Danish Intelligence Oversight Board

Standards for Danish intelligence review activities

Mapping of IT infrastructure v. 2.0

Risk and materiality assessment v. 2.1

Methodology, performance of compliance review and verification of information v. 2.0

Standards for Danish intelligence review activities

Mapping of IT infrastructure v. 2.0

Risk and materiality assessment v. 2.1

Methodology, performance of compliance review and verification of information v. 2.0

February 2024

CONTENT

APPENDIX

VERSIONS SINCE THE PUBLICATION OF TET'S STANDARDS

Standard for TET's mapping of IT infrastructure

VERSION	PUBLISHED	CHANGES
2.0 (current)	19 February 2024	Extensive update of TET's standard for mapping IT infrastructure in DSIS, DDIS, CFCS and PPNR
1.1	2 June 2022	Minor changes as a result of annual update
1.0	24 June 2021	Original version

Standard for TET's risk and materiality assessment

VERSION	PUBLISHED	CHANGES
2.1 (current)	19 February 2024	Minor corrections, including graphical support, as a result of annual update
2.0	2 June 2022	Extensive update of TET's risk and materiality assessment model for DSIS, DDIS, CFCS and PPNR
1.0	24 June 2021	Original version

Standard for TET's methodology, performance of compliance review and verification of information

VERSION	PUBLISHED	CHANGES
2.0 (current)	19 February 2024	Extensive update of TET's standard for methodology, performance of review and verification of information
1.1	2 June 2022	Minor changes as a result of annual update
1.0	24 June 2021	Original version

Introduction

TET's compliance review of the Danish Security and Intelligence Service (DSIS), the Danish Defence Intelligence Service (DDIS), the Danish Centre for Cyber Security (CFCS) and the PNR Unit of the Danish Police (PPNR) requires knowledge of the various agencies' IT infrastructure, prioritisation of the oversight resources and effective methods for carrying out the review.

TET is only able to review the parts of DSIS, DDIS, CFCS and PPNR that TET is aware of. Furthermore, TET does not have the resources to perform a full review of all parts of DSIS, DDIS, CFCS and PPNR. Finally, TET's reviews must be able to document the conditions in DSIS, DDIS, CFCS and PPNR using a limited amount of resources.

TET's standards aim to address these fundamental challenges. For this purpose, TET's work consists of three main elements:

TET's 1 mapping of IT infrastructure in DSIS, DDIS, CFCS and PPNR, respectively, aims to provide TET with the necessary knowledge of the procurement, the processing and the disclosure of information in DSIS, DDIS, CFCS and PPNR.

TET compiles and assesses information about relevant parts of the IT infrastructure in order to create the right basis for performing complete risk and materiality assessments of all processes and systems in DSIS, DDIS, CFCS and PPNR.

TET's methodology for mapping IT infrastructure is self-developed. The method is a further development of TET's initial mapping of IT systems in DSIS and DDIS in 2014-2015, which has prompted a need for both adjustment, structuring and formalisation of the methodology.

The selection of methodology reflects a trade-off between the need for technical detail in mapping to support TET's review activities, the extent of IT resources, and the IT governance maturity level within TET as well as DSIS, DDIS, CFCS and PPNR.

The standard for TET's mapping of IT infrastructure in DSIS, DDIS, CFCS and PPNR is described in more detail in Section 1.

TET's 2 planning of compliance reviews for the coming year aims to prioritise TET's resources so that the reviews are directed at those parts of DSIS, DDIS, CFCS and PPNR assessed to pose the greatest risk of non-compliance with legislation.

The planning is based on an annual risk and materiality assessment of processes and systems (hereinafter referred to as "review subjects") in DSIS, DDIS, CFCS and PPNR for the purpose of assessing the risk of non-compliance with legislation. On this basis, TET prepares risk analyses that makes the foundation for the selection of reviews in the coming year. The selected reviews are summarised in review plans for DSIS, DDIS, CFCS and PPNR for the coming year.

The purpose of the risk analyses is to ensure that TET's reviews are focused on areas, which pose the greatest risk of non-compliance with legislation. In addition, other relevant factors are taken into account, for example, review areas given special weight by the legislature such as the rules on legitimate political activity.

Review areas assessed to pose a lower risk of non-compliance with legislation are generally reviewed every five years in order to ensure completeness in reviewing DSIS, DDIS, CFCS and PPNR. In addition, this measure intends to ensure that the assessment of the risk of non-compliance with legislation in the area remains accurate.

The standard for TET's risk and materiality assessment of DSIS, DDIS, CFCS and PPNR is described in more detail in Section 2.

TET's reviews 3 are carried out throughout the year based on the review plans applicable to DSIS, DDIS, CFCS and PPNR, respectively. TET does not determine methods for individual reviews in connection with the preparation of risk assessments and analyses. As such, the selection of method is determined prior to initiating a specific review.

TET uses various methods to review the individual subjects, including full reviews, random or targeted sampling, content screenings, inspections and interview- and consultation-based reviews.

TET's selection methodology of review is based on a specific risk assessment of the review subject, experience from previous reviews and TET's findings in connection with the specific review. In that connection, prior to reviewing subjects not previously reviewed, TET holds a start-up meetings with relevant DSIS, DDIS, CFCS and PPNR employees in order to ensure an adequate police and/or intelligence professional and technical understanding of the subject, which will enable the reviews to be adjusted and adequately performed.

As part of TET's performance of reviews, verification reviews are also carried out on the IT infrastructure of DSIS, DDIS, CFCS and PPNR. The purpose of the verification is to ensure

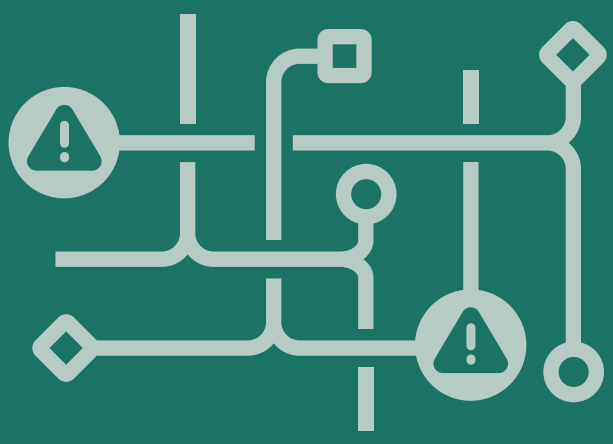
that TET's reviews are based on data from DSIS, DDIS, CFCS and PPNR the accuracy of which has been verified by TET.

The standard for TET's methodology, performance of review and verification of information is described in more detail in Section 3.

The process for TET's 1 mapping, 2 planning 3 performance and verification of its reviews is illustrated in the below figure. The processes are supported by ongoing quality assurance by approval at executive and board levels, respectively, and by consultation with external parties on legal, factual or classification related matters.


See TET's standard for mapping of IT infrastructure (Section 1)
Mapping of DSIS', DDIS', CFCS' and PPNR's IT infrastructure
QUALITY ASSURANCE
External consultation on factual matters
QUALITY ASSURANCE
Approval at executive level
See TET's standard for risk and materiality assessment (Section 2)
Risk and materiality assessment of DSIS, DDIS, CFCS and PPNR
QUALITY ASSURANCE
Approval at executive level
Submission of risk and materiality assessment of DSIS, DDIS, CFCS and PPNR and decision on review plans for the coming year
QUALITY ASSURANCE
Discussion and approval at board level
See TET's standard for methodology, performance of review and verification of information (Section 3)
Clarification of review type for all planned reviews
QUALITY ASSURANCE
Approval at executive level
Briefing of DSIS, DDIS, CFCS and PPNR on TET's review plans
Technical and legal clarification of review subjects
QUALITY ASSURANCE
External consultation on legal and factual matters
Decision on review method for each review
QUALITY ASSURANCE
Approval at executive level
Performance of reviews
QUALITY ASSURANCE
Approval at executive level
Consultation of DSIS, DDIS, CFCS or PPNR in connection with reviews
QUALITY ASSURANCE
External consultation on legal and factual matters
Submission and completion of reviews
QUALITY ASSURANCE
Discussion and approval at board level
Sending of follow-up letters to DSIS, DDIS, CFCS or PPNR
QUALITY ASSURANCE
External quality assurance for any comments regarding the compliance review
Preparation of annual reports on DSIS and PPNR, DDIS and CFCS
QUALITY ASSURANCE
Discussion and approval at board level
QUALITY ASSURANCE
External quality assurance when consulting on factual or classification issues
Publication of TET's annual reports

1 Mapping of IT infrastructure



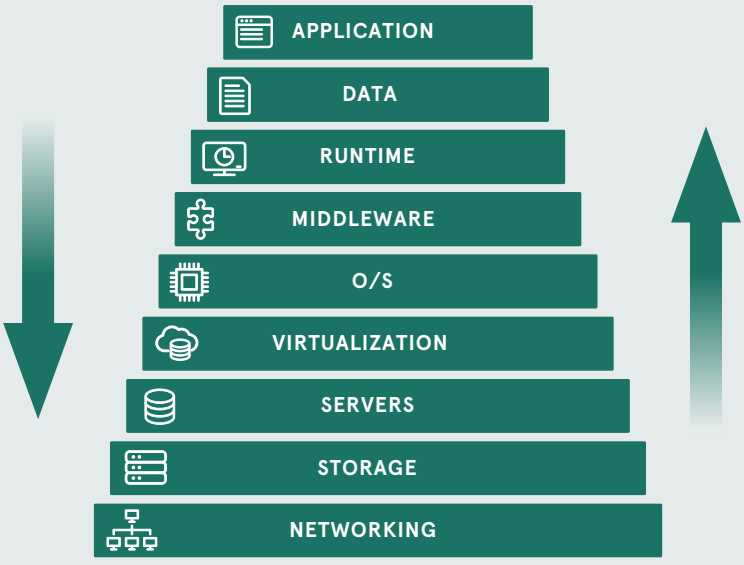
The purpose of TET's mapping of the IT infrastructure of DSIS, DDIS, CFCS and PPNR is to compile and assess information about relevant server-based parts of the IT infrastructure of DSIS, DDIS, CFCS and PPNR. TET's mapping provides a solid platform for TET's annual risk and materiality assessments, which form the basis for decisions on TET's annual review plans.

TET's method for mapping of IT infrastructures has been developed by TET itself, as a mapping standard designed for the specific purpose needed by TET does not exist. The method is a further development of TET's initial mapping of the IT systems of DSIS and DDIS in 2014-2015, which has prompted a need to adjust, structure, and formalisation of the methodology.

Thus, the selection of method reflects a balancing of the need for a technical degree of detail to be able to support TET's reviews, the required level of IT resources, and the IT governance maturity level within TET as well as DSIS, DDIS, CFCS and PPNR.

As an external agency, TET is very much dependent on which IT tools DSIS, DDIS, CFCS and PPNR already have at their disposal and use as well as the types of system access being available. TET strives to use view-only access to the systems and data of DSIS, DDIS, CFCS and PPNR. However, where this is not possible, TET may need to use privileged access.

TET's IT infrastructure mapping standard is based on cross-validation of components at different levels of the IT infrastructure. TET maps, among other things, networks, storage facilities, servers, etc., and compares the results of this with the application level and assigned user rights. This enables TET to identify servers or databases that TET has not yet mapped or otherwise identified. This also includes test and development environments, which are found in most organisations that develop and/or operate their own IT systems.



TET's method for mapping of IT infrastructures is developed in order to ensure comparability – both within a given year and over time. In addition, the assessments must be reproducible. At the same time, the method must be dynamic and capable of being further developed over time, including in relation to information that may subsequently be included in future risk assessments.

This standard describes in detail the process for the mapping activities and for the preparation of TET's internal system list as well as the method for analysing and assessing the collected data, which results in input for TET's annual risk and materiality assessments in the form of updated system lists containing an IT professional relevance score.

Overall, the process documentation for TET's annual mapping of DSIS, DDIS, CFCS and PPNR IT infrastructures may be broken down into the following elements:

- *Process guide* concerning TET's mapping of the IT infrastructures of DSIS, DDIS, CFCS and PPNR (this standard).
- Schematic template for an *infrastructure overview* for collection of relevant information about DSIS, DDIS, CFCS and PPNR IT infrastructures concerning all networks and servers put into operation (see Appendix 1).
- Schematic template for TETs internal *system list*, which is prepared based on an analysis and assessment of the collected data (see Appendix 2).
- *Review memoranda* prepared since the last update of TET's mapping of IT infrastructure (see Appendix 6).

The purpose of breaking down TET's IT infrastructure mapping as outlined above is to handle data collection and management for practical purposes in a spreadsheet, which makes it is easy to sort and filter data as needed.

In order to ensure optimum utilisation of the IT resources of TET as well as DSIS, DDIS, CFCS and PPNR, TET focusses exclusively on requesting information used in the preparation of TET's products and maintaining a manageable data structure that is easy to work with for DSIS, DDIS, CFCS and PPNR as well as TET.

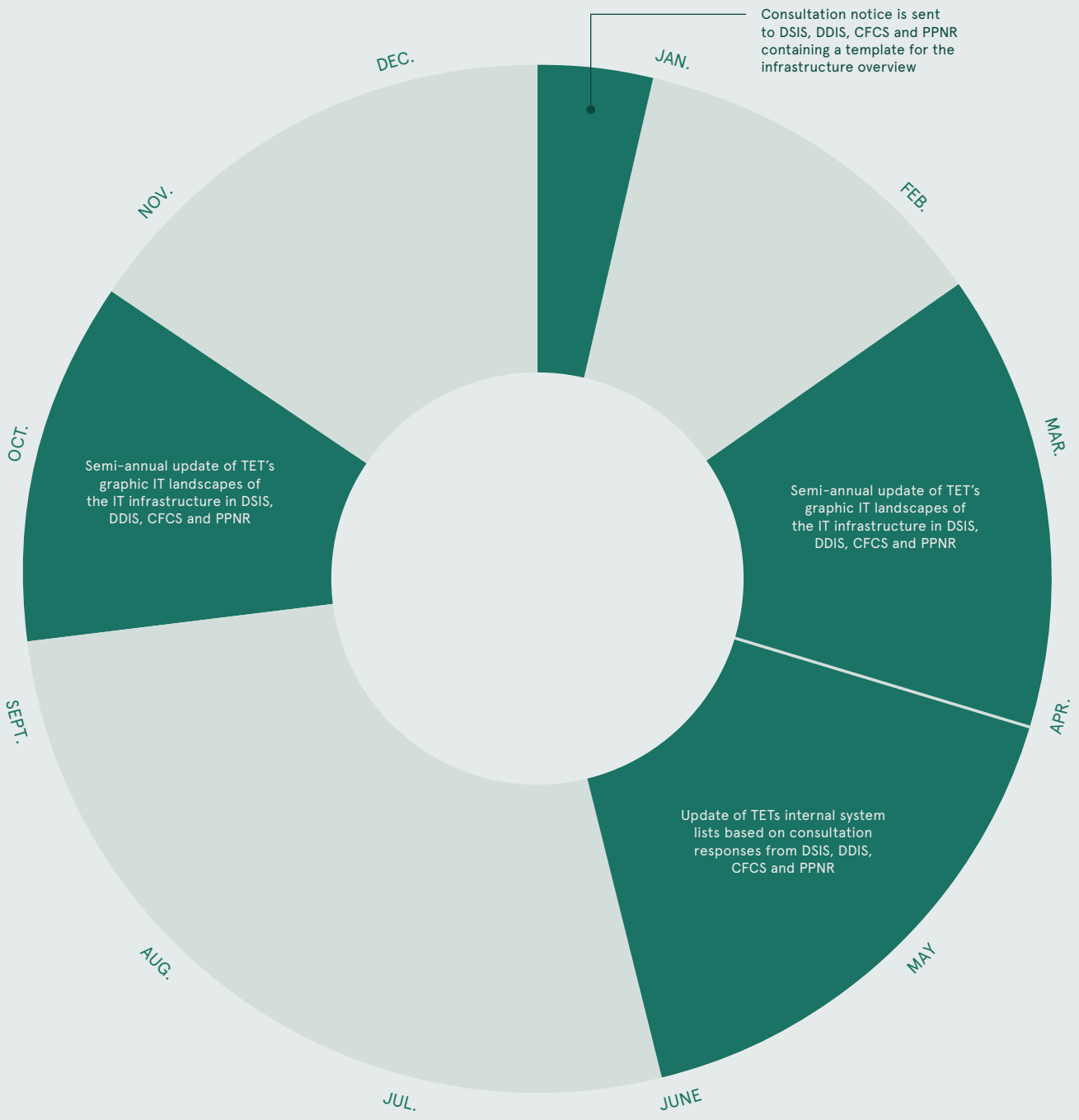
The need for information continuously changes as and when TET's review needs changes, TET's knowledge of systems and data improves and when DSIS', DDIS', CFCS' and PPNR's use their IT systems, data volumes, tools and applied technologies change.

1.1 Process for mapping of IT infrastructures

The overall IT infrastructure mapping process starts at the beginning of January with TET requesting relevant information from DSIS, DDIS, CFCS and PPNR CFCS and PPNR. The overall IT infrastructure mapping process ends in June with the preparation of input for TET's annual risk and materiality assessments in the form of updated system lists of all existing DSIS, DDIS, CFCS and PPNR IT systems.

The system lists contains an IT professional assessment of the systems that should be included in TET's risk and materiality assessments. In this regard, it ensures that new systems are included and phased-out systems are removed. The system lists thereby ensure the necessary IT professional input so that TET's knowledge concerning IT infrastructure changes (the size of new or changed systems, the number of users, etc.) is included in TET's ranking of reviews. The mapping process stretches throughout the year as follows:

Annual cycle of TET's mapping of IT infrastructure



JANUARY: TET sends consultation notice to DSIS, DDIS, CFCS and PPNR containing a template for the infrastructure overview and requesting that relevant data for all DSIS, DDIS, CFCS and PPNR servers be entered in the overview. After having sent the consultations, TET engages in dialogue with DSIS, DDIS, CFCS or PPNR to address any questions about the process or the template design.

MARCH: Based on review memoranda prepared by TET in connection with specific reviews performed in the past six months, TET's graphic IT landscapes of the IT infrastructure in DSIS, DDIS, CFCS and PPNR are updated.

APRIL–JUNE: TET receives consultation responses from DSIS, DDIS, CFCS and PPNR, processes collected data and updates its internal system lists.

OCTOBER: Based on review memoranda prepared by TET in connection with specific reviews performed in the past six months, TET's graphic IT landscapes of the IT infrastructure in DSIS, DDIS, CFCS and PPNR are updated.

