerrettigheder i systemet? F.eks. Active Directory, intern brugerdatabase, en kombination af flere systemer, etc.]

JURIDISKE SPØRGSMÅL	
Hvordan har CFCS sikret, at kun medarbejdere ved centret har adgang til de dele af informationssystemerne, hvor der behandles data, som er omfattet af kapitel 4 i lov om CFCS, jf. CFCS-cirkulærets § 4, stk. 1 og 2?	[Angiv hvordan CFCS har sikret, at kun medarbejdere ved centret har adgang til de dele af informationssystemerne, hvor der behandles sådanne data. Spørgsmålet skal ses i sammenhæng med det tekniske spørgsmål "Rettighedsstyring" ovenfor]

5. Sletning af data i praksis

TEKNISKE SPØRGSMÅL	
Initiering af sletning	[Hvem sikrer, at der sker en rutinemæssig sletning/oprydning i data i overensstemmelse med eventuelle slettefrister?]
Gennemførsel af sletning	[Sker sletningen af data i systemet manuelt eller automatisk f.eks. via scripts? Ved manuel sletning, hvem er da udførende?]
Hvordan angives det for sletning relevante indhentningstidspunkt/indførselstidspunkt/alder/e.l. på data i systemet?	[Sker angivelsen af alder på data eksempelvis ved felt med creation date i en database eller ved oprettelsestidspunkt i metadata på filer?]

Frekvens	[Hvor ofte foretages rutinemæssig sletning/oprydning af data i systemet?]

JURIDISKE SPØRGSMÅL

Indeholder systemet data, der er omfattet af CFCS-lovens § 17, stk. 1?	[Ja/Nej Spørgsmålet skal ses i sammenhæng med det tekniske spørgsmål "Hvordan angives det for sletning relevante indhentningstidspunkt/indførselstidspunkt/alder/e.l. på data i systemet?" ovenfor]
Indeholder systemet data, der er tilknyttet en sikkerhedshændelse, jf. CFCS-lovens § 17, stk. 2, nr. 1?	[Ja/Nej Spørgsmålet skal ses i sammenhæng med det tekniske spørgsmål "Hvordan angives det for sletning relevante indhentningstidspunkt/indførselstidspunkt/alder/e.l. på data i systemet?" ovenfor]
Indeholder systemet data, der ikke er tilknyttet en sikkerhedshændelse, men stammer fra myndigheder, som i særlig grad beskæftiger sig med udenrigs-, sikkerheds- og forsvarspolitiske forhold, samt virksomheder og organisationer, hvis aktiviteter har særlig betydning for disse forhold, jf. CFCS-lovens § 17, stk. 2, nr. 2?	[Ja/Nej Spørgsmålet skal ses i sammenhæng med det tekniske spørgsmål "Hvordan angives det for sletning relevante indhentningstidspunkt/indførselstidspunkt/alder/e.l. på data i systemet?" ovenfor]
Indeholder systemet øvrige data, der ikke er tilknyttet en sikkerhedshændelse, jf. CFCS-lovens § 17, stk. 2, nr. 1?	[Ja/Nej] Spørgsmålet skal ses i sammenhæng med det tekniske spørgsmål "Hvordan angives det for sletning relevante indhentningstidspunkt/indførselstidspunkt/alder/e.l. på data i systemet?" ovenfor]

6. Backup og restore

TEKNISKE SPØRGSMÅL

Backup af data	[Tages der backup af data i systemet?]
Data retention	[Hvor langt tilbage er det muligt at genskabe data?]
Restore af data	[Hvordan sikres det, at data, der er slettet som følge af revision ikke fejlagtigt genskabes?]

7. Logning af brugerhandlinger

TEKNISKE SPØRGSMÅL

Brugerhændelseslogning	[Sker der logning af de handlinger/transaktioner, som brugerne foretager?]
Hændelsestyper	[Hvilke typer af brugerhandlinger logges? F.eks. læsning, skrivning, ændring, sletning, søgning, søgeresultat etc.]
Adgang til hændelseslog	[Hvor og hvordan tilgås systemets brugerhændelseslogs]
Søgning i hændelseslogs	[Hvorledes kan søgning i hændelseslogs ske? Og kan denne søgning tidsafgrænses?]