The process for TET's mapping of the IT infrastructure in DSIS, DDIS, CFCS and PPNR, respectively, follows the annual cycle of work.

1.2 Preparation and use of the infrastructure overview

TET has decided to structure its reviews so that within an review subject, the individual IT systems are used as a basis. This method contributes to ensuring completeness in TET's reviews. This is the reason why TET's mapping of the IT infrastructure at DSIS, DDIS, CFCS and PPNR is based on the individual IT systems. The connection between operational matters, systems and procedures, including data flow mapping, is subsequently mapped in connection with TET's individual reviews (see Section 3).

TET has decided to map DSIS', DDIS', CFCS' and PPNR's IT infrastructures each year in a template, comprising the minimum amount of data, which TET currently considers to be necessary in order to obtain an overview of which networks and domains exist at the relevant time and which IT systems exist thereon. The template also contains information about the servers on which the IT systems are run and which primary software is used.

These relatively few types of information enable TET to make an overall assessment of the IT systems containing operational data of relevance to TET's reviews.

For a closer look at each item in TET's infrastructure list, please refer to the corresponding template (see Appendix 1). The content of the infrastructure overview is adjusted and updated annually as needed.

1.3 Analysis and assessment of data in the infrastructure overview

In TET's analysis and assessment of data concerning DSIS', DDIS', CFCS' and PPNR's IT infrastructure, it is the system name that is the primary key in TET's infrastructure overview

and system list. The system name binds the two lists together and serves as input to TET's annual risk and materiality assessments.

The infrastructure overview ties the individual servers to an IT system and may therefore be used to cross-check and validate whether there are any

- IT systems with no servers attached;
- servers, which do not form part of an IT system;
- IT systems and/or servers which TET has no knowledge of yet; and
- IT systems and/or servers, which have been added or removed since the last updated infrastructure overview was compiled.

The infrastructure overview enables TET to cross-check and validate whether servers appearing on the infrastructure overview correspond to the servers, which in practice run in DSIS', DDIS', CFCS' and PPNR's IT environments. This is reviewed in part by means of inspection reviews of DSIS', DDIS', CFCS' and PPNR's virtualisation layers (hypervisor administration tools) and by physical servers placed in server rooms. At the same time, TET reviews whether there are any servers that have been turned off or are no longer in use (see Section 3).

Moreover, TET screens and assesses the relevance of the individual servers for the review by identifying the following:

- The primary software being run on the server
- The primary role of the server
- The network location of the server
- The server name since, for purely practical reasons, the server is often named according to established rules and conventions tied to the function of the server
- Which other servers form part of the same IT system or context

In particular, the primary software of the server is essential as for purposes of, among other things, clarity, performance and operational reliability in relation to troubleshooting, monitoring and redundancy (fault tolerance) in major IT installations, it is expedient and therefore standard practice to place critical or central functions in an IT system on a separate server.

Additionally, operational systems and pure IT infrastructure servers (for example, for management, antivirus, software roll-out, etc.) are normally not located on the same servers.

Furthermore, TET's assessment of servers is based on TET's accumulated knowledge about DSIS, DDIS, CFCS and PPNR as well as their IT systems, including the results of previous years' compliance reviews and the ongoing dialogue with relevant employees of DSIS, DDIS, CFCS or PPNR.

1.4 Verification of data in the infrastructure overview

Verification of the information entered by DSIS, DDIS, CFCS and PPNR in the infrastructure overviews is carried out by TET's ongoing verification reviews (see Section 3.4). Furthermore, the infrastructure overviews are used regularly for TET's regular reviews to validate the information provided by DSIS, DDIS, CFCS and PPNR in conjunction with initial consultations for review type A (see Sections 3.2 and 3.8).

1.5 Preparation and use of the system list

TET's system list is compiled based on the above mentioned infrastructure overview, system documentation available in DSIS, DDIS, CFCS and PPNR, and TET's accumulated knowledge. The system list serves as an internal tool for TET that is continuously updated with relevant technical information. The system list is important for TET's understanding of systems used by DSIS, DDIS, CFCS and PPNR, including the connection between them.

The system list provides an assessment of relevance and the score of new and/or unknown IT systems, which TET has not previously reviewed or which in TET's assessment have undergone extensions or changes, which may affect TET's risk and materiality assessment of the system in question.

The system list contains the following:

- Reference
- System name
- Short system description
- Network/Context/Environment
- Applied system list (year)
- Relevance score
- Relevance assessment
- Name change

A more detailed explanation of the individual items in the system list is available in the template (see Appendix 2). The system list columns are adjusted and updated annually.

1.6 Detailed process description

The following is a review of the process for conducting TET's mapping of IT infrastructure in DSIS, DDIS, CFCS and PPNR and for updating system lists for each authority. The update of system lists must be finalised prior to TET's annual risk and materiality assessment of DSIS, DDIS, CFCS and PPNR.

PROCESS	DEADLINE
1. Preparation of the system list for the coming year	
a. Creation of system list for the upcoming calendar year is based on the previous year's list	September
b. Update each source with the year in the citation columns.	
c. Setting the values in the "Name change" column to "No"	
d. Approval of review memorandum regarding the preparation of the system list (Sections 1-4) retained by the Deputy Secretary-General	
2. Ongoing additions to system list	
a. Ongoing addition of new systems	Ongoing
b. State the source type on which the addition is based	
c. State which year's system list the system was originally added to	
3. Annual request for system list sources	
a. Consultation with DSIS, DDIS, CFCS and PPNR regarding the infrastructure overview	January
4. Preparation of system list	
a. Review of selected sources to validate existing systems on the system list and identify new systems	April-May
b. Creation of identified systems that are not already listed in the system list	
c. State the source in which the system is identified, in the source column	
d. Indicate the system list for the year to which the system was originally applied	
e. List all sources where both existing and new systems are identified	
f. State if an existing system has changed its name	
5. Identification of new, suspended and changed systems	
a. Identification of new systems by sorting the "Applied system list" column of the system list so that only systems entered into this year's system list are shown	April-May
b. Identification of suspended systems is found by sorting current source columns so that only systems where no current sources are marked are shown	

PROCESS	DEADLINE
c. Identification of changed systems is found by sorting the "Name change" column of the system list so that only systems that have changed their name are shown	
d. Extraction of new, defunct and modified systems for independent tabs	
e. Deletion of suspended systems from this year's system list	
6. Possible supplementary consultation with DSIS, DDIS, CFCS or PPNR	
a. Forwarding of any supplementary consultation with DSIS, DDIS, CFCS and PPNR if, during the preparation of the annual system list, doubts arise as to whether a system name is part of a system complex, a redundant name of a different system, application or similar	Maj
b. Setting the consultation period to 14 days	
c. Update of system list based on consultation responses	
7. Transfer of system list	
a. Transfer of the finalised system list to relevant employees for the purpose of risk and materiality assessment	Juli
8. Evaluation	
a. Approval of the review memorandum for the preparation of the system list (Section 5) with the Deputy Secretary-General, which includes a description of the process of preparing the system list.	August

2 Risk and materiality assessment

The purpose of TET's risk and materiality assessment of DSIS, DDIS, CFCS and PPNR, respectively, is to compile and assess risks to create the proper basis for decisions on TET's own motion reviews and other reviews based on indirect subject access requests under Section 13 of the Danish Intelligence Service Act (the DSIS Act) and Section 10 of the Danish Defence Intelligence Service (the DDIS Act).

The methodology for risk and materiality assessment of DSIS, DDIS, CFCS and PPNR is developed by TET. TET's need to develop the methodology in-house is due to the fact that the target field of TET's risk and materiality assessments is not internal processes of its own activities but rather assessment of other agencies' processes, systems and data processing practices. Thus, it is only relevant for TET to analyse risks in relation to non-compliance with legislation, and not other strategic, economic, political or administrative/procedural consequences.

TET conducted its first annual risk assessment of DSIS, DDIS and CFCS in 2016. TET's risk assessment methodology has been updated four times (most recently in 2023 due to the implementation of system support for the process).

TET's risk and materiality assessment method applied in relation to DSIS, DDIS, CFCS and PPNR is to ensure comparability – both within a given year and over time. In addition, the assessments must be reproducible. At the same time, the method must be dynamic and capable of being developed further over time, including in relation to factors that may subsequently be included in future risk assessments.

This process guide describes the process for preparing TET's annual risk and materiality assessments as well as the method for assessing risks and ranking review areas.

TET's annual risk and materiality assessments of DSIS, DDIS, CFCS and PPNR may be broken down into the following elements:

RISK ASSESSMENTS	TET's system-supported risk assessments of all review subjects in DSIS, DDIS, CFCS and PPNR contain risk scores for each review subject, as well as an indication of whether a given system in DSIS and DDIS are being reviewed or should be reviewed based on indirect access requests.
RISK ANALYSES (OWN MOTION REVIEWS)	TET's ranked risk analyses of DSIS, DDIS, CFCS and PPNR, respectively, regarding TET's own motion reviews emphasise factors that indicate whether a given review subject should be included, be given higher priority or should be de-prioritised in the review plan for the coming year.
RISK ANALYSES (INDIRECT SUBJECT ACCESS)	TET's ranked risk analyses of DSIS and DDIS, respectively, regarding the subject access scheme contains detailed assessments of whether TET's reviews on the basis of indirect access requests are adequate in view of the risks identified and assessed in the risk assessments.
REVIEW PLANS	TET's plans for the review of DSIS, DDIS, CFCS and PPNR the coming year approved by TET's board based on an overall assessment of the above material.

The purpose of breaking down TET's risk and materiality assessments as outlined above is to ensure openness and transparency in TET's assessment of DSIS, DDIS, CFCS and PPNR.

2.1 Process for TET's risk and materiality assessment

TET follows the below steps when preparing its annual risk and materiality assessments:

ALL YEAR: When reviews are finalised, TET revises its risk assessments of the individual review subjects in DSIS, DDIS, CFCS and PPNR.

SEPTEMBER-OCTOBER: TET performs risk assessment of new and not previously reviewed subjects in DSIS, DDIS, CFCS and PPNR.

OCTOBER-NOVEMBER: Based on the risk assessments, TET prepares risk analyses of DSIS, DDIS, CFCS and PPNR, respectively, regarding TET's own motion reviews and ranked risk analyses of DSIS and DDIS respectively, regarding requests for indirect subject access. Finally, draft review plans are prepared for the following year's review of DSIS, DDIS, CFCS and PPNR.

NOVEMBER: TET's board is presented with the material and approves the review plans for the following year's own motion review of DSIS, DDIS, CFCS and PPNR. Furthermore, the board decides on the scope of TET's review based on indirect subject access requests, i.e. which systems are to be included in TET's review thereof.

DECEMBER: TET meets with DSIS, DDIS, CFCS and PPNR to discuss TET's review plans for the following year.

The process for TET's risk and materiality assessment of DSIS, DDIS, CFCS and PPNR follows the annual cycle of work.

The purpose of TET informing DSIS, DDIS, CFCS and PPNR about its risk and materiality assessments and review plans is to enable DSIS, DDIS, CFCS and PPNR to take into account this information in their internal compliance reviews and their preparation of their own risk and materiality assessments. This provides for the mutual exchange of experience that will strengthen the risk-oriented selection as well as the impact of TET's compliance reviews.

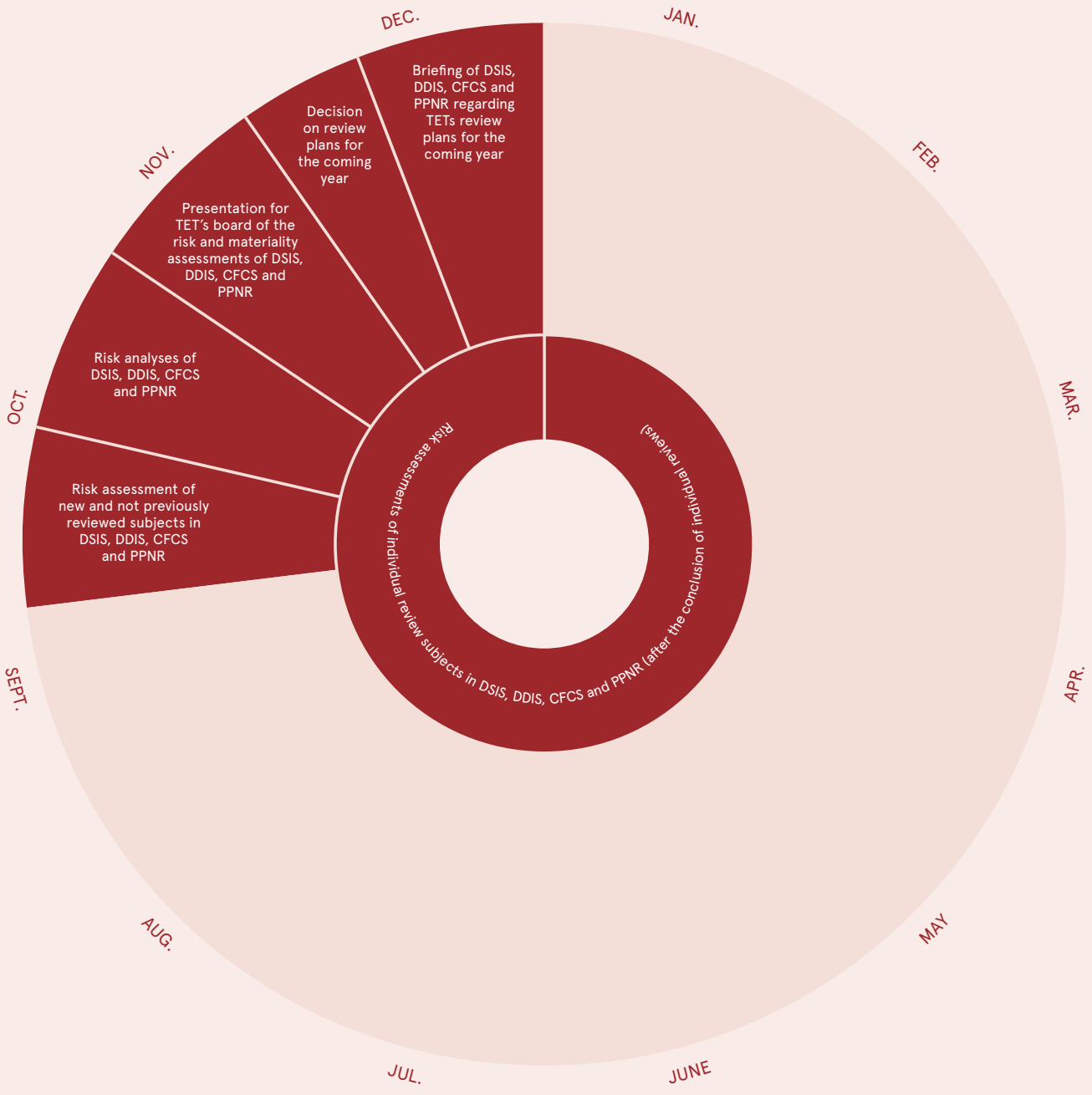
TET's direct access to the systems of DSIS, DDIS, CFCS and PPNR prevents DSIS, DDIS, CFCS and PPNR from predicting which files and data will be subjected to review by TET. However, TET may sometimes have to notify DSIS, DDIS, CFCS and PPNR about the time and method of a review, e.g. if TET needs access to specific physical premises or needs to interview specific employees.

2.2 Risk assessment of review subjects

In order to be able to make a risk-oriented selection of review subjects and, by extension, perform efficient and targeted compliance reviews, it is essential for TET to have in-depth knowledge of DSIS, DDIS, CFCS and PPNR.

TET's risk assessment of review areas is based on TET's accumulated knowledge about DSIS, DDIS, CFCS and PPNR, including in particular the performance and results of previous years' compliance reviews as well as the ongoing dialogue with relevant employees of

Annual cycle of TET's risk and materiality assessment



DSIS, DDIS, CFCS and PPNR. This ensures a high degree of validity in the risk assessment and the subsequent ranking and selection of review subjects.

As a basis for TET's ranked risk analyses of DSIS, DDIS, CFCS and PPNR, TET has produced a risk score calculation model for the individual review subjects of interest. The risk score reflects the overall risk/likelihood of a given statutory rule being violated within an review area in which DSIS, DDIS, CFCS and PPNR are engaged.

The model weighs in different ways the following variables based on relevant statutory provisions (see Appendix 1):

- *The quality of the data* in the given review subject, i.e., whether the data is structured so that the metadata is fixed and cannot be changed by the ordinary user.

- *The extent of personal data* contained in the given review subject.

- *The method of data processing* in the given review subject, i.e., whether this takes place by means of fully automated processes or fully/partial manual processes.

- *The location of the data processing* for the given review subject, i.e., whether the processing takes place on a centralised basis whereby TET has access in its own right, or whether it takes place on a decentralised basis where TET's access presupposes DSIS', DDIS', CFCS' and PPNR's intervention.

- *Logging and rights management* in relation to the data processing within the given review subject, i.e., whether all relevant user actions are correctly logged, including whether their integrity is ensured, and to what extent it is ensured that only persons with a need to access data contained in the review subject are able to do so.

- The extent of DSIS', DDIS', CFCS' and PPNR's *internal legal compliance assurance* of the given review subject, including an assessment of

  - whether DSIS, DDIS, CFCS and PPNR have an established practice in place for legal approval of intelligence or operational activities; and

  - if so, whether this approval takes place via automated circumvention proof and anti-circumvention stop-and-go processes; and

  - whether relevant staff are trained in the rules for using the given review subject, including whether such training is based on introductory training or an ongoing dialogue.

- The extent of DSIS', DDIS', CFCS' and PPNR's *internal compliance reviews* of the given review subject, including

  - whether DSIS, DDIS, CFCS and PPNR subsequently conduct a legal compliance review of a given review subject and, if so,

  - whether this internal compliance review is planned on the basis of an established practice or whether it is carried out on an ad hoc or decentralised basis; and

  - whether the internal compliance review has revealed any non-compliance with legislation.

- Whether *TET has conducted any reviews in the past* of the review subject, including stating
  - the date of TET's most recent review;
  - whether TET's reviews within the last 3 years have revealed any non-compliance with legislation;
  - whether TET's reviews within the last 3 years have given rise to any comments; and
  - the nature of such errors and comments previously identified.

Thus, TET's risk score calculation model for the individual processes and systems within DSIS, DDIS, CFCS and PPNR includes the following variables and potential values:

TET's risk score calculation model

VARIABLES	VALUES	
Data quality	Structured	0
	Unstructured	2
	Unknown	3
Extent of personal data	Minor extent	0
	Material extent	2
	Unknown	3
Method of data processing	Automated	0
	Semi-automated	1
	Manual	2
	Unknown	3
Location of processing	Central, and TET has independent access	0
	Central, but TET has no independent access	1
	Decentralised	2
	Unknown	3
Logging and rights management	Yes, to a relevant extent	0
	Yes, but to a lesser relevant extent	1
	No	2
	Unknown	3
	N/A	0
Are internal legal compliance assurance performed?	Yes, including established practice in place for legal approval	0
	Yes, but there is no established practice in place for legal approval	1
	No	3
	Unknown	3
Are internal compliance reviews performed?	Yes, satisfactory	0
	Yes, but ad hoc/decentralised/unsatisfactory	1
	No	3
	Unknown	3
Did internal compliance reviews reveal non-compliance with legislation?	Yes, non-compliance with legislation	2
	Yes, minor non-compliance with legislation	1
	No	0
	N/A	0
Has TET carried out reviews?	Yes	0
	No	2
When was the last time TET carried out a review?	≥ 4 years	3
	3 years	2
	2 years	1
	≤ 1 year	0
	N/A	0
Have TET's previous reviews shown non-compliance with legislation?	No	0
	Yes, minor errors in the most recent review	2
	Yes, non-compliance with legislation in the most recent review	5
	Yes, minor errors in previous reviews (≤ 3 years)	1
	Yes, non-compliance with legislation in previous reviews (≤ 3 years)	3
	N/A	0
Did TET's previous reviews give rise to any comments?	No	0
	Yes, minor comments in the most recent review	2
	Yes, significant comments in the most recent review (criticisable/highly criticisable)	5
	Yes, minor comments in previous reviews (≤ 3 years)	1
	Yes, significant comments in previous reviews (criticisable/highly criticisable) (≤ 3 years)	3
	N/A	0

TET's risk assessment of the individual review subjects in DSIS, DDIS, CFCS and PPNR is system-supported so that answering the above variables results in risk score calculation for each review subject in relation to the risk of non-compliance with the individual legal requirements within each review subject.

Risk scores are given on a scale from 0-26 with the following indications:

Risk scores 0-5	**Low risk** of non-compliance with legislation
Risk scores 6-12	**Limited risk** of non-compliance with legislation
Risk scores 13-19	**Medium risk** of non-compliance with legislation
Risk scores 20-26	**High risk** of non-compliance with legislation

In addition to answering the above parameters in the risk assessments of the individual review subject, it is possible to make comments about the nature and the amount of instances of non-compliance with legislation reflected in compliance reviews of DSIS, DDIS, CFCS and PPNR to date. This includes whether the non-compliance with legislation constituted breaches of statutory provisions or internal guidelines, or whether the reviews to date have given rise to other comments from TET, which have not concerned specific breaches of statutory provisions or internal guidelines, etc.

It is essential that this opportunity for additional comments is utilised systematically in order to ensure the possibility of keeping the risk score up against factors that the model does not directly take into account. This makes it possible to differentiate and weight the individual risk scores in the ranking of the given review subject in the subsequent risk analysis.

2.3 Ranked risk analysis and review plans

Based on the risk assessments and the individual risk scores, TET prepares risk analyses of DSIS, DDIS, CFCS and PPNR, respectively, concerning TET's own motion reviews. Subsequently, TET prepares a draft review plan based on said reviews for the following year. In addition, TETs prepares separate risk analyses of DSIS and DDIS, respectively, related to TET's reviews based on indirect subject access requests.

In the risk analyses of TET's own motion reviews, review subjects are given priority by highlighting the factors that determine whether a given review subject is included, or up- or down-prioritised in TET's review plan for the following year.

The risk score, which is derived from the prior risk assessments of the review subjects, form the basis for prioritising the review subjects. TET has the option to include additional factors in the risk analysis, including information listed in the risk assessment comments field, which enables a qualified differentiation and prioritisation between the derived risk scores.

In TET's risk analyses, the following additional factors are included in the ranking of review subjects:

Factors included in TET's risk analysis of DSIS, DDIS, CFCS and PPNR

CATEGORY	FACTORS/CONSIDERATIONS
External circumstances	**Political attention.** In the past year, has there been interest at the political level to perform compliance reviews of areas within TET's mandate that have not previously been reviewed or have not been reviewed within the last 3 years?
	Public awareness. In the past year, have there been any cases in the public domain/the media, which should prompt a more detailed compliance review of areas within TET's mandate that have not previously been reviewed or have not been reviewed within the last 3 years?
	International co-operation. In the past year, as part of TET's international co-operation, was any information about review areas within TET's mandate accessed that are not included in TET's risk and materiality assessment of DSIS, DDIS, CFCS or PPNR?
Internal environment in DSIS, DDIS, CFCS or PPNR	**Whistleblowing.** In the past year, has TET received information from current or former employees of DSIS, DDIS, CFCS and PPNR that warrants a more detailed compliance review by TET?
	Areas under development. Are there any areas in DSIS, DDIS, CFCS and PPNR concerning handling of personal data that are or have been undergoing significant changes in the past year?
	Follow-up on previous compliance reviews. Has TET's follow-up on previous compliance reviews of DSIS, DDIS, CFCS and PPNR revealed risks that are not included in TET's annual risk and materiality assessments?
	DSIS', DDIS', CFCS' and PPNR's internal compliance reviews. In the past year, have DSIS', DDIS', CFCS' and PPNR's internal compliance reviews revealed any risks that are not included in TET's annual risk and materiality assessments?
	Security of processing. In the past year, have TETs compliance reviews of DSIS', DDIS', CFCS' and PPNR's security of processing revealed any risks that are not included in TET's annual risk and materiality assessments?
Technology	**Machine Learning (ML) / Artificial Intelligence (AI) and algorithms.** Are there areas in DSIS, DDIS, CFCS and PPNR where automated decision-making or the self-learning algorithms, ML or AI, are used?
	Bycatch. Are there areas in DSIS, DDIS, CFCS and PPNR that make use of technical capabilities that involve a particular risk of obtaining information about non-relevant individuals from an intelligence point of view?
	Application of new technology. Are there areas in DSIS, DDIS, CFCS and PPNR where processing of personal data takes place using non-previously verified technology?

In addition, the risk analyses must contain detailed descriptions of subjects for which it is not possible to calculate a specific risk score based on the above model. This includes TET's detailed assessment of the authority's internal compliance reviews and a general assessment of the IT systems of the DSIS, DDIS, CFCS and PPNR, and whether it is necessary to revise TET's mapping thereof.

Finally, draft review plans for the following year's review of DSIS, DDIS, CFCS and PPNR are prepared based on the risk analyses.

In the risk analyses of TET's reviews based on indirect subject access requests under Section 13 of the DSIS Act and Section 10 of the DDIS Act, it is assessed whether TET's reviews of DSIS and DDIS are adequate considering the risks identified and assessed in the risk assessments. On this basis, it is for TET's board to decide whether the reviews are sufficient or whether they are to be supplemented or downgraded with specified systems.

3 Methodology, performance of compliance review and verification of information

TET uses various methods to review DSIS, DDIS, CFCS and PPNR, including full reviews, random or targeted samplings, content screenings, inspections and interview- and consultation-based reviews.

The selection of methodology is dependent on a specific risk assessment of the review subject based on experiences from previous reviews, the prior technical and legal findings in connection with the specific review, and experience from previous reviews.

Therefore, before a methodology for review is selected, it is essential to determine whether TET has access to the relevant data in its own right and whether the data in question are structured or unstructured data.

3.1 Process for selection of methodology, performance of compliance reviews and verification of information

The process for TET's selection of method of review and performance of compliance reviews is as follows:

DECEMBER: Sending of initial consultations to DSIS, DDIS, CFCS and PPNR regarding technical and legal discoveries of review subjects for the coming year that TET has not previously reviewed or where the prerequisites for compliance reviews have or may have changed (review type A, see Section 3.2).

JANUARY-FEBRUARY: Preparation and approval of review memoranda for review subjects that can be carried out according to an already established method without a start-up meeting with DSIS, DDIS, CFCS or PPNR (review type B, see Section 3.2).

JANUARY-DECEMBER: Performance of compliance reviews of known review subjects (review type B, see Section 3.2).

FEBRUARY-SEPTEMBER: Holding of start-up meetings with DSIS, DDIS, CFCS and PPNR regarding review subjects that TET has not previously reviewed or where the prerequisites for compliance reviews have or may have changed (review type A, see Section 3.2).

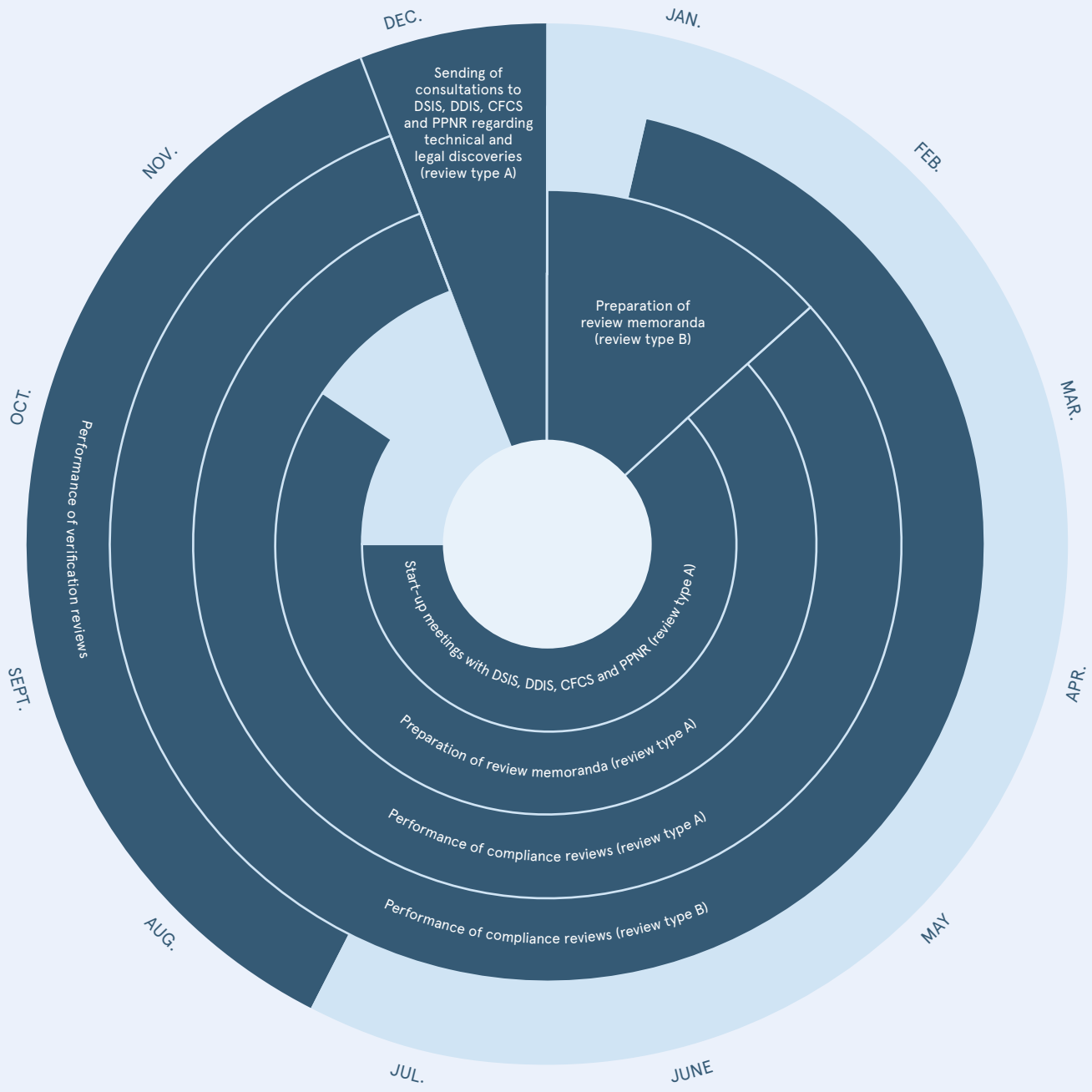
FEBRUARY-OCTOBER: Preparation and approval of review memoranda for review subjects that TET has not previously reviewed, or where the prerequisites for compliance reviews have or may have changed (review type A, see Section 3.2).

FEBRUARY-DECEMBER: Performance of compliance reviews of review subjects that TET has not previously reviewed or where the prerequisites for compliance reviews have or may have changed (review type A, see Section 3.2).

AUGUST-NOVEMBER: Performance of compliance reviews to ensure that information received by TET from DSIS, DDIS, CFCS and PPNR regarding their IT infrastructure is accurate (see Section 3.4). TET's verification reviews are categorised as review type B, see Section 3.2.

Process for TET's selection of method of review, performance of compliance reviews and verification is based on the annual cycle of work.

Annual cycle of TET's selection of methodology, performance of compliance review and verification of information



3.2 Review type

When TET has approved the review plans for the following year's reviews of DSIS, DDIS, CFCS and PPNR (see Section 2), it must initially be assessed whether the individual reviews concern:

REVIEW TYPE A	A new review subject or a subject where the assumptions on which the review is based have or may have changed. As such, there is a need to clarify the framework and method of the review, including by way of a start-up meeting with DSIS, DDIS, CFCS or PPNR. This type of review involves a preliminary consultation with DSIS, DDIS, CFCS or PPNR in order to identify technical, factual and legal matters concerning the review subject (see Appendix 5). In addition, a start-up meeting is held with DSIS, DDIS, CFCS or PPNR before TET determines which methodology of review to apply.
REVIEW TYPE B	A known review subject with a fairly fixed framework for the review, which can be performed according to an already fixed methodology without a start-up meeting with DSIS, DDIS, CFCS or PPNR.

Any decision to that effect is stated in the review plans concerning DSIS, DDIS, CFCS and PPNR next to the individual reviews.

It is TET's caseworker in charge who is responsible for any changes to the assessment of the review type by ad hoc inclusion of new review subjects or, if it turns out that a given review cannot be performed by an already established method.

A change of the assessment must be approved by the Deputy Secretary-General of TET and be updated in the review plan.

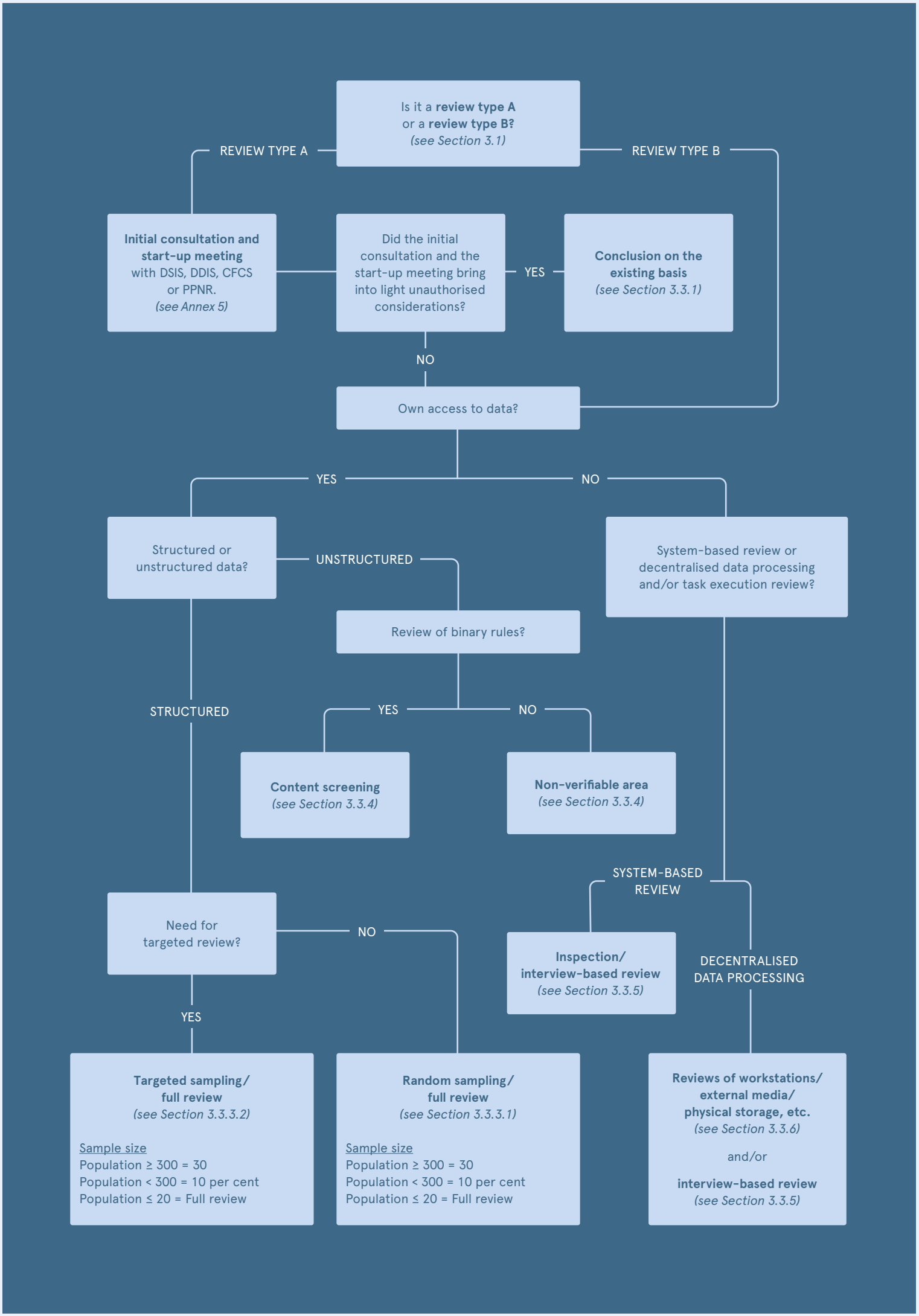
3.3 Review methods

When the review type for a given review subject has been clarified, the method for the review must be determined. The method is selected based on experience from previous reviews, the specific risk assessment of the review subject based on the technical and legal findings at the start-up meetings with DSIS, DDIS, CFCS and PPNR, including the actual issues identified by TET during the specific review.

Therefore, before an review method is selected, it is essential to determine whether TET has access to the relevant data in its own right and whether they are structured or unstructured data.

The different review methods applied by TET are discussed below. It is the responsibility of the caseworker in charge to arrange for an internal discussion of suitable review methods for a given review subject in close dialogue with the relevant Section Leader and other relevant section employees. On this basis, a proposed review method is prepared, which is subject to the approval of the Deputy Secretary-General of TET in all cases.