8. Dokumentation og vejledninger

TEKNISKE SPØRGSMÅL

Brugervejledning til søgning	[Vedlæg kopi eller angiv placeringen af eksisterende brugervejledninger vedrørende søgning i systemet]
Brugervejledning til systemet	[Vedlæg kopi eller angiv placeringen af eksisterende brugervejledninger vedrørende brug af systemet]
Anden systemdokumentation	[Vedlæg kopi eller angiv placeringen af eksisterende dokumentation vedrørende systemets opbygning og funktionalitet]

9. Generelle spørgsmål vedrørende behandlingssikkerhed

JURIDISKE SPØRGSMÅL

Hvilke tekniske og organisatoriske foranstaltninger har CFCS truffet mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes og mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med lov om CFCS, jf. CFCS-lovens § 18?	[Angiv tekniske og organisatoriske foranstaltninger]

Såfremt CFCS har udarbejdet dokumentation, som besvarer ovenstående spørgsmål vedrørende behandlingssikkerhed, anmodes tjenesten om tillige at fremsende dette.

UDFYLDES AF TET

Eventuelle opfølgende spørgsmål til opstartsmøde

NUMMER	SPØRGSMÅL	SVAR
1		
2		
3		

Informationsark for RPNRs it-system [kontrolobjekt]

UDFYLDES AF TET

Dato for opstartsmøde	Mødedeltagere fra TET	Mødedeltagere fra PPNR
[DATO]	[NAVNE]	[NAVNE]

Vejledning til udfyldelse af skema (Word) og tilhørende flow-baseret systemdiagram (Visio)

Skemaet indeholder tekniske og juridiske spørgsmål. Teksten i firkantede parenteser i skemaet nedenfor tjener som vejledning og skal fjernes i forbindelse med udfyldelse. Felter udfyldes med N/A hvis de ikke er relevante for det pågældende system.

Såfremt systemet består af flere selvstændige delsystemer, hvor det skønnes at medføre uhensigtsmæssig kompleksitet eller uoverskuelighed at samle alle informationer i et enkelt skema, udfyldes i stedet ét skema pr. delsystem. Diagramtegningen bør imidlertid stadig udarbejdes som én samlet oversigt.

Formålet med diagramtegningen (Visio) er at skabe et overblik, der både beskriver selve systemet, men også samtidig illustrerer dataflow fra data skabes eller indsamles til det lagres eller overføres til andre systemer. Diagramtegningen skal derfor indeholde:

- Hvilke data, der tilflyder, behandles og forlader systemet
- Hovedkomponenter og datalagringspunkter (f.eks. databaser, filshares eller mailsystemer) i systemet
- Flow-pile, der viser, hvilke veje og retning data flyder gennem systemet

UDFYLDES AF PPNR (BOKS 1-9)

1. Overordnet beskrivelse af systemet

Formål med systemet	[Beskrivelse af hvad systemet anvendes til, herunder de primære funktioner og dets operative formål]

2. Stamdata for systemet

TEKNISKE SPØRGSMÅL

Systemnavn(e)	[Angiv systemets kaldenavn(e)]
Anvendte produkter/producenter	[F.eks. MS Exchange 2010, Apache Tomcat v7.0, udviklet af NNIT etc. samt det aktuelle versionsnummer]
Idriftsættelsesdato	[Alternativt angiv måned og år for idriftsættelse]
Driftsansvarlig	[Angiv hvilken afdeling, sektion eller f.eks. anden ekstern myndighed, der er ansvarlig for den daglige drift af systemet]
Erstatning/opgradering	[Hvis systemet erstatter eller er en versionsopgradering af et eksisterende system, angiv da det tidligere navn]
Dataejer	[Angiv dataejer for systemet]
Kopier i andre it-miljøer	[Findes der hele eller delvise kopier af systemet i andre it-miljøer end drifts-/produktionsmiljøet? F.eks. udviklings-, test- eller staging-miljøer?]
Planlagte ændringer	[Såfremt der er planlagt større ændringer for systemet eller brugen heraf i indeværende år, bedes disse beskrevet]

3. Systemets it-infrastruktur

TEKNISKE SPØRGSMÅL	
Netværk/kontekst og domæne	[Kaldenavn på netværket/konteksten, som systemet er tilsluttet]
Servere(navngivne) og deres primære roller	[F.eks. applikations-, database-, filserver-, share etc.]
Klienttype(r)	[Webbrowser eller applikation, anfør weblink eller forklar hvorledes systemet tilgås/klient opstartes]
Datakilder til systemet	[F.eks. system hos anden myndighed, indhentningssystem, ESDH etc.]
Dataformater, der overføres til systemet	[F.eks. PCAP, ZIP, XML, CSV etc.]
Datamængder, der overføres til systemet	[Estimat i relevant format f.eks. poster, MB, GB, antal dokumenter etc.]
Modtagere af data fra systemet	[F.eks. system hos anden myndighed, anden afdeling, ESDH, intern database etc.]
Dataformater, der overføres fra systemet	[F.eks. PCAP, ZIP, XML, CSV etc.]
Datamængder, der overføres fra systemet	[Estimat i relevant format f.eks. poster, MB, GB, antal dokumenter etc.]
Datalagringspunkter	[Alle databaser (navneliste), filsystemer, eksterne medier eller øvrige placeringer, hvor data lagres (evt. midlertidigt) af systemet eller daglig anvendelse af systemet]