Overall, TET's selection of review method follows the below procedure:


Is it a **review type A** or a **review type B?** *(see Section 3.1)*
REVIEW TYPE A
REVIEW TYPE B
Initial consultation and start-up meeting with DSIS, DDIS, CFCS or PPNR. *(see Annex 5)*
Did the initial consultation and the start-up meeting bring into light unauthorised considerations?
YES
Conclusion on the existing basis *(see Section 3.3.1)*
NO
Own access to data?
YES
NO
Structured or unstructured data?
UNSTRUCTURED
System-based review or decentralised data processing and/or task execution review?
Review of binary rules?
STRUCTURED
YES
NO
Content screening *(see Section 3.3.4)*
Non-verifiable area *(see Section 3.3.4)*
SYSTEM-BASED REVIEW
Need for targeted review?
NO
Inspection/ interview-based review *(see Section 3.3.5)*
DECENTRALISED DATA PROCESSING
YES
Targeted sampling/ full review *(see Section 3.3.3.2)*
Sample size
Population ≥ 300 = 30
Population < 300 = 10 per cent
Population ≤ 20 = Full review
Random sampling/ full review *(see Section 3.3.3.1)*
Sample size
Population ≥ 300 = 30
Population < 300 = 10 per cent
Population ≤ 20 = Full review
Reviews of workstations/ external media/ physical storage, etc. *(see Section 3.3.6)*
and/or
interview-based review *(see Section 3.3.5)*

3.3.1 Conclusion on the existing basis

If TET's start-up meeting with DSIS, DDIS, CFCS or PPNR brings to light considerations, which, based on an immediate assessment, are not found to be in accordance with applicable legislation, consultation is carried out in order to obtain DSIS', DDIS', CFCS' or PPNR's comments.

If, based on the consultation response, TET still assesses that the considerations in question are not in compliance with the legislation, the review will be finalised based on the existing information. In this connection, TET will inform DSIS, DDIS, CFCS or PPNR that TET will not carry out further data-related reviews of the subject until the relevant considerations have been brought into compliance with the legislation.

If, on the other hand, TET, based on the consultation response, assesses that the considerations in question are in accordance with the legislation or are otherwise not an obstacle to performing a more detailed data-oriented review of the subject, a decision must be made on the review method, cf. Sections 3.3.2-3.3.6.

3.3.2 Full review

A full review of a given review subject may be a very resource-intensive method. Full reviews are thus reserved for very small populations (records/files/individuals, etc. ≤ 20) or exceptional cases where it is deemed essential to examine all of the data.

An imaginary example of small populations could be a review of DDIS' raw data searches where the examination of a specific log extract – where false positives have been sorted out beforehand – shows that within a given review period, DDIS has only made 20 or fewer raw data searches directed at persons resident in Denmark. In this situation, a full review is required.

The category "exceptional cases" contains TET's special review of DDIS in 2019/2020 and cases where it is considered necessary to identify the total number of errors or processing of data in violation of legislation.

In case of populations ≥ 21, sampling must generally be made (see Section 3.3.3), unless, due to exceptional circumstances, full reviews should continue to be made.

3.3.3 Sampling

In a review based on sampling, a small number of records/files/individuals, etc. are sampled from a larger population of data. Thus, sampling is a subset of a population and provides TET with an estimate of the population properties.

Sampling is an efficient method to review large volumes of data. However, it is important to understand how the sample was selected and, by extension, the degree to which the result of the review may be extrapolated to the full data set. By using simple random sampling, i.e. *random sampling* (see Section 3.3.3.1), it is possible to generalise a finding observed in the sample to the whole population (extrapolation).

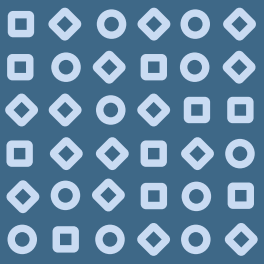
How accurate are TET's samplings?

The advantage of sampling is that it is both faster and less resource-intensive than examining an entire population of records/cases/information about individuals, etc. However, what are the properties of sampling?

SAMPLING

- Averages can be calculated
- The proportion of personal data that has not been collected, processed or disclosed in accordance with the law, can be calculated

POPULATION

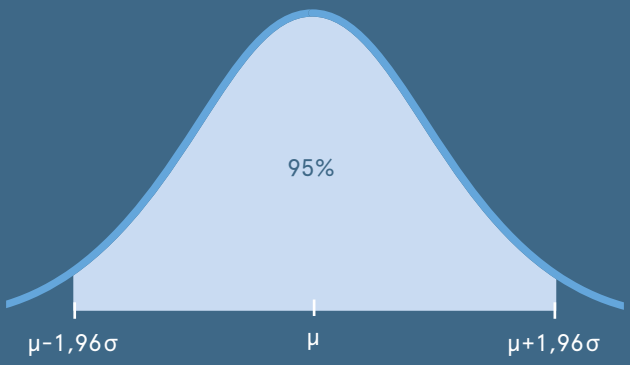


- Average is unknown
- Proportion of personal data not collected, processed or disclosed in accordance with the law is unknown (unless fully audited)

Examining records/cases/information about individuals in a sample makes it possible to make statements about the full population. In other words, this means that a sample gives you an estimate of the population properties.

If a population of records/cases/information about individuals is larger than 10,000, according to the central limit theorem, it can be assumed that the distribution of values in the population corresponds to a normal distribution.

In statistics, **NORMAL DISTRIBUTION** is the most important and most commonly occurring of all probability distributions. For example, it describes the distribution of measurement results when these are subject to some uncertainty. The normal distribution has the shape of a bell curve, where the peak of the curve indicates the mean value (μ) of the statistical material and the width of the curve is a measure of the spread (μ) or standard deviation.



A **CONFIDENCE INTERVAL** is a statistical method of indicating – expressed as a range – how accurate a measurement or sampling is. For example, a 95 per cent confidence interval around a mean value indicates that you expect with 95 per cent certainty that the true measure will fall within this interval.

However, where does the constant 1.96 in the figure come from? If you look at the distribution function for a normal distribution with mean 0 and variance 1, then the total area under the curve is 1. If you are interested in finding the area under the graph that covers 95 per cent of the area, you need to remove 2.5 per cent of the area at both ends. The ±1.96 corresponds to the area under the curve that gives an area of 95 per cent.

The **CONFIDENCE LEVEL** refers to the percentage of times that the confidence interval you calculate will contain the true measure in repeated sampling. A confidence level of 95 per cent is common and means that if you repeated the sampling many times, 95 per cent of the resulting confidence intervals contain the true measure.

In other words, the normal distribution describes the distribution of the data. The confidence interval is a range that estimates the true measure and the confidence level is the percentage of times we expect this range to contain the true measure based on repeated sampling.

The effect of sample sizes is to narrow the confidence interval – that is, the band of guesses around the mean of the estimate – at the same confidence level. With a larger sample size, you can make an accurate statement about the population with the same degree of confidence than with smaller sampling. In small populations, the distribution is slightly different, which means that a sample size can be smaller for the same margin of uncertainty.

For random sampling, TET uses what is known as simple randomised sampling. This fulfils the requirements for applying the probability theory.

TET's **SAMPLING** uses a 95 per cent confidence interval. Thus, at least 95 per cent of the sampling results, if sampled again and again, will contain the true measure of the population; in this case, the percentage of data/cases/records/personal information that has not been collected, processed or disclosed in accordance with the law.

For example, if TET by means of sampling finds that 16 per cent of the extracted personal data has not been collected, processed or disclosed in compliance with the legislation, TET can with a 95 per cent certainty claim that the same is true for the entire population of data.

However, in TET's reviews, it will sometimes be necessary to carry out sampling based on a prior modelling/division of the data (population) by means of methods used in relation to stratification, i.e., dividing the population into mutually exclusive parts (strata), or cluster random sampling. These methodological concepts are used in this standard broadly under the term *targeted sampling* (see Section 3.3.3.2).

3.3.3.1

Random sampling

In simple random sampling, records/files/individuals, etc. are randomly selected for reviewing using a random number generator without prior processing of the data (the population).

TET uses a dedicated random number generator to generate random sampling by entering the size of the population and the ideal sample size.

The sample size depends on the size of the population:

- Population ≥ 300 = 30 records/files/individuals, etc.
- Population < 300 = 10 per cent of records/files/individuals, etc.
- Population ≤ 20 = Full review

If TET's standards for sample size are adhered to, it is possible based on random sampling to extrapolate the finding observed in a sample to the entire population.

3.3.3.2

Targeted sampling

In targeted sampling, records/files/individuals, etc. are randomly selected for reviewing based on prior processing of the data (the population).

Processing of the data includes all forms of targeting in TET's data collection, including by using search strands to retrieve a specific group of files or sort out false positives in connection with a log extract examination.

In targeted sampling, records/files/individuals, etc. are as a general rule randomly selected using TET's random number generator based on the processed data. However, depending on the need for targeting the sampling, it may be useful to select the sampling based on a screening of the processed data, i.e., manual selection of the records/files/individuals, etc. best suited for reviewing.

Like random sampling, the sample size depends on the size of the population:

- Population ≥ 300 = 30 records/files/individuals, etc.
- Population < 300 = 10 per cent of records/files/individuals, etc.
- Population ≤ 20 = Full review

If TET's standards for sample size are adhered to, it is possible based on targeted sampling to extrapolate the finding observed in a sample to the processed population.

3.3.4 Content screening or non-verifiable area

If the data for a review is characterised by unstructured data – i.e. data with no fixed metadata, no efficient retrieval methods and/or no user event logging system being available – TET's reviewing options are substantially limited.

In such situations, the only review option available to TET is to perform its review based on binary rules, i.e. rule-making provisions that do not enable discretionary assessments, such as provisions on time limits for deletion, which may be reviewed by way of content screenings/searches.

In relation to unstructured data, content screening is not a viable method to identify the complete scope of non-compliance with, for example, the provisions on time limits for deletion, but may be used in a general examination of whether a given population contains non-compliance with the provisions. Content screening is used primarily in connection with reviews of DSIS', DDIS', CFCS' or PPNR's deletion of information in decentralised systems where it is not possible to use features in the systems to retrieve information that is older than the deletion deadline.

In cases where TET's reviews are not focused on binary rules and where the data are characterised by unstructured data, the review subject will be classified as a "non-verifiable area" and then submitted to TET for approval (see Section 3.5).

If an review subject is classified as a "non-verifiable area", DSIS, DDIS, CFCS or PPNR will be notified according to the applicable procedure in this respect (see Section 3.6). In this connection, DSIS, DDIS, CFCS and PPNR is requested to put in place as soon as possible pathways for efficient reviews of the review subject. In addition, the public will be made aware of such reviews in the annual reports published by TET on its review activities.

3.3.5 Inspection or interview-based review

If TET does not have access to the relevant data in its own right in relation to a given review subject, it must be clarified whether a system-based review (this section) or a decentralised data processing review and/or task execution review (see Section 3.3.6) – or a combination of the two – is required.

A system-based review includes an examination of the technical and procedural set-up of a given obtaining, processing, disclosure system etc., including, where possible, verification of system compliance with binary rules like, for example, the handling of automated deletion of information.

Generally, a system-based review will take the form of a combination of a system level inspection and an interview-based review that together – in addition to verifying whether the review subject's data management is in compliance with relevant binary rules – are intended to identify risks of non-compliance with legislation.

In an interview-based review it is crucial to prepare a clear frame of questions for the review, including, where relevant, notify DSIS, DDIS, CFCS or PPNR in advance of the overall theme for the review in order to ensure that the relevant technicians/users of the system are available for interview by TET during the inspection.

When preparing the questions for an interview-based review, focus must be on ensuring effective communication between TET and DSIS, DDIS, CFCS or PPNR. In this context, it is important to prepare clear and unambiguous questions the purpose of which is to establish facts. Similarly, where a complex issue is addressed, it is important to ask review-based questions by placing the same question in a new context (supplementary questions).

Data collected from the inspection or the interview-based review must then be compared against the previously collected data in the form of the technical clarification of the review subject and/or data from previous years' reviews.

3.3.6 Review of decentralised data processing

Review of decentralised systems include workstations, transit media and the like where it may be difficult to secure documentation of the results of the review. Thus, in connection with this type of review of decentralised systems, all of the above referenced methods will be applied (Section 3.3.2-3.3.5). However, special focus must be on securing the proper documentation. For this purpose, the selected review methodology will be supplemented by means of the following tools:

- Review form
- Screenshot
- Camera
- Written confirmation

Before the review is initiated, a pre-meeting will be held between those of TET's employees who are assigned to perform the review. During that meeting,

- the individual questions in the review form will be discussed, including what is considered full and satisfactory answers; and
- the matters, which the employees must be particularly aware of in connection with the relevant review, will be discussed.

3.3.6.1

Screenshot

If there is a need in connection with the review to document findings that are stored electronically (e.g. on file drives, etc.), documentation of the finding must be secured according to the following procedure:

1) The DSIS, DDIS, CFCS or PPNR employee is requested to take a screenshot of the finding.
    a. For documentation of files on file drives, the screenshot must clearly show the file type, file name, date of change, date of creation, size and location.
    b. For documentation of emails in mailboxes, a screenshot is taken of the contents of the folder containing the email clearly showing the sender, the subject field and the date of receipt/sending of the email. Where necessary for the review, the contents of the email will also be documented. It must be noted in the form if personal data

are found in several of the emails appearing in the screenshot in order to allow for identification of the emails containing personal data.

c. For documentation of files and emails, the clock in the lower right-hand corner will appear in the screenshot.

2) An appendix number is assigned to the screenshot. The appendix number is noted in the review form together with a brief description of the finding.

3) Next, the legal department of the DSIS, DDIS, CFCS or PPNR will send the document to TET. The DSIS, DDIS, CFCS or PPNR employee's employee number is stated in the subject field of the email.

4) Before sending the email, two of TET's employees will review that the screenshot fulfils the requirements described above.

5) Immediately after the review is completed, it will be verified that TET has received the correct screenshots.

Documentation should also be secured in cases of doubt as to the relevance of a finding. Where necessary, TET's employees will inform the employee in question that the documentation does not necessarily mean that processing has taken place in violation of legislation.

3.3.6.2

Camera

If it has been agreed with DSIS, DDIS, CFCS or PPNR, and if it is necessary in connection with a decentralised data processing review to document a finding which is *not* stored electronically (e.g., in safety cabinets), documentation of the finding must be secured in accordance with the following procedure:

1) TET's employee takes a photo of the finding using specially secured equipment.

a. The photo must clearly show a heading, document date, file number, serial number and other data of importance to the review.

b. The photo must also show where the material was found. Where necessary, two separate photos may be taken of the material and its location.

2) The DSIS, DDIS, CFCS or PPNR employee is requested to estimate for how long the document has been stored at the given location and the answer is noted in the review form.

3) The appendix number of the photo is also noted in the review form together with a brief description of what the photo shows.

4) Immediately after the review, the photos will be transferred to TET's classified system and an appendix number will be assigned to each photo. Finally, the camera's memory card is formatted, thereby deleting all material on it, and then shredded so as to prevent any classified photo material being left on the camera after the review.

Documentation should also be secured in cases of doubt as to the relevance of a finding. Where necessary, TET's employees will inform the employee in question that the documentation does not necessarily mean that processing has taken place in violation of legislation.

3.3.6.3 *Written confirmation*

If it is not possible to document the finding by use of screenshots or camera, for instance, for security reasons, a form brought along by TET's employee is filled in.

In order to ensure consensus about the description of the finding, the form is signed by TET's employee as well as a representative from the legal department of DSIS, DDIS, CFCS or PPNR.

3.4 Verification reviews

Based on TET's mapping of the IT infrastructure in DSIS, DDIS, CFCS and PPNR, TET performs annual verification reviews of the information received.

In other words, TET cross-validates whether servers mapped in DSIS, DDIS, CFCS and PPNR correspond to the servers that are actually running in the IT environments concerned. Furthermore, TET also screens and assesses the relevance of the individual servers for the review. This is reviewed partly by means of annual inspection reviews of DSIS', DDIS', CFCS' and PPNR's virtualisation layers (hypervisor administration tools) and by physical servers in server rooms. At the same time, it is reviewed whether there are any servers that have been turned off or are no longer in use.

The information entered by DSIS, DDIS, CFCS and PPNR in the infrastructure overviews, which are prepared in connection with TET's mapping of IT infrastructure (see Section 1), is verified against the existing servers by cross-checking server names on the infrastructure overview with the current servers appearing in the user and object directory and/or server administration consoles (e.g. hypervisor administration modules) of the DSIS, DDIS, CFCS and PPNR. This requires view-only access to the mentioned administration modules or printouts from DSIS, DDIS, CFCS and PPNR, which may be printed out during an inspection meeting.

Reviews of context and network grades are cross-checked against configuration lists from network equipment and firewalls, including lists of the existing networks (including VLAN).

3.5 Reporting to TET's board

The required decision-making basis must be available before a review is submitted to the members of TET. This is ensured through detailed documentation as well as recording and filing of

- TET's meetings with DSIS, DDIS, CFCS or PPNR;
- TET's specific risk assessment of the review area;
- TET's selection of review method;
- TET's performance of reviews, including log lists, review forms, etc.;

- TET's consultations and responses to consultations; and
- TET's review memorandum (see Section 3.5.1).

Until the abovementioned documentation has been secured, a review may not be submitted to TET's board for discussion and/or approval.

3.5.1 Review memorandum

Review memoranda are a consolidation of all material information concerning a review subject, including

- the background to and purpose of the review as well as TET's overall risk assessment of the subject;
- an objective description of the review subject, including on the basis of information received from DSIS, DDIS, CFCS or PPNR at meetings etc.;
- TET's specific risk assessment of the review subject on the basis of start-up meetings with DSIS, DDIS, CFCS or PPNR;
- TET's selection of review method;
- the results of TET's review; and
- experience gained from performing the review, including an assessment of the need to perform a similar review and/or adjusting the review method in the future, etc.

The template for the preparation of review memoranda is provided in Appendix 6.

Before submission of a review to TET's members, relevant documentation must be recorded and filed. In addition, TET's Deputy Secretary-General must approve the review memorandum.

The review may then be submitted to TET's members for discussion and/or approval, including for inclusion in TET's internal reviews (see Section 3.5.2.3).

3.5.2 Submission of review at board meeting

Once a review is ready for being submitted to TET's members, a recommendation to that effect is prepared in the commented agenda (CA) for the next board meeting. The CA and related appendices are reviewed by the Chair and members of TET in connection with their preparations for the board meeting.

Before a recommendation for the CA is prepared, it must be clarified whether the result is to be recommended for discussion by TET or approval without further discussion at the meeting (see Section 3.5.2.1).

When preparing the recommendation for TET, it is important to ensure that only relevant descriptions/details are included in the CA. This is done to ensure that only clear and uniform recommendations are submitted to TET.

Thus, if a technically and/or legally complex subject is submitted to TET, it is crucial to use fact boxes in the CA and/or to enclose detailed appendices.

3.5.2.1 *Results of reviews for discussion and/or approval*

Generally, a review must only be submitted to TET's board for discussion if the results thereof have given rise to issues of fundamental importance, which need to be put before the decision of the board. In case of doubt, TET's caseworker will clarify this with the relevant Section Leader and/or TET's Secretary-General or Deputy Secretary-General.

If a review is recommended to be submitted to TET's board for discussion, this is indicated in the CA next to the recommendation by a note stating *"to be discussed at board meeting"*.

3.5.2.2 *Submission of appendices*

As a general rule, appendices (technical mappings, review forms, consultations, consultation responses, etc.) are only submitted to TET's board where the review has shown non-compliance with the rules or the review otherwise gives rise to comments to DSIS, DDIS, CFCS or PPNR, which are subsequently to be addressed in a follow-up letter (see Section 3.6).

3.5.2.3 *TET's internal reviews*

TET's reviews are submitted to TET's members at board meetings for the purpose of their discussion and approval. Review material is generally only presented at board meetings when the reviews have given rise to consultations with DSIS, DDIS, CFCS or PPNR (see Section 3.5.2.2).

Consequently, TET's members perform internal reviews of TET's review activities that have not given rise to consultations with DSIS, DDIS, CFCS or PPNR. The reason for this is that a substantial amount of TET's review material is not submitted to TET's board as the material does not document processing in violation of legislation and therefore does not give rise to consultation with DSIS, DDIS, CFCS or PPNR.

The procedure for TET's internal reviews is as follows:

- TET's internal review is performed on material from the reviews that are expected to be completed at the next board meeting.
- The review material included in the internal reviews has not given rise to consultation with DSIS, DDIS, CFCS or PPNR, which is why the material is not appended to the meeting material.
- The reviews of DSIS, DDIS, CFCS or PPNR included in TET's internal review is divided into individual numerical groups and a single number will be assigned to each individual review (e.g. DSIS-1, DDIS-3, CFCS-2, PPNR-2).
- A designated member of TET's board will select one review from each of the agencies subject to review by randomly selecting a number without knowing which review the number relates to.
- The designated member of TET's board will receive a review form for each randomly selected review.
- The designated member of TET's board will also receive a review memorandum as well as other relevant documentation for each randomly selected review so that

the member attains background knowledge for the reviews, including material on the selection of method and evaluation of the results. This will provide TET's board with more detailed knowledge about TET's considerations in relation to the specific review as well as the consequences of the review as far as future reviews concern.

- Finally, the designated member of TET's board will receive a review form, which can be used to write down comments. The member signs the review form when the internal review is completed.

- The designated member of TET's board will present the results of the internal review at the next board meeting.

3.6 Reporting to DSIS, DDIS, CFCS and PPNR

When TET's board has approved a review, a follow-up letter will be sent to DSIS, DDIS, CFCS or PPNR. A template for the draft follow-up letter is provided in Appendix 7.

When TET's board has approved the follow-up letter, it is signed by the Chair of TET and then, without undue delay, sent to DSIS, DDIS, CFCS or PPNR.

3.7 Reporting to the Minister of Justice, the Minister of Defence and publication of TET's annual reports

Based on the follow-up letters sent by TET to DSIS, DDIS, CFCS and PPNR within a given review year, TET prepares annual reports, which are submitted to the Minister of Justice (DSIS and PPNR) and the Minister of Defence (FE and CFCS), respectively.

TET's draft reports are generally approved at a board meeting held in late February, after which TET submits the reports to DSIS, DDIS, CFCS and PPNR, respectively, for clarification of whether the reports contain classified or incorrect information.

After reporting to the Minister of Justice and the Minister of Defence, TET will await information on when the reports have been submitted to the Parliamentary Intelligence Services Committee, after which the reports may be published.

3.8 Detailed process description

In the following section, the process of TET's reviews is described:

PROCESS	DEADLINE

1. Practical preparation of reviews

December

a. *Creating records* for all reviews on the annual review plan

b. *Categorising* all planned reviews as either review types A or B

c. *Assign a responsible caseworker* for each review

d. *Briefing and potential meeting with DSIS, DDIS, CFCS and PPNR* about the review plan for the coming year

1.A SENDING OF PRELIMINARY CONSULTATION (APPLIES ONLY TO REVIEW TYPE A)

a. *Sending of* preliminary consultation notice containing information sheet for all reviews (review type A), including a call for a start-up meeting (see Appendix 5) — End of December

The start-up meeting is called stating a week number. The meeting may be scheduled starting from week 8 at the earliest

The consultation period is set to Monday at the end of working hours two weeks before the week of the start-up meeting

Example of setting a consultation period:
Sending out a consultation notice with accompanying information sheets and a call for a start-up meeting to be held during week 8. The response deadline for request will be Monday of week 6 by the end of the day

b. *Adding dates* for consultation and consultation period applicable to the record

1.B PREPARATION OF START-UP MEETING (APPLIES ONLY TO REVIEW TYPE A)

a. *Review of* consultation responses with accompanying information sheet — Before start-up meeting

b. *Preparation of questionnaire* in the information sheet for the start-up meeting

c. *Inclusion of infrastructure overview* where relevant

1.C START-UP MEETING (APPLIES ONLY TO REVIEW TYPE A)

Preparation — N/A

a. *Print* relevant material for all attendees prior to the meeting

b. *Internal discussion* of the material and the questionnaire prior to the meeting

Summary

a. *Review* the results of the meeting with other meeting attendees from TET

b. *Recording* answers to the questionnaire in the information sheet for the start-up meeting

c. *Forwarding* any unresolved questions and queries to DSIS, DDIS, CFCS or PPNR

2. Decision on review methodology

Own reviews

a. *Review* whether TET has access and relevant user rights to the review subject

b. *Examine* how the review subject is accessed (application, web or the like) and works (client and system), including functions, types of data and interfaces

Review type A
No later than 1 week after the start-up meeting was held

Review type B
By week 6 at the latest

PROCESS	DEADLINE
c. *Request access/user rights* if TET does not have the relevant access to the review subject	
d. *Retrieve existing information* on the review subject, including, for example, previous review memoranda, IT landscape, detail form, own notes and DSIS, DDIS, CFCS or PPNR documentation, etc.	
e. *Record and file* all relevant documentation	
Determining the review methodology	
a. *Prepare* recommendation for review method (see Section 3.3) by filling in Sections 1-4 of the review memorandum (see Appendix 6) with the involvement of the Section Leader	
b. *Record and file* review memorandum, information sheet and any additional relevant material	
c. *Send draft review memorandum for comments* to the individuals who attended the start-up meeting	
d. *Incorporate* any comments	
e. *Approval of review memorandum* (Sections 1-4) by TET's Deputy Secretary-General	
3. Performance of reviews	
Performing the review	N/A
a. *Perform the review* according to the approved method	
b. *Approval of review form* by TET's Section Leader	
In case of potential non-compliance with legislation, send consultation notice to DSIS, DDIS, CFCS or PPNR	
a. *Approval of draft consultation* by TET's Secretary-General	
b. *Setting a consultation period* in accordance with TET's process of consultation with DSIS, DDIS, CFCS and PPNR (see appendix)	
c. *Adding dates* for consultation and consultation period to the record	
Receiving of consultation responses	
a. *Record and file* consultation responses	
b. *Add date* for consultation responses to the record	
4. Completion of review	
Approval of review memorandum	No later than one week before the board meeting is held
a. *Complete* draft review memorandum	
b. *Approval* of review memorandum (Section 5) by TET's Deputy Secretary-General	
Approval of follow-up letter and item for commented agenda (CA) for board meeting	
a. *Prepare* draft follow-up letter and item for CA for the board meeting and submit for the approval of TET's Section Leader	
b. *Submission* for final approval by TETs Secretary-General	
c. *Final approval* of follow-up letter at board meeting	

PROCESS	DEADLINE
Sending of follow-up letter to DSIS, DDIS, CFCS or PPNR a. *Send* follow-up letter to DSIS, DDIS, CFCS or PPNR b. *Finalise recording and filing* of the review c. *Enter review* in TET's the follow-up review forms for the coming year	Within three days after the board meeting is held
Receiving of comments a. *Receipt* any comments from DSIS, DDIS, CFCS or PPNR b. *Decide* whether comments give rise to corrections or additions to previously submitted follow-up letter	4 weeks after sending the TET follow-up letter

5. Preparation of TET's annual reports

Approval of drafts for TET's annual reports a. *Approval* of draft reports at board meeting	Weeks 8-13
Consult with DSIS, DDIS, CFCS and PPNR a. *Submit* drafts of TET's annual reports to DSIS, DDIS, CFCS and PPNR for clarification of whether the drafts contain classified or incorrect information. The consultation period is set to 2 weeks. b. *Incorporate* any comments from DSIS, DDIS, CFCS or PPNR	Weeks 9-14
Submission of TET's annual reports on DSIS, including PPNR, DDIS and CFCS, to the Minister of Justice and the Minister of Defence, respectively	N/A
Publication of TET's annual reports on DSIS, including PPNR, DDIS and CFCS	Once TET has received a briefing from the Ministry of Justice and the Ministry of Defence that the reports have been presented to the Parliamentary Intelligence Services Committee

Appendix

APPENDIX A

Glossary

This glossary explains the most important concepts used in these standards.

CONCEPT	EXPLANATION
Binary rules	Rule-making provisions that do not form the basis of discretionary assessments. For example, provisions on time limits for deletion, which may be verified by way of simple look-ups.
Review subject	The subject of TET's review, i.e. system/process/area, which TET has decided to review.
Review type A	A new area or an area where the assumptions on which the review is based have or may have changed and, as such, there is a need to clarify the framework and review methodology, including by way of scheduling a start-up meeting with DSIS, DDIS, CFCS or PPNR.
Review type B	A known review subject with a fairly fixed framework for review, which can be performed according to an already established method without scheduling a start-up meeting with DSIS, DDIS, CFCS or PPNR.
Population	The entire data being subject to a specific review.
Sampling	A smaller set of data from a larger population. Sampling may be selected randomly or based on targeted parameters (see Section 3.3.3).
Unstructured data	Data with no fixed metadata, no efficient retrieval methods and/or no user event logging system being available.

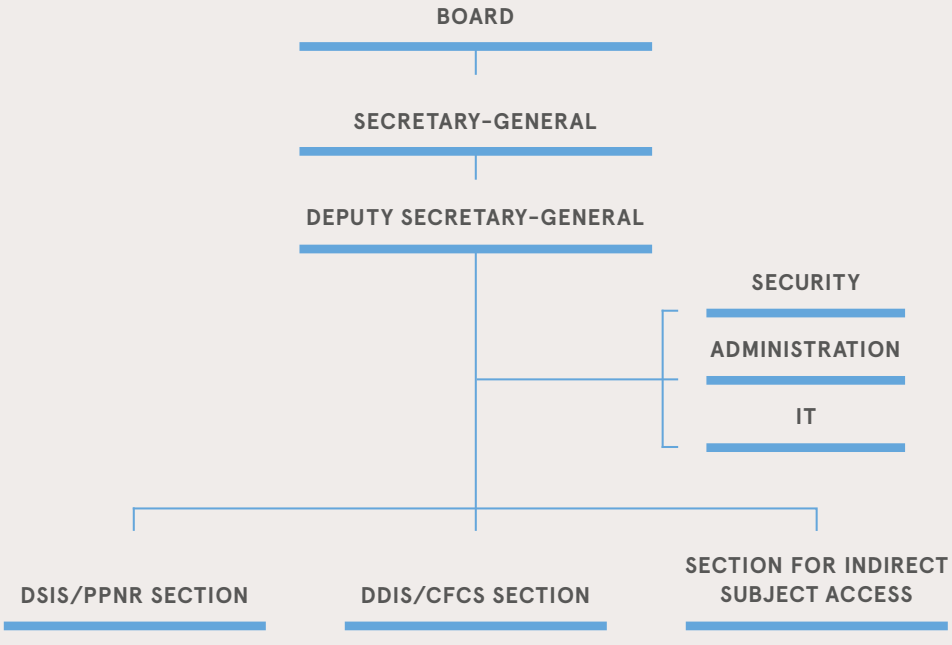
APPENDIX B

TET's organisation

TET's board is composed of five members appointed by the Minister of Justice following consultation with the Minister of Defence. The Chair, who must be a High Court judge, is appointed on the recommendation of the Presidents of the Danish Eastern and Western High Courts, while the remaining four members are appointed following consultation with the Parliamentary Intelligence Services Committee.

TET's board is supported by a secretariat, which is subject solely to the instructions of the board in the performance of its duties. TET recruits its own staff for the secretariat and, as such, decides which educational and other qualifications the relevant candidates must have. The main professional groups employed in TET are lawyers, political scientists and IT specialists.

TET is divided into sections, which are concerned with DSIS/PPNR, DDIS/CFCS, respectively, and indirect subject access requests. In order to ensure subject-matter coordination and experience sharing, TET's staff works across sections.



APPENDIX C

General requirements for review and TET's expectations of DSIS, DDIS, CFCS and PPNR

TET's review activities contribute to the legitimisation of the activities carried out by DSIS, DDIS, CFCS and PPNR by strengthening public confidence in the legality of these activities.

TET's operations are determined by law. As such,

- TET, following a complaint or on its own initiative, oversee that DSIS, DDIS, CFCS and PPNR processes personal data in compliance with the legislation,
- TET may require DSIS, DDIS, CFCS and PPNR to provide any information and material of importance to TET's activities,
- TET is entitled at any time to access any premises where the information in question is being accessed or where technical facilities are being used,
- TET may require DSIS, DDIS, CFCS and PPNR to provide written statements on factual and legal matters of importance to TET's activities,
- if DSIS, DDIS, CFCS or PPNR, in exceptional cases, decide not to follow a recommendation in a statement from TET, they must submit the matter, without undue delay, to the Minister of Justice or the Minister of Defence, respectively, for a decision,
- TET informs the Minister of Justice and the Minister of Defence, respectively, of matters that the respective ministers, in the opinion of TET, should be aware of, and
- TET must submit annual reports on its activities, which must be published.

If DSIS, DDIS, CFCS or PPNR fails fully to comply with these basic requirements for effective and fair compliance review, it will significantly weaken TET's ability to verify the legality of the DSIS, DDIS, CFCS or PPNR, thereby ensuring the legitimacy of the authorities in the eyes of the public.

TET has the following expectations for DSIS, DDIS, CFCS or PPNR in their fulfilment of these requirements:

TET's access to information

TET expects DSIS, DDIS, CFCS or PPNR to provide TET with unrestricted, complete and timely access to all material relevant for TET to carry out correct and effective compliance reviews.

TET expects that DSIS, DDIS, CFCS or PPNR ensure that TET has the correct user access to the IT infrastructure of DSIS, DDIS, CFCS or PPNR, ensuring direct and unrestricted access to relevant information for TET's review.

TET expects that in cases where full information and user rights cannot be provided for technical reasons to selected parts of DSIS', DDIS', CFCS' or PPNR's IT infrastructure, that TET be informed of

- the nature and the full scope of the part of the IT infrastructure to which TET does not have access in its own right; and
- the nature and scope of the data processed in the part of the IT infrastructure to which TET does not have access in its own right.

Unrestricted, complete and timely access to material relevant to TET's operations is essential in order to maintain effective and accurate review activities.

In special circumstances, DSIS, DDIS, CFCS or PPNR will be able to deliver an opinion on failure to review selected pieces of information. To ensure compliance with requirements for TET's statutory access to information, however, TET alone has the power to decide whether selected pieces of information can be omitted in connection with a review.

If TET is unable to verify that the information in question, which DSIS, DDIS, CFCS or PPNR has requested be omitted in connection with a review, is not relevant for the review activities undertaken by TET, this will pose a significant risk of circumvention of the law.

Responding to TET's consultation notices

TET expects consultation responses from DSIS, DDIS, CFCS or PPNR to be complete, transparent and unbiased.

TET expects DSIS, DDIS, CFCS or PPNR to inform TET of the existence of other relevant information or material of importance to the review activities, which DSIS, DDIS, CFCS or PPNR acknowledges that TET does not have access to.

TET expects DSIS', DDIS', CFCS' or PPNR's consultation responses to be submitted in a timely manner and within the timeframes set out in TET's consultation process (see TET's consultation process in relation to DSIS, DDIS, CFCS and PPNR).

In order to ensure effective and accurate compliance reviews, TET submits targeted requests for opinions on issues of factual and legal matters of importance to TET's activities.

TET has the decision-making powers in deciding whether selected pieces of information are relevant to the compliance review, which is why the consultation responses submitted by DSIS, DDIS, CFCS and PPNR must be complete, transparent and unbiased.

Thus, when submitting consultation responses to TET, DSIS, DDIS, CFCS or PPNR are not permitted to independently assess whether selected requests for information are relevant to TET's activities.

Follow-up on TET's compliance reviews

TET expects – if DSIS, DDIS, CFCS or PPNR have any comments on the results of the individual reviews carried out by TET – that these comments be forwarded to TET by the deadline stated in TET's follow-up letter.

TET expects – if, in exceptional cases, DSIS, DDIS, CFCS or PPNR decides not to follow a recommendation from TET – that they fulfil their duty of disclosure and without undue delay submit the case to the Minister of Justice or the Minister of Defence, respectively, for decision.

Practices that TET deems to be unlawful, and where DSIS, DDIS, CFCS or PPNR is in agreement, must cease immediately, and disagreements with regard to the interpretation of the legal basis should be resolved without undue delay. Thus, it is crucial that DSIS, DDIS, CFCS or PPNR respond in a timely manner to TET's recommendations, including, if necessary, by submitting a given case to the Minister of Justice and the Minister of Defence, respectively, for decision.