4. Bruger- og rettighedsstyring

TEKNISKE SPØRGSMÅL	
Brugere af systemet	[Hvilke grupper af brugere anvender systemet, f.eks. afdelinger, sektioner, eksterne]
Antal brugere (læserettigheder)	[Brugere eller brugergrupper, der kun kan læse data]
Antal brugere (skriverettigheder)	[Brugere eller brugergrupper, der kan opdatere (skrive) data]
Rettighedsstyringssystem	[Hvilket system anvendes til styring af brugerrettigheder i systemet? F.eks. Active Directory, intern brugerdatabase, en kombination af flere systemer, etc.]

5. Sletning af data i praksis

TEKNISKE SPØRGSMÅL	
Initiering af sletning	[Hvem sikrer, at der sker en rutinemæssig sletning/oprydning i data i overensstemmelse med eventuelle slettefrister?]
Gennemførsel af sletning	[Sker sletningen af data i systemet manuelt eller automatisk f.eks. via scripts? Ved manuel sletning, hvem er da udførende?]
Hvordan angives det for sletning relevante indhentningstidspunkt/indførselstidspunkt/alder/e.l. på data i systemet?	[Sker angivelsen af alder på data eksempelvis ved felt med creation date i en database eller ved oprettelsestidspunkt i metadata på filer?]
Frekvens	[Hvor ofte foretages rutinemæssig sletning/oprydning af data i systemet?]

JURIDISKE SPØRGSMÅL	
Hvordan sikrer PPNR, at PNR-oplysninger, jf. bilag 1, fra luftfartsselskaber slettes efter en periode på 5 år efter videregivelsen til PNR-enheden, jf. PNR-lovens § 5?	[Angiv hvordan PPNR sikrer sletning af sådanne data]

6. Backup og restore

TEKNISKE SPØRGSMÅL

Backup af data	[Tages der backup af data i systemet?]
Data retention	[Hvor langt tilbage er det muligt at genskabe data?]
Restore af data	[Hvordan sikres det, at data, der er slettet som følge af revision ikke fejlagtigt genskabes?]

7. Logning af brugerhandlinger

TEKNISKE SPØRGSMÅL

Brugerhændelseslogning	[Sker der logning af de handlinger/transaktioner, som brugerne foretager?]
Hændelsestyper	[Hvilke typer af brugerhandlinger logges? F.eks. læsning, skrivning, ændring, sletning, søgning, søgeresultat etc.]
Adgang til hændelseslog	[Hvor og hvordan tilgås systemets brugerhændelseslogs]
Søgning i hændelseslogs	[Hvorledes kan søgning i hændelseslogs ske? Og kan denne søgning tidsafgrænses?]

JURIDISKE SPØRGSMÅL

Foretager PPNR logning, jf. PNR-lovens § 24, stk. 1 og 2, af følgende behandlingsaktiviteter: 1) Indsamling 2) Søgning 3) Ændring 4) Videregivelse 5) Maskering og afmaskering. 6) Sletning	[Ja/Nej]
Hvordan sikrer PPNR, at logningen af oplysninger opbevares i 5 år, jf. PNR-lovens § 24, stk. 4?	[Angiv periode for opbevaring af logdata]

8. Dokumentation og vejledninger

TEKNISKE SPØRGSMÅL

Brugervejledning til søgning	[Vedlæg kopi eller angiv placeringen af eksisterende brugervejledninger vedrørende søgning i systemet]
Brugervejledning til systemet	[Vedlæg kopi eller angiv placeringen af eksisterende brugervejledninger vedrørende brug af systemet]
Anden systemdokumentation	[Vedlæg kopi eller angiv placeringen af eksisterende dokumentation vedrørende systemets opbygning og funktionalitet]