APPENDIX D

Scale of TET's comments to DSIS, DDIS, CFCS and PPNR

TET's comments to DSIS, DDIS, CFCS and PPNR, forwarded in a classified follow-up letter (see Appendix 7) and subsequently published in TET's annual reports on its activities in an unclassified version, are based on the following scale:

COMMENTS	BASIS OF COMMENTS
*[...] **does not give rise to any comments***	Used when TET agrees with DSIS, DDIS, CFCS or PPNR on how they are generally or specifically administering the law.
*TET finds **no** grounds on the existing basis **for assessing** [...]*	Used when TET's review is limited by either factual or legal circumstances.
*TET finds it **striking** [...]*	Used for situations in DSIS, DDIS, CFCS, PPNR or the legislation which do not quite match the general or immediate impression of an outsider.
*TET finds it **problematic** [...]*	Used for situations where no actual non-compliance with legislation has been established, but where there is considered to be a high risk that the situation could lead to non-compliance with legislation or where TET has been prevented from performing its activities for a certain period of time.
*TET has **identified** [...]*	Used for situations where actual non-compliance with legislation of an isolated nature or non-compliance with internal guidelines has been identified.
*TET finds it **criticisable** [...]*	Used for situations where actual non-compliance with legislation of a not insignificant extent has been identified or where TET has been prevented from exercising its activities for a prolonged period.
*TET finds it **highly criticisable** [...]*	Used for situations where serious non-compliance with legislation has been identified or where TET has been prevented from performing its activities for a prolonged period without DSIS, DDIS, CFCS or PPNR having demonstrated a willingness to ensure the necessary remedial action.

APPENDIX E

TET's process for consulting DSIS, DDIS, CFCS and PPNR

The following process applies to TET's consultation with DSIS, DDIS, CFCS and PPNR, respectively:

1) When sending a consultation notice, TET sets a consultation period of 25 working days. The consultation period starts from the first working day upon receipt of the consultation notice. The following weeks are not included when determining the duration of consultation periods:

   - Week 7
   - Weeks 28, 29 and 30
   - Week 42
   - Week 52

2) If the scope or complexity of the consultation means that TET believes that a response is not possible within 25 working days, TET shall set a consultation period of 60 working days.

3) If, after receiving a consultation notice from TET, DSIS, DDIS, CFCS or PPNR finds that the consultation notice cannot be accommodated within the specified consultation period, DSIS, DDIS, CFCS and PPNR have the following options:

   Upon receipt of a consultation notice with a response period of *25 working days*

   i. In exceptional cases, DSIS, DDIS, CFCS or PPNR may request in writing that TET extend the consultation period from 25 working days to 60 working days. It is assumed that the request is generally made no later than *15 working days* upon receipt of the consultation notice and includes a specific justification.

   Upon receipt of a consultation notice with a response deadline of *60 working days*

   ii. In exceptional cases, DSIS, DDIS, CFCS or PPNR may respond in writing within 15 working days of receipt of the consultation notice from TET that it will not be possible to respond to the consultation notice by the specified deadline. It is assumed that the request includes a specific justification.

   In this case, TET will cease reviewing the area in question, after which TET will enter into a dialogue with DSIS, DDIS, CFCS or PPNR in terms of when the review area is expected to be ready for reviews.

   Subsequently, it will appear from TET's annual report that the planned review measures could not be carried out in the current year, but that TET and DSIS, DDIS, CFCS or PPNR are engaged in a discussion on preparing the area for future review.

[Danish Security and Intelligence Service /
Danish Defence Intelligence Service /
Centre for Cyber Security /
PNR Unit of the Danish Police]

Danish Intelligence Oversight Board

Date:
Caseworker: [Name 1] [Name 2]
File no.: [Case no.]
Doc.: [Document no.]

Request regarding [DSIS', DDIS', CFCS' and PPNR's] IT infrastructure

TET plans, adapts and implements its reviews of [DSIS, DDIS, CFCS and PPNR] based on ongoing annual risk and materiality assessments of [DSIS', DDIS', CFCS' and PPNR's] work processes and IT systems.

TET's knowledge of [DSIS', DDIS', CFCS' and PPNR's] IT infrastructure, including systems, is essential for the completeness of the review as well as for TET's ability to assess risks in relation to [DSIS', DDIS', CFCS' and PPNR's] procurement, processing, deletion and disclosure of data.

For the purpose of its subsequent processing and compilation of data, TET needs to collect the information by filling out the attached Excel template, which is referred to as the "Infrastructure overview". The template includes the minimum amount of information that TET deems sufficient to obtain a general overview of what networks, domains and servers currently exist and which IT systems are running on them.

Accordingly, TET request that [DSIS / DDIS / CFCS / PPNR] complete the enclosed Infrastructure overview (see the enclosed Appendix A) containing information about all networks and all servers, both virtual and physical ones, located in all of parts of the IT environments and forward them to TET by 1 May [year], cf. [Section 20(3) of the DSIS Act / Section 17(3) of the DDIS Act / Section 22(3) of the CFCS Act].

Yours sincerely,
Danish Intelligence Oversight Board

by/[Name]
[Titel]

Borgergade 28, 1
DK-1300 Copenhagen K
t +45 25 50 10 34
www.tet.dk

Guide to completing TET's infrastructure overview

INTRODUCTION AND PURPOSE

TET's infrastructure overview is divided into two separate tabs containing a network list and a server list, which together aim to map the full IT infrastructure in DSIS, DDIS, CFCS and PPNR, respectively. Compilation and assessing the information from the network list (see tab A. Network list) and the server list (see tab B. Server list) provides TET with a basic understanding of the structure and coherence of the IT infrastructure in DSIS, DDIS, CFCS and PPNR. Based on the infrastructure list, among other things, TET annually prepares a list of systems in DSIS, DDIS, CFCS and PPNR, which forms the basis for TET's annual risk and materiality assessments of DSIS, DDIS, CFCS and PPNR. Based on the risk and materiality assessments, TET determines its annual review plans.

The network list can be used in conjunction with the server list to cross-check and validate the existence of

- networks, environments or VLANs that TET is not already familiar with,
- networks, environments or VLANs for which no associated servers or systems are disclosed,
- systems or servers associated with networks, environments or VLANs that are not on the network list,
- servers that are not part of an IT system,
- systems and/or servers that TET is not yet aware of, and
- systems and/or servers that have been added or removed since the last update.

The infrastructure overview also allows TET to cross-check and validate whether the servers on the server list correspond to the servers that are actually running in the IT environments at DSIS, DDIS, CFCS and PPNR.

TET has chosen to annually map DSIS', DDIS', CFCS' and PPNR's IT infrastructures in this Excel template, which includes the information that TET currently deems necessary to obtain an overview of the current networks and domains as well as the systems that exist on said networks and domains.

TET's IT mapping process is described in detail in TET's standards, which are available at www.tet.dk.

INSTRUCTIONS FOR THE INDIVIDUAL COLUMNS ON TAB A. NETWORK LIST

System call name for IT environment/ security context	In this column, enter the system call name(s) by which the individual IT environment/security context is referred to on a daily basis. An IT environment/security context is defined in this context as a grouping of one or more VLANs on a physical network that together form a separate IT environment, such as a production, test, retrieval, processing or development environment.
Physical network name	In this column, enter the name of the physical network. A physical network in this context is defined as a local area network (LAN) consisting of network components connected by cables (fibre, UTP, STP or similar) delimited by e.g. airgaps or diodes.
VLANs in IT environment/ network context	In this column, indicate which VLANs are included in each IT environment/security context.
Network classification	In this column, indicate the highest classification that the current network is authorised for.
Brief description of the use/ function/role of the IT environment/security context	In this column, provide a brief description of what the IT environment/security context is used for, e.g. test environment for internal IT or used to test new systems, only anonymised information is used for testing.

INSTRUCTIONS FOR THE INDIVIDUAL COLUMNS ON TAB B. SERVER LIST

Name	In this column, enter the name of the server. All physical and virtual servers on all networks must be listed in this column. If a server with the same name is found in three different IT environments/security contexts, the server name must appear three times in this column. The name of the server is specified as either NETBIOS name or DNS name.
System name	In this column, specify the business system(s) that the server is part of. System names entered in this column will form the basis of TET's annual risk and materiality assessment and review plan for the coming

	year. For this reason, it is important that the system names used are consistent with the system names used in e.g. a retention plan, asset lists, documentation systems or in the organisation in general. It is also important that all systems that the server is part of are added to the list. For example, if a database server and a file server are used in system A and system B, both systems are listed next to both servers. Servers that handle e.g. print, shares for installation software, Active Directory, terminal servers, Citrix infrastructure, antivirus, DHCP, DNS, VCenter, certificate infrastructure, jump servers, load balancing, management servers for network components SAN or similar are listed in this column as "Infrastructure". Similarily, a brief description of the server's function is listed in the column "Brief description of the server's function/role". If the server cannot be connected to with a system or categorised as infrastructure, enter N/A and add an explanatory description under "Brief description of the server's function/role".
System call name for IT environment/security context	In this column, indicate which IT environment/security context the server is connected to. It is important that the nicknames used in this column are unambiguous throughout this table and consistent with the network list (see the Network Overview guide for further description of the concept of IT environment/security context), so that TET can get an overview of which servers/systems are present in each IT environment/security context. If one server is connected to multiple IT environments/security contexts, please specify all of them.
VLAN ID	In this column, specify the ID of the VLAN to which the server is connected in the current IT environment/security context. If no VLAN technology is used in the IT environment/security context to which the server is connected, this is indicate as "VLAN not used".
DNS domain	In this column, indicate whether the server is part of a DNS domain. If so, it must be specified with the DNS name (e.g. statens-it.local) as N/A or the workgroup name.
Primary software	In this column, specify the server's primary software product. If the server is a database server, the primary software product could be MSSQL, Oracle, MySql, MongoDB or similar. If the server's primary function is based on a function that is built into the operating system, DNS, print, file sharing, DFS or similar can be specified, depending on which service the server provides.
Brief description of server function/role	In this column, provide an explanation and/or remarks regarding the server's function, data or other relevant pieces of information that may help to understand the server's role in the service's IT environment.

A. Network list

CALL NAME OF IT ENVIRONMENT/SECURITY CONTEXT	NAME OF PHYSICAL NETWORK	VLANS IN IT ENVIRONMENT/ SECURITY CONTEXT	CLASSIFICATION OF NETWORK	BRIEF DESCRIPTION OF THE USE/ FUNCTION/ROLE OF THE IT ENVIRONMENT/ SECURITY CONTEXT
***Example** – DMZ*	*DMZ-net*	*242*	*UNCLAS*	*Exposes external services such as authentication and mail services*
***Example** – Closed network*	*HEM-FiberNet*	*36, 42, 43, 46, 47, 48, 49*	*HEM*	*Used for final analysis of cases and general administration*
***Example** – DEV-net, Sandbox*	*HEM-FiberNet*	*568,570, 599*	*HEM*	*Used in connection with the development and initial functional testing of proprietary software, as well as initial testing of customised systems*
***Example** – STAG-net, Staging*	*HEM-FiberNet*	*663, 664, 665*	*HEM*	*Used for final installation tests that are tested exclusively using anonymised test data.*
***Example** – Open network*	*UNCLAS-UTPNet*	*250, 251, 260*	*UNCLAS*	*Used by users for non-operational email communication with external stakeholders.*
***Example** – Visitors network*	*WLAN-internet*	*128-136*	*UNCLAS*	*Used for guests who wish to connect a device they brought with them, or employees who wish to update phones or tablets. Please note that the network only provides internet access.*

B. Server list

NAME	SYSTEM NAME	CALL NAME FOR IT ENVIRONMENT/ SECURITY CONTEXT	VLAN ID	DNS DOMAIN	PRIMARY SOFTWARE	BRIEF DESCRIPTION OF SERVER FUNCTION/ ROLE
Server name (NETBIOS or DNS)	**Business system(s) of which the server is part of**	**Specify call name for the IT environment/ security context the server is part of**	**Enter the ID of the VLAN the server is connected to**	**If the server is part of a DNS domain, please specify accordingly, otherwise specify N/A or workgroup**	**The server's primary software product**	**Explanations and/or comments regarding the server's function, data or other relevant facts that can help clarify the server's role**
***Example** – ServerX*	*Infrastructure*	*HEM-NET*	*42*	*HEMDOM.local*	*Windows AD*	*User database in the form of Microsoft Active Directory, which is used in connection with user validation.*
***Example** – ServerY*	*Hobbit / ComBIT*	*HEM-NET*		*N/A*	*Data diode Receiver*	*Receives messages via email from UNCLAS-NET to the HEM-NET network.*
***Example** – ServerZ*	*Historical archive*	*HEM-NET*	*36*	*HEMDOM.local*	*ScanArkiv 4.0*	*Contains all scanned documents and OCR recognises all PDF files.*
***Example** – ServerQ*	*Infrastructure and Systems E, D and G*	*HEM-NET*	*46*	*HEMDOM.local*	*Splunk 5.6*	*Splunk is used to search log files delivered from systems E, D and G.*
***Example** – ServerR*	*Analysis system*	*HEM-NET*	*43*	*HEMDOM.local*	*Linux*	*File server for Linux-based analysis system*
***Example** – ServerS*	*Hobbit / ComBIT*	*UNCLAS-NET*	*128*	*N/A*	*Data diode Sender*	*Sends messages via email from UNCLAS-NET to the HEM-NET network.*
***Example** – ServerT*	*Infrastructure*	*HEM-NET*	*42*	*HEMDOM.local*	*Windows*	*File server on HEM-NET – Hosts all departmental drives.*
***Example** – ServerU*	*Systems E, D and G*	*HEM-NET*	*46*	*HEMDOM.local*	*MS SQL 2019*	*Operational data, data is stored in 3 different databases and read/edited via systems E, D and G*

System list [year]

REFERENCE					SYSTEM NAME	SHORT SYSTEM DESCRIPTION	NETWORK/CONTEXT/ ENVIRONMENT	APPLIED SYSTEM LIST	RELEVANCE SCORE	RELEVANCE ASSESSMENT	NAME CHANGE
Infrastructure overview (year)	Documentation received (year)	Asset management (year)	ESDH identified (year)	Management system (year)	State system name	Provide brief description of the system	State the environment, context or network on which the system is running. If the system is running on multiple environments, please specify which.	State the name of the system list on which the system was originally added.	Systems are broken down into 3 categories: 3. Not relevant system 2. Relevant system 1. Relevant system where a review is recommended	Written explanation of or comment on category breakdown, if applicable.	Specify whether an existing system has been renamed, including the systems most recent names
				x	***Example*** *- MAILMAN*	*Mail system used by all users on HEM-NET to send emails internally*	*HEM-NET*		*2*		*No*
	x				***Example*** *- GOLIAT*	*Used to register bugging, including formalities regarding creation and removal*	*HEM-NET*		*1*	*This system is complex and entails manual workflows. In addition, it appears to contain large amounts of legacy personal data.*	*Yes, DAVID*

COMMENTS

RISK SCORE ACCORDING TO LEGAL BASIS

0-5 = Low risk
6-12 = Limited risk
13-19 = Medium risk
20-26 = High risk

ANY COMMENTS BY TET?

No or N/A = 0
Yes, minor comments in connection with previous compliance check (≤ 3 years) = 1
Yes, minor comments in connection with most recent compliance check = 2
Yes, material comments in connection with previous compliance check (criticisable/highly criticisable) (≤ 3 years) = 3
Yes, material comments in connection with most recent compliance check (criticisable/highly criticisable) = 5

ANY ERRORS REVEALED BY TET'S COMPLIANCE CHECKS?

No or N/A = 0
Yes, minor errors in connection with previous compliance check (≤ 3 years) = 1
Yes, minor errors in connection with most recent compliance check = 2
Yes, non-compliance with legislation in connection with previous compliance check (≤ 3 years) = 3
Yes, non-compliance with legislation in connection with most recent compliance check = 5

TET'S MOST RECENT COMPLIANCE CHECK?

≤ 1 year or N/A = 0
2 years = 1
3 years = 2
≥ 4 years = 3

ANY COMPLIANCE CHECKS PERFORMED BY TET?

Yes or N/A = 0
No = 2

ANY ERRORS REVEALED IN CONNECTION WITH INTERNAL COMPLIANCE CHECKS?

No or N/A = 0
Yes, minor errors = 1
Yes, non-compliance with legislation = 2

INTERNAL COMPLIANCE CHECKS?

Yes, satisfactory or N/A = 0
Yes, but ad hoc/decentralised/not satisfactory = 1
No or Unknown = 3

INTERNAL LEGAL COMPLIANCE CHECKS?

Yes, including established practice in place for legal approval or N/A = 0
Yes, but no established practice in place for legal approval = 1
No or Unknown = 3

LOGGING AND RIGHTS MANAGEMENT?

Yes, to a relevant extent or N/A = 0
Yes, but to a lesser relevant extent = 1
No = 2
Unknown = 3

LOCATION OF PROCESSING?

Central, and TET has independent access or N/A = 0
Central, but TET has no independent access = 1
Decentralised = 2
Unknown = 3

METHOD OF DATA PROCESSING?

Automated or N/A = 0
Semi-automated = 1
Manual = 2
Unknown = 3

EXTENT OF PERSONAL DATA?

Minor extent or N/A = 0
Material extent = 2
Unknown = 3

DATA QUALITY?

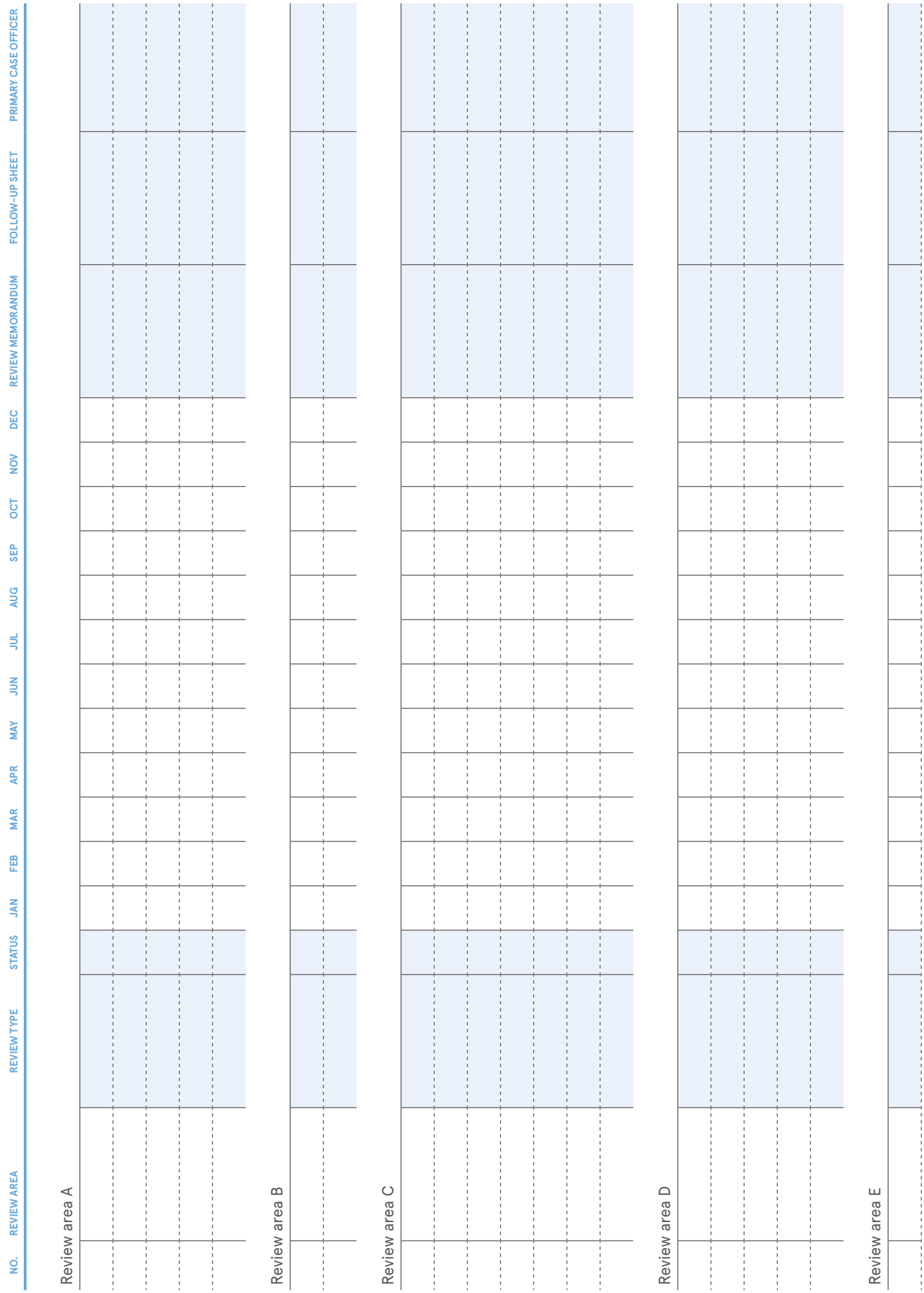
Structured or N/A = 0
Unstructured = 2
Unknown = 3

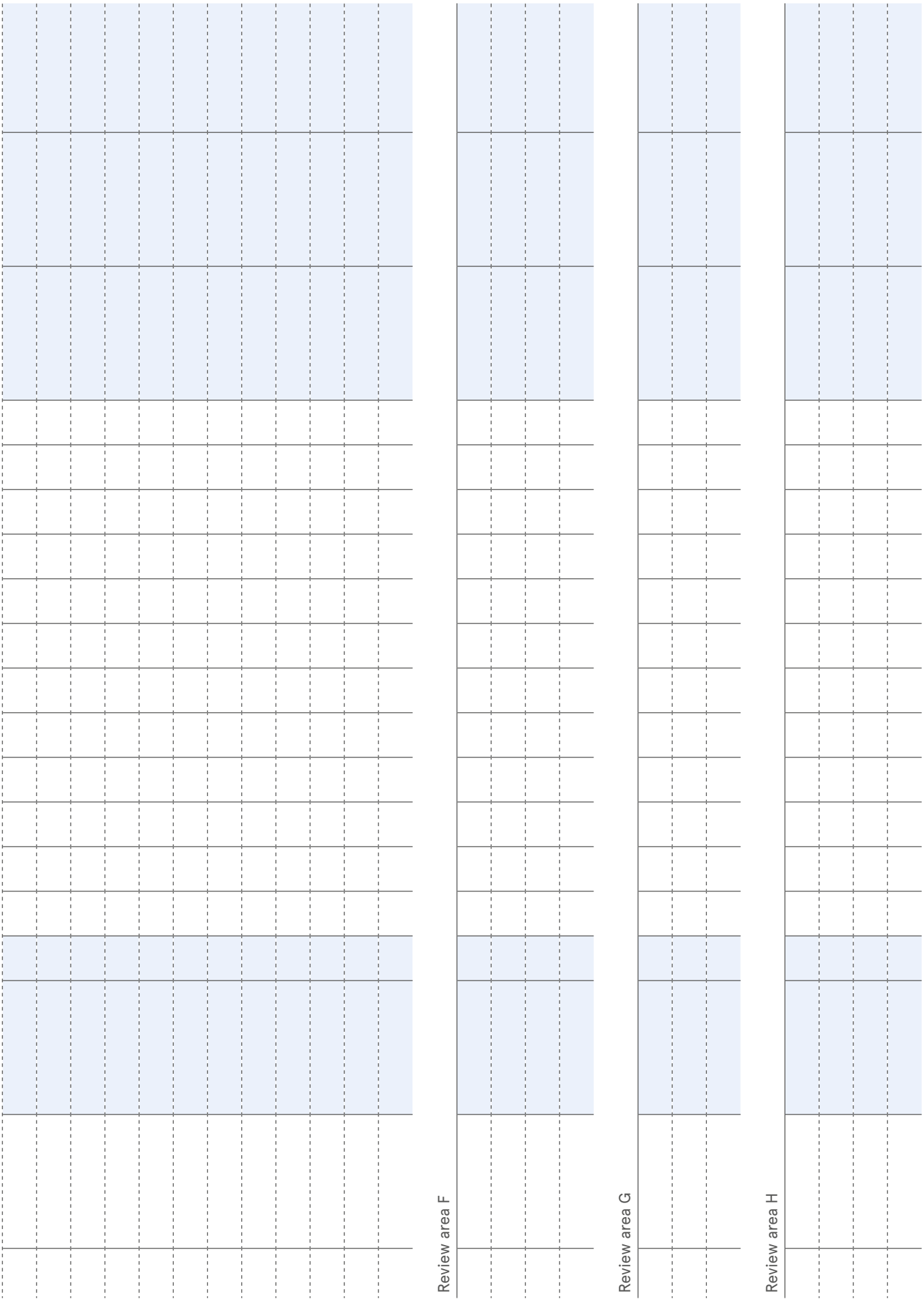
STATUTORY RULES	Statutory provision A	Statutory provision B	Statutory provision C	Statutory provision D	Statutory provision E	Statutory provision A	Statutory provision B	Statutory provision C	Statutory provision D	Statutory provision E	Statutory provision A	Statutory provision B	Statutory provision C	Statutory provision D	Statutory provision E	Statutory provision A	Statutory provision B	Statutory provision C	Statutory provision D	Statutory provision E
SYSTEM	System A					System B					System A					System B				
REVIEW AREA	Review area A										Review area B									

Review area C	System A	Statutory provision A															
		Statutory provision B															
		Statutory provision C															
		Statutory provision D															
		Statutory provision E															
	System B	Statutory provision A															
		Statutory provision B															
		Statutory provision C															
		Statutory provision D															
		Statutory provision E															
Review area D	System A	Statutory provision A															
		Statutory provision B															
		Statutory provision C															
		Statutory provision D															
		Statutory provision E															
	System B	Statutory provision A															
		Statutory provision B															
		Statutory provision C															
		Statutory provision D															
		Statutory provision E															

Other systems
(systems/databases, which in TET's immediate assessment should not form part of TET's general reviews but only TET's technical review of access rights etc.)

SYSTEM	DESCRIPTION	MOST RECENT INSPECTION
System A		
System B		
System C		
System D		
System E		
System F		


NO.
REVIEW AREA
REVIEW TYPE
STATUS
JAN
FEB
MAR
APR
MAY
JUN
JUL
AUG
SEP
OCT
NOV
DEC
REVIEW MEMORANDUM
FOLLOW-UP SHEET
PRIMARY CASE OFFICER
Review area A
Review area B
Review area C
Review area D
Review area E


Review area F
Review area G
Review area H

[Danish Security and Intelligence Service /
Danish Defence Intelligence Service /
Centre for Cyber Security /
PNR Unit of the Danish Police]

Danish Intelligence Oversight Board

Date:
Caseworker: [Name 1] [Name 2]
File no.: [Case no.]
Doc.: [Document no.]

Initial consultation and request for start-up meeting regarding review of [review subject] in [year (Pxx-xx / Fxx-xx / Cxx-xx / Rxx-xx)]

At the meeting held on [date], TET decided a check must be performed in [year] of [review subject].

In this regard, TET shall request a start-up meeting to be held during week [week number]. Furthermore, TET shall request that [DSIS/DDIS/CFCS/PPNR] initiate the start-up meeting by offering a demonstration of the system.

For the preparation thereof, TET must also request that [DSIS / DDIS / CFCS / PPNR] prepare and submit the material described below, cf. [Section 20(3) of the DSIS Act / Section 17(3) of the DDIS Act / Section 22(3) of the CFCS Act], no later than Monday [Monday two weeks before the start-up meeting] at the end of working hours:

a. Material for the start-up meeting:

TET plans, adapts and implements its reviews of [DSIS / DDIS / CFCS / PPNR] based on ongoing, annual risk and materiality assessments of the systems and work processes [of DSIS / DDIS / CFCS / PPNR]. It is a prerequisite for the completion of the assessments and subsequent reviews that TET gathers detailed knowledge of the systems, including their technical structure and functions, data in the system and the specific processes and workflows relating thereto.

In order to achieve an efficient and targeted review, TET wishes to acquire technical knowledge of a system prior to a planned review. TET also wishes to standardise and structure its acquisition of technical knowledge for the individual systems/databases in a way that can better form the basis for the ongoing and often recurring technical dialogue about the systems.

Borgergade 28, 1
DK-1300 Copenhagen K
t +45 25 50 10 34
www.tet.dk

On that basis, TET will collect and document its knowledge in an information sheet (see the attached Appendix A) and a technical, data flow-based system chart, respectively, (see examples in the attached Appendix B) for each system included in TET's review. In TET's experience, both products are necessary in order to create the best possible foundation for understanding complex systems and associated workflows.

The aim is for only one information sheet to be completed per system. However, in case of complex systems consisting of a number of independent sub-systems, it may be advantageous to fill out one information sheet per sub-system. However, only one flow-based system chart in which all sub-systems are included should be filled out.

Thus, TET shall request the following:

- Completed information sheet regarding [review subject] (see the attached Appendix A)
- Flow-based flowchart in Visio format

To illustrate the desired level of detail for the system drawing, TET has prepared fictitious examples of system drawings in a Visio sheet. (see the attached Appendix B).

Moreover, TET shall request the following:

- Reference to relevant specific legislation that may apply to review area in the form of executive orders and/or circulars
- Reference to [DSIS' / DDIS' / CFCS' / PPNR's] possible internal guidelines, instructions, etc. that apply to the review area in question

If the request, including the individual items in Appendix A [and Appendix B], give rise to questions or concerns, TET must request that [DSIS / DDIS / CFCS / PPNR] contact TET as soon as possible for clarification.

Finally, TET request that [DSIS / DDIS / CFCS / PPNR] ensure that all meeting attendees have been cleared for participation in the discussion of the above topic.

If TET does not receive a response or an extension request from [DSIS / DDIS / CFCS / PPNR] by the response deadline, reviews will be finalised on the based on the existing information.

Yours sincerely,
Danish Intelligence Oversight Board

by/[Name]
[Titel]

Information sheet on DSIS' IT system [review subject]

TO BE COMPLETED BY TET

Date of start-up meeting	Meeting attendees from TET	Meeting attendees from DSIS
[DATE]	[NAMES]	[NAMES]

Guide to completing form (Word) and related system flowchart (Visio)

The form includes questions of technical and legal nature. The text in square brackets in the form below serves as a guide and must be removed when completing the form. Enter N/A for fields that are not relevant to the system in question.

If the IT system consists of several independent sub-systems where combining all information in a single form is deemed to result in inexpedient complexity or lack of clarity, one form is instead filled in for each sub-system. However, the chart drawing should still be executed in the form of a single overview.

The purpose of the chart drawing (Visio) is to gain an overview that not only describes the system itself but also illustrates the data flow from data being created or collected up to the point of being stored or transferred to other IT systems. This means that the chart drawing must include the following:

- The data flowing to, being processed in and leaving the system
- The main components and data storage points (e.g. databases, file shares or email systems) in the system
- Flow arrows illustrating the flow routes and direction of data making its way through the system

TO BE COMPLETED BY DSIS (FIELDS 1-9)

1. Overall description of the system

Purpose of the IT system	[Description of what the system is used for, including the primary system functions and its operational purposes]

2. System master data

TECHNICAL QUESTIONS

System name(s)	[State the system call name or names if the system has more than one name]
Products/manufacturers used	[E.g. MS Exchange 2010, Apache Tomcat v7.0, developed by NNIT, etc. as well as the current version number]
Date of commissioning	[Alternatively, state month and year of the commissioning]
Operations Manager	[State the department, section or, where relevant, another external agency responsible for the day-to-day operation of the IT system]
Replacement/upgrading	[If the IT system replaces or is a version upgrade of an existing system, state the previous system name]
Data owner	[State the data owner for the system]
Copies in other IT environments	[Are there any full or partial copies of the IT system in any other IT environments besides the operating/production environment? E.g. development, test or staging environments?]
Planned changes	[If any major changes to the IT system or the use thereof are planned in the current year, please describe them]

3. IT infrastructure of the system

TECHNICAL QUESTIONS	
Network/context and domain	[Name of network/context to which the system is connected]
Servers (named) and their primary roles	[E.g. applications, database, file server, share, etc.]
Client type(s)	[Web browser or application, specify web link or explain how the IT system is accessed/the client is commissioned]
Data sources of the IT system	[E.g. IT system used by another agency, intelligence gathering system, EDMS, etc.]
Data formats being transferred to the IT system	[E.g. PCAP, ZIP, XML, CSV, etc.]
Data volumes being transferred to the IT system	[Estimate in a relevant format, e.g. records, MB, GB, number of documents, etc.]
Recipients of data from the system	[E.g. IT system used by another agency, other departments, EDMS, internal database, etc.]
Data formats being transferred from the IT system	[E.g. PCAP, ZIP, XML, CSV, etc.]
Data volumes being transferred from the IT system	[Estimate in a relevant format, e.g. records, MB, GB, number of documents, etc.]
Data storage points	[All databases (list of names), file systems, external media or other locations where data are being (temporarily) stored by the IT system or daily use of the IT system]

4. User and rights management

TECHNICAL QUESTIONS	
Users of the IT system	[Which user groups use the IT system, e.g. departments, sections, external]
Number of users (view-only access)	[Users or user groups with only view-only access]
Number of users (write-only access)	[Users or user groups that may update (write) data]
Rights management system	[What system is used for user rights management in the system? E.g. Active Directory, internal user database, a combination of multiple systems, etc.]

LEGAL QUESTIONS	
How does DSIS ensure that only individuals who are authorised have access to the information on natural and legal persons processed in the system, cf. Sections 10 and 11 of the DSIS Security Order?	[The question should be seen in the context of the technical questions above]
Does DSIS carry out reviews on rejected access attempts, cf. Section 16 of the DSIS Executive Order on Security?	[Yes/No If yes, please provide additional information]

5. Deleting data in practice

TECHNICAL QUESTIONS	
Initiation of data deletion	[Who ensures routine deletion/cleansing of data in accordance with any deadlines for deletion?]
Deletion	[Are data in the system deleted manually or automatically, e.g. via scripts? In case of manual deletion, who does it?]

In terms of relevant information regarding deletion of data, how is relevant information regarding time of collection/time of entry/age/etc. entered into the system?	[For example, is the age specified by a creation date field in a database or by creation time in file metadata?]
Frequency	[How often are data routinely deleted/cleansed in the system?]

LEGAL QUESTIONS

Is the system an electronic record, cf. Section 1(1) of the DSIS Executive Order?	[Yes/No. The question must be seen in the context of the technical question "In terms of relevant information regarding deletion of data [...]?" above]
Is the system a database, cf. Section 2(1) of the DSIS Executive Order?	[Yes/No]
If the system is a database, what is the time limit for deletion set by DSIS, cf. Section 2(2) of the DSIS Executive Order?	[Specify the deletion deadline if this is a database, cf. Section 2(1) of the DSIS Executive Order. The question must be seen in the context of the technical question "In terms of relevant information regarding deletion of data [...]?" above]
Is the system a transit system, i.e., the system is neither an electronic record, cf. Section 1(1) of the DSIS Executive Order nor a database, cf. Section 2(2) of the DSIS Executive Order?	[Yes/No. The question must be seen in the context of the technical question "In terms of relevant information regarding deletion of data [...]?" above]

6. Backup and restore

TECHNICAL QUESTIONS

Data backup	[Is there a data backup system in place?]
Data retention	[How far back will it be possible to restore data?]
Restoring of data	[What measures are in place to ensure that data, which have been deleted after an audit, are not inadvertently restored?]

7. Logging of user activities

TECHNICAL QUESTIONS

User activity logging	[Are the actions/transactions of users being logged?]
Incident types	[What types of user actions are being logged? E.g. viewing, writing, changing, deleting, searching, search results, etc.]
Access to activity logs	[Where and how to access the user activity logs in the system]
Searching the activity logs	[How do you search activity logs? Is it possible to time-limit this search?]

LEGAL QUESTIONS

Has DSIS established a logging system that at a minimum contains information about time, user, type of application and indication of the person to whom the data related or the search criterion used, cf. Section 17(1)(1) of the DSIS Executive Order on Security?	[Yes/No If yes, please provide additional information. The question should be seen in the context of the technical question "Incident types" above]
How long is the log kept, cf. Section 17(1)(2) and (3) of the DSIS Executive Order on Security?	[Specify log data retention period]

8. Documentation and guides

TECHNICAL QUESTIONS	
Search user guide	[Enclose copy or state location of existing user guides for searching the system]
User guide for IT system	[Enclose copy or state location of existing user guides for use in connection with the system]
Other system documentation	[Enclose a copy or provide the location of existing documentation regarding the system's structure and functionality]
Detail form in case DSIS assesses that it is an RM system	[Enclose copy or state location of existing detail form for use in connection with the system]

9. General questions regarding security of processing

LEGAL QUESTIONS	
Which technical and organisational measures has DSIS taken to prevent that information about natural and legal persons is accidentally or unlawfully destroyed, lost or impaired and protected against unauthorised disclosure, misuse or other processing in violation of the DSIS Act, cf. Section 3 of the DSIS Executive Order on Security?	[Specify technical and organisational measures]
Has DSIS laid down more detailed internal regulations on security measures, cf. Section 4(1) of the DSIS Executive Order on Security? If so, when did DSIS last review these regulations, cf. Section 4(2) of the DSIS Executive Order on Security?	[Yes/No If yes, please provide additional information]
Did DSIS provide instruction to the employees who process information on natural and legal persons, cf. Section 5 of the DSIS Executive Order on Security?	[Yes/No If yes, please provide additional information]
Has DSIS taken precautions at locations where processing of information about natural and legal persons takes place, in order to prevent unauthorised access to said information, cf. Section 7 of the DSIS Executive Order on Security?	[Yes/No If yes, please provide additional information]

If DSIS has prepared documentation that answers the above questions regarding processing security, DSIS is requested to submit such documentation as well.