9. Generelle spørgsmål vedrørende behandlingssikkerhed

JURIDISKE SPØRGSMÅL

Hvilken dokumentation opbevarer PPNR vedrørende behandlingssystemet og procedurer herfor, jf. PNR-lovens § 23, omfattende 1) navn og kontaktoplysninger på personalet i PNR-enheden, der behandler PNR-oplysninger, jf. bilag 1, 2) de forskellige niveauer af autorisationer vedrørende adgangen til oplysninger for personalet i PNR-enheden, 3) anmodninger indgivet af henholdsvis de kompetente myndigheder, der er angivet i bilag 3, eller Politiets Efterretningstjeneste eller Forsvarets Efterretningstjeneste og de kompetente myndigheder eller PNR-enheder i andre EU-medlemsstater og 4) anmodninger om og overførsler af PNR-oplysninger til tredjelande og internationale organisationer?	[Angiv hvilken dokumentation PPNR opbevarer vedrørende behandlingssystemet og procedurer herfor]

Såfremt PPNR har udarbejdet dokumentation, som besvarer ovenstående spørgsmål vedrørende behandlingssikkerhed, anmodes tjenesten om tillige at fremsende dette.

UDFYLDES AF TET

Eventuelle opfølgende spørgsmål til opstartsmøde

NUMMER	SPØRGSMÅL	SVAR
1		
2		
3		

Kontrol af [myndighed] i [årstal] ([kontrolobjekt])

1. Baggrund og formål

Benævnelse af TETs beslutning (dato for møde), formålet med kontrollen samt TETs overordnede risikovurdering af kontrolområdet

"TET besluttede på møde den [dato], at der i [årstal] skal foretages kontrol af [kontrolobjekt]."

"Formålet med kontrollen er, at [...]."

"TETs risikovurdering af [PET / FE / CFCS / PPNR] i [årstal] viste en [lav / begrænset / middel / høj] risiko for brud på lovgivningen i forhold til [tjenestens / centrets / enhedens] [tilvejebringelse / behandling / videregivelse / behandling af oplysninger om lovlig politisk virksomhed] ved anvendelse af [systemnavn]."

2. Beskrivelse af kontrolobjektet

Angivelse af kontrolobjektet (system, database, proces mv.) og kort objektiv beskrivelse heraf og/eller henvisning til hvor nærmere dokumentation kan findes; fremhævelse af de for kontrollen særligt relevante dele af kontrolobjektet

"[Kontrolobjektet] er [PET / FE / CFCS / PPNR] [system / database / proces] til [...]."

"[Kontrolobjektet] indeholder [...], hvoraf [...] vurderes at være særligt relevant for TETs kontrol."

3. Indledende analyse/specifik risikovurdering af kontrolobjekt

Kort beskrivelse af omfanget af data og afdækkede processer samt og risikovurderingen heraf, herunder på baggrund af eventuelt afholdt teknisk møde og/eller opstartsmøde med PET, FE, CFCS eller PPNR og eventuelle tidligere kontroller om lignende. Endvidere behandles indledende overvejelser om metode til kontrol, beskrivelse af eventuel ændret fokus for kontrol siden TETs beslutning som følge af indledende analyse.

"Det er på baggrund af [opstartsmøde med PET / FE / CFCS / PPNR / tidligere kontroller] konstateret, at [...]"

"På baggrund heraf [...]".

4. Metode for kontrol

Angivelse af endeligt fokus og metode for kontrol (systemmæssig, fuldstændig eller stikprøvevis kontrol mv.); overordnet beskrivelse af sagsudvælgelsen i kontrollen og/eller henvisning til vedlagt udvælgelsesark; overordnet angivelse af eventuelle udfordringer med at sikre fuldstændighed i kontrollen, dvs. sikkerheden for at kontrolelementerne (de kontrollerede data såvel som kontrolformen) er tilstrækkelige til at kunne vurdere området. Herefter kort beskrivelse af, hvilken kontrol der er foretaget.

"På baggrund af ovenstående er fokus for TETs kontrol [...]"

Kontrollen er foretaget ved [fuldstændig kontrol / stikprøve / indholdsscreening / inspektion / interviewbaseret kontrol / kontrol af decentral datahåndtering], hvor [system / proces er gennemgået ved drøftelser med PETs / FEs / CFCS' / PPNRs medarbejdere og/eller tekniske undersøgelser] / [udvælgelsen af [sager / poster mv.] er sket på baggrund af [tilfældig/målrettet udvælgelse]."

"Den kontrollerede population af [sager/poster/individer] var i alt på [antal]. På den baggrund har TET udtrukket en stikprøve på [30 sager/poster/individer / 10 pct.], som er gennemgået ved [...]"

TET vurderer, at [der er sikret fuldstændighed i kontrollen / det ikke har været muligt at sikre fuldstændighed i kontrollen], idet [...]"

5. Erfaringer

Efter endt kontrol anføres erfaringer fra kontrollen, herunder en overordnet gengivelse af relevante dele af kontrollen og metodiske erfaringer, og hvorvidt risikovurderingen holdt stik i forhold til resultatet af kontrollen. Det angives om lignende kontrol anbefales foretaget fremover eller eventuelle forslag til alternative kontrolmetoder.

"Kontrollen viste, at [...]"

"TET vurderer på baggrund heraf, at [der ikke er behov for at foretage en lignende kontrol næste år/at der bør foretages en lignende kontrol næste år/at der alternativt bør foretages kontrol af [...]/at der bør foretages lignende kontrol næste år, men at metoden for kontrollen skal justeres, således at [...]."

Godkendt den **[dato]** / **[initialer]**

[Politiets Efterretningstjeneste/
Forsvarets Efterretningstjeneste/
Center for Cybersikkerhed/
Politiets PNR-enhed]

Tilsynet med Efterretningstjenesterne

Dato:
Sagsbeh.: [Navn 1] [Navn 2]
Sagsnr.: [Sagsnr.]
Dok.: [Dokumentnr.]

Opfølgning på Tilsynet med Efterretningstjenesternes kontrol af [kontrolobjekt] i [årstal] / Orientering vedrørende Tilsynet med Efterretningstjenesternes planlagte kontrol af [kontrolobjekt] i [årstal] [1]

Tilsynet med Efterretningstjenesterne (TET) har ved sin kontrol af [Politiets Efterretningstjeneste (PET) / Forsvarets Efterretningstjeneste (FE) / Center for Cybersikkerhed (CFCS) / Politiets PNR-enhed] i [årstal] blandt andet foretaget kontrol af [kontrolobjekt] med fokus på [PETs / FEs / CFCS' / PPNRs] overholdelse af reglerne om [tilvejebringelse / intern behandling / videregivelse af oplysninger / lovlig politisk virksomhed mv.].

Kontrollen blev gennemført ved [Beskrivelse af TETs metode for kontrol]. / [PET / FE / CFCS / PPNR] oplyste ved orientering af [dato], at [...]. TET har på den baggrund besluttet, at kontrollen ikke gennemføres.

[Kontrollen gav ikke anledning til spørgsmål. / Kontrollen gav anledning til spørgsmål vedrørende [...]. Ved skema / e-mail / brev herom blev [PET / FE / CFCS / PPNR] den [dato] hørt.]

[PET / FE / CFCS / PPNR] besvarede ved brev af [dato] TETs høring.

[PET / FE / CFCS / PPNR] oplyste [høringssvar samt eventuelle bemærkninger]].

TET [finder, at kontrollen ikke giver anledning til bemærkninger. / finder ikke på det foreliggende grundlag, at det er muligt at vurdere [...] / finder det bemærkelsesværdigt [...] / finder det problematisk [...] / kan konstatere [...] / finder det kritisabelt [...] / finder det overordentligt kritisabelt [...]].

1 NB! "Orientering" anvendes alene i de tilfælde, hvor kontrolobjektet har vist sig at falde uden for TETs kompetence

Borgergade 28, 1
DK-1300 København K
t 25 50 10 34
www.tet.dk

Såfremt [PET / FE / CFCS / PPNR] har bemærkninger til, hvilke oplysninger der kan indgå i TETs redegørelse i forhold til beskrivelsen af kontrolområdet eller i øvrigt har oplysninger vedrørende opfølgning på kontrollen, skal tilsynet anmode om, at bemærkningerne fremsendes senest den [dato] af hensyn til tilsynets interne proces for udarbejdelse af redegørelse for [årstal]. TET vil inddrage eventuelle bemærkninger fra [PET / FE / CFCS / PPNR] i vurderingen af, hvordan kontrolområdet og en eventuel opfølgning på kontrollen beskrives i tilsynets redegørelse for [årstal].

Der henvises til [PETs / FEs / CFCSs / PPNRs journalnummer [...] samt] TETs kontrolnummer [se kontrolplan].

Med venlig hilsen
Tilsynet med Efterretningstjenesterne

v/[navn]
Formand

Standarder for TETs virksomhed
Udgivet af TET, februar 2024

Layout + illustrationer: Eckardt ApS

Publikationen kan downloades fra TETs hjemmeside på www.tet.dk

Tilsynet med Efterretningstjenesterne
Borgergade 28, 1. sal, 1300 København K
www.tet.dk