TO BE COMPLETED BY TET

Any follow-up questions for the start-up meeting

NUMBER	QUESTION	ANSWER
1		
2		
3		

Information sheet on DDIS' IT system [review subject]

TO BE COMPLETED BY TET

Date of start-up meeting	Meeting attendees from TET	Meeting attendees from DDIS
[DATE]	[NAMES]	[NAMES]

Guide to completing form (Word) and related system flowchart (Visio)

The form includes questions of technical and legal nature. The text in square brackets in the form below serves as a guide and must be removed when completing the form. Enter N/A for fields that are not relevant to the system in question.

If the IT system consists of several independent sub-systems where combining all information in a single form is deemed to result in inexpedient complexity or lack of clarity, one form is instead filled in for each sub-system. However, the chart drawing should still be executed in the form of a single overview.

The purpose of the chart drawing (Visio) is to gain an overview that not only describes the system itself but also illustrates the data flow from data being created or collected up to the point of being stored or transferred to other IT systems. This means that the chart drawing must include the following:

- The data flowing to, being processed in and leaving the system
- The main components and data storage points (e.g. databases, file shares or email systems) in the system
- Flow arrows illustrating the flow routes and direction of data making its way through the system

TO BE COMPLETED BY DDIS (FIELDS 1-9)

1. Overall description of the system

Purpose of the IT system	[Description of what the system is used for, including the primary system functions and its operational purposes]

2. System master data

TECHNICAL QUESTIONS

System name(s)	[State the system call name or names if the system has more than one name]
Associated passwords	[List all DDIS passwords used (capitalised) that are associated with or included in the system, its sub-systems or applications]
Products/manufacturers used	[E.g. MS Exchange 2010, Apache Tomcat v7.0, developed by NNIT, etc. as well as the current version number]
Date of commissioning	[Alternatively, state month and year of the commissioning]
Operations Manager	[State the department, section or, where relevant, another external agency responsible for the day-to-day operation of the IT system]
Replacement/upgrading	[If the IT system replaces or is a version upgrade of an existing system, state the previous system name]
Data owner	[State the data owner for the system]
Copies in other IT environments	[Are there any full or partial copies of the IT system in any other IT environments besides the operating/production environment? E.g. development, test or staging environments?]
Planned changes	[If any major changes to the IT system or the use thereof are planned in the current year, please describe them]

3. IT infrastructure of the system

TECHNICAL QUESTIONS	
Network/context and domain	[Name of network/context to which the system is connected]
Servers (named) and their primary roles	[E.g. applications, database, file server, share, etc.]
Client type(s)	[Web browser or application, specify web link or explain how the IT system is accessed/the client is commissioned]
Data sources of the IT system	[E.g. IT system used by another agency, intelligence gathering system, EDMS, etc.]
Data formats being transferred to the IT system	[E.g. PCAP, ZIP, XML, CSV, etc.]
Data volumes being transferred to the IT system	[Estimate in a relevant format, e.g. records, MB, GB, number of documents, etc.]
Recipients of data from the system	[E.g. IT system used by another agency, other departments, EDMS, internal database, etc.]
Data formats being transferred from the IT system	[E.g. PCAP, ZIP, XML, CSV, etc.]
Data volumes being transferred from the IT system	[Estimate in a relevant format, e.g. records, MB, GB, number of documents, etc.]
Data storage points	[All databases (list of names), file systems, external media or other locations where data are being (temporarily) stored by the IT system or daily use of the IT system]

4. User and rights management

TECHNICAL QUESTIONS	
Users of the IT system	[Which user groups use the IT system, e.g. departments, sections, external]
Number of users (view-only access)	[Users or user groups with only view-only access]
Number of users (write-only access)	[Users or user groups that may update (write) data]
Rights management system	[What system is used for user rights management in the system? E.g. Active Directory, internal user database, a combination of multiple systems, etc.]

5. Deleting data in practice

TECHNICAL QUESTIONS	
Initiation of data deletion	[Who ensures routine deletion/cleansing of data in accordance with any deadlines for deletion?]
Deletion	[Are data in the system deleted manually or automatically, e.g. via scripts? In case of manual deletion, who does it?]
In terms of relevant information regarding deletion of data, how is relevant information regarding time of collection/time of entry/age/etc. entered into the system?	[For example, is the age specified by a creation date field in a database or by the creation time in file metadata?]
Frequency	[How often are data routinely deleted/cleansed in the system?]

LEGAL QUESTIONS	
Does the system contain recognised information obtained under Section 1(1) of the DDIS Act, cf. Section 6(1)?	[Yes/No. The question must be seen in the context of the technical question "In terms of relevant information regarding deletion of data [...]?" above]

Does the system include raw data, cf. Section 6(2) of the DDIS Act?	[Yes/No. The question must be seen in the context of the technical question "In terms of relevant information regarding deletion of data [...]?" above]

6. Backup and restore

TECHNICAL QUESTIONS

Data backup	[Is there a data backup system in place?]
Data retention	[How far back will it be possible to restore data?]
Restoring of data	[What measures are in place to ensure that data, which have been erased after an audit, are not inadvertently restored?]

7. Logging of user activities

TECHNICAL QUESTIONS

User activity logging	[Are the actions/transactions of users being logged?]
Incident types	[What types of user actions are being logged? E.g. viewing, writing, changing, deleting, searching, search results, etc.]
Access to activity logs	[Where and how to access the user activity logs in the system]
Searching the activity logs	[How do you search activity logs? Is it possible to time-limit this search?]

8. Documentation and guides

TECHNICAL QUESTIONS

Search user guide	[Enclose copy or state location of existing user guides for searching the system]
User guide for IT system	[Enclose copy or state location of existing user guides for use in connection with the system]
Other system documentation	[Enclose a copy or provide the location of existing documentation regarding the system's structure and functionality]

9. General questions regarding security of processing

LEGAL QUESTIONS

Which technical and organisational measures has DDIS taken to prevent that information about resident natural and legal persons accidentally or unlawfully are destroyed, lost or compromised, including measures preventing anyone from obtaining unauthorised knowledge, and against misuse or otherwise ensuring that such information is processed in violation of the DDIS Act, cf. Section 3 of the DDIS Executive Order on Security?	[Specify technical and organisational measures]

If DDIS has prepared documentation that answers the above questions regarding processing security, the service is requested to submit such documentation as well.

TO BE COMPLETED BY TET

Any follow-up questions for the start-up meeting

NUMBER	QUESTION	ANSWER
1		
2		
3		

Information sheet on CFCS' IT system [review subject]

TO BE COMPLETED BY TET

Date of start-up meeting	Meeting attendees from TET	Meeting attendees from CFCS
[DATE]	[NAMES]	[NAMES]

Guide to completing form (Word) and related system flowchart (Visio)

The form includes questions of technical and legal nature. The text in square brackets in the form below serves as a guide and must be removed when completing the form. Enter N/A for fields that are not relevant to the system in question.

If the IT system consists of several independent sub-systems where combining all information in a single form is deemed to result in inexpedient complexity or lack of clarity, one form is instead filled in for each sub-system. However, the chart drawing should still be executed in the form of a single overview.

The purpose of the chart drawing (Visio) is to gain an overview that not only describes the system itself but also illustrates the data flow from data being created or collected up to the point of being stored or transferred to other IT systems. This means that the chart drawing must include the following:

- The data flowing to, being processed in and leaving the system
- The main components and data storage points (e.g. databases, file shares or email systems) in the system
- Flow arrows illustrating the flow routes and direction of data making its way through the system

TO BE COMPLETED BY CFCS (FIELDS 1-9)

1. Overall description of the system

Purpose of the IT system	[Description of what the system is used for, including the primary system functions and its operational purposes]

2. System master data

TECHNICAL QUESTIONS

System name(s)	[State the system call name or names if the system has more than one name]
Associated passwords	[List all CFCS passwords used (capitalised) that are associated with or included in the system, its sub-systems or applications]
Products/manufacturers used	[E.g. MS Exchange 2010, Apache Tomcat v7.0, developed by NNIT, etc. as well as the current version number]
Date of commissioning	[Alternatively, state month and year of the commissioning]
Operations Manager	[State the department, section or, where relevant, another external agency responsible for the day-to-day operation of the IT system]
Replacement/upgrading	[If the IT system replaces or is a version upgrade of an existing system, state the previous system name]
Data owner	[State the data owner for the system]
Copies in other IT environments	[Are there any full or partial copies of the IT system in any other IT environments besides the operating/production environment? E.g. development, test or staging environments?]
Planned changes	[If any major changes to the IT system or the use thereof are planned in the current year, please describe them]

3. IT infrastructure of the system

TECHNICAL QUESTIONS	
Network/context and domain	[Name of network/context to which the system is connected]
Servers (named) and their primary roles	[E.g. applications, database, file server, share, etc.]
Client type(s)	[Web browser or application, specify web link or explain how the IT system is accessed/the client is commissioned]
Data sources of the IT system	[E.g. IT system used by another agency, intelligence gathering system, EDMS, etc.]
Data formats being transferred to the IT system	[E.g. PCAP, ZIP, XML, CSV, etc.]
Data volumes being transferred to the IT system	[Estimate in a relevant format, e.g. records, MB, GB, number of documents, etc.]
Recipients of data from the system	[E.g. IT system used by another agency, other departments, EDMS, internal database, etc.]
Data formats being transferred from the IT system	[E.g. PCAP, ZIP, XML, CSV, etc.]
Data volumes being transferred from the IT system	[Estimate in a relevant format, e.g. records, MB, GB, number of documents, etc.]
Data storage points	[All databases (list of names), file systems, external media or other locations where data are being (temporarily) stored by the IT system or daily use of the IT system]

4. User and rights management

TECHNICAL QUESTIONS	
Users of the IT system	[Which user groups use the IT system, e.g. departments, sections, external]
Number of users (view-only access)	[Users or user groups with only view-only access]
Number of users (write-only access)	[Users or user groups that may update (write) data]
Rights management system	[What system is used for user rights management in the system? E.g. Active Directory, internal user database, a combination of multiple systems, etc.]

LEGAL QUESTIONS	
How does CFCS ensure that only employees at the centre have access to the parts of the information systems in which data covered by Chapter 4 of the CFCS Act is processed, cf. Section 4(1) and (2) of the CFCS circular?	[Specify how CFCS ensures that only employees at the centre have access to the parts of the information systems in which such data is processed. The question should be seen in the context of the technical question "Rights management system" above]

5. Deleting data in practice

TECHNICAL QUESTIONS	
Initiation of data deletion	[Who ensures routine deletion/cleansing of data in accordance with any deadlines for deletion?]
Deletion	[Are data in the system deleted manually or automatically, e.g. via scripts? In case of manual deletion, who does it?]
In terms of relevant information regarding deletion of data, how is relevant information regarding time of collection/time of entry/age/etc. entered into the system?	[For example, is the age specified by a creation date field in a database or by creation time in file metadata?]

Frequency	[How often are data routinely deleted/cleansed in the system?]

LEGAL QUESTIONS

Does the system contain data covered by Section 17(1) of the CFCS Act?	[Yes/No. The question must be seen in the context of the technical question "In terms of relevant information regarding deletion of data [...]?" above]
Does the system contain data that is associated with a security incident, cf. Section 17(2)(1) of the CFCS Act?	[Yes/No. The question must be seen in the context of the technical question "In terms of relevant information regarding deletion of data [...]?" above]
If the system contains data that is not related to a security incident, but originates from agencies that are particularly concerned with foreign, security and defence policy as well companies and organisations whose activities are of particular importance to these matters, cf. Section 17(2)(2) of the CFCS Act?	[Yes/No. The question must be seen in the context of the technical question "In terms of relevant information regarding deletion of data [...]?" above]
If the system contains other data that is not related to a security incident, cf. Section 17(2)(1) of the CFCS Act?	[Yes/No. The question must be seen in the context of the technical question "In terms of relevant information regarding deletion of data [...]?" above]

6. Backup and restore

TECHNICAL QUESTIONS

Data backup	[Is there a data backup system in place?]
Data retention	[How far back will it be possible to restore data?]
Restoring of data	[What measures are in place to ensure that data, which have been erased after an audit, are not inadvertently restored?]

7. Logging of user activities

TECHNICAL QUESTIONS

User activity logging	[Are the actions/transactions of users being logged?]
Incident types	[What types of user actions are being logged? E.g. viewing, writing, changing, deleting, searching, search results, etc.]
Access to activity logs	[Where and how to access the user activity logs in the system]
Searching the activity logs	[How do you search activity logs? Is it possible to time-limit this search?]

8. Documentation and guides

TECHNICAL QUESTIONS

Search user guide	[Enclose copy or state location of existing user guides for searching the system]
User guide for IT system	[Enclose copy or state location of existing user guides for use in connection with the system]
Other system documentation	[Enclose a copy or provide the location of existing documentation regarding the system's structure and functionality]

9. General questions regarding security of processing

LEGAL QUESTIONS

Which technical and organisational measures has CFCS taken to prevent accidental or unlawful destruction, loss or deterioration of data and against unauthorised disclosure, misuse or other processing in violation of the CFCS Act, cf. Section 18 of the CFCS Act?	[Specify technical and organisational measures]

If CFCS has prepared documentation that answers the above questions regarding processing security, the service is requested to submit such documentation as well.

TO BE COMPLETED BY TET

Any follow-up questions for the start-up meeting

NUMBER	QUESTION	ANSWER
1		
2		
3		

Information sheet on PPNR's IT system [review subject]

TO BE COMPLETED BY TET

Date of start-up meeting	Meeting attendees from TET	Meeting attendees from PPNR
[DATE]	[NAMES]	[NAMES]

Guide to completing form (Word) and related system flowchart (Visio)

The form includes questions of technical and legal nature. The text in square brackets in the form below serves as a guide and must be removed when completing the form. Enter N/A for fields that are not relevant to the system in question.

If the IT system consists of several independent sub-systems where combining all information in a single form is deemed to result in inexpedient complexity or lack of clarity, one form is instead filled in for each sub-system. However, the chart drawing should still be executed in the form of a single overview.

The purpose of the chart drawing (Visio) is to gain an overview that not only describes the system itself but also illustrates the data flow from data being created or collected up to the point of being stored or transferred to other IT systems. This means that the chart drawing must include the following:

- The data flowing to, being processed in and leaving the system
- The main components and data storage points (e.g. databases, file shares or email systems) in the system
- Flow arrows illustrating the flow routes and direction of data making its way through the system

TO BE COMPLETED BY PPNR (FIELDS 1-9)

1. Overall description of the system

Purpose of the IT system	[Description of what the system is used for, including the primary system functions and its operational purposes]

2. System master data

TECHNICAL QUESTIONS

System name(s)	[State the system call name or names if the system has more than one name]
Products/manufacturers used	[E.g. MS Exchange 2010, Apache Tomcat v7.0, developed by NNIT, etc. as well as the current version number]
Date of commissioning	[Alternatively, state month and year of the commissioning]
Operations Manager	[State the department, section or, where relevant, another external agency responsible for the day-to-day operation of the IT system]
Replacement/upgrading	[If the IT system replaces or is a version upgrade of an existing system, state the previous system name]
Data owner	[State the data owner for the system]
Copies in other IT environments	[Are there any full or partial copies of the IT system in any other IT environments besides the operating/production environment? E.g. development, test or staging environments?]
Planned changes	[If any major changes to the IT system or the use thereof are planned in the current year, please describe them]

3. IT infrastructure of the system

TECHNICAL QUESTIONS	
Network/context and domain	[Name of network/context to which the system is connected]
Servers (named) and their primary roles	[E.g. applications, database, file server, share, etc.]
Client type(s)	[Web browser or application, specify web link or explain how the IT system is accessed/the client is commissioned]
Data sources of the IT system	[E.g. IT system used by another agency, intelligence gathering system, EDMS, etc.]
Data formats being transferred to the IT system	[E.g. PCAP, ZIP, XML, CSV, etc.]
Data volumes being transferred to the IT system	[Estimate in a relevant format, e.g. records, MB, GB, number of documents, etc.]
Recipients of data from the system	[E.g. IT system used by another agency, other departments, EDMS, internal database, etc.]
Data formats being transferred from the IT system	[E.g. PCAP, ZIP, XML, CSV, etc.]
Data volumes being transferred from the IT system	[Estimate in a relevant format, e.g. records, MB, GB, number of documents, etc.]
Data storage points	[All databases (list of names), file systems, external media or other locations where data are being (temporarily) stored by the IT system or daily use of the IT system]

4. User and rights management

TECHNICAL QUESTIONS	
Users of the IT system	[Which user groups use the IT system, e.g. departments, sections, external]
Number of users (view-only access)	[Users or user groups with only view-only access]
Number of users (write-only access)	[Users or user groups that may update (write) data]
Rights management system	[What system is used for user rights management in the system? E.g. Active Directory, internal user database, a combination of multiple systems, etc.]

5. Deleting data in practice

TECHNICAL QUESTIONS	
Initiation of data deletion	[Who ensures routine deletion/cleansing of data in accordance with any deadlines for deletion?]
Deletion	[Are data in the system deleted manually or automatically, e.g. via scripts? In case of manual deletion, who does it?]
In terms of relevant information regarding deletion of data, how is relevant information regarding time of collection/time of entry/age/etc. entered into the system?	[For example, is the age specified by a creation date field in a database or by creation time in file metadata?]
Frequency	[How often are data routinely deleted/cleansed in the system?]

LEGAL QUESTIONS	
How does PPNR ensure that PNR data, cf. Annex 1, from airlines are deleted after a period of 5 years after the transfer to the PNR unit, cf. Section 5 of the PNR Act?	[Specify how PPNR ensures deletion of such data]

6. Backup and restore

TECHNICAL QUESTIONS	
Data backup	[Is there a data backup system in place?]
Data retention	[How far back will it be possible to restore data?]
Restoring of data	[What measures are in place to ensure that data, which have been erased after an audit, are not inadvertently restored?]

7. Logging of user activities

TECHNICAL QUESTIONS	
User activity logging	[Are the actions/transactions of users being logged?]
Types of actions	[What types of user actions are being logged? E.g. viewing, writing, changing, deleting, searching, search results, etc.]
Access to activity logs	[Where and how to access the user activity logs in the system]
Searching the activity logs	[How do you search activity logs? And is it possible to time-limit this search?]

LEGAL QUESTIONS	
Performs PPNR logging, cf. Section 24(1) and (2) of the PNR Act the following processing activities: 1) Collection 2) Search 3) Amendment 4) Disclosure 5) Masking and unmasking 6) Deletion	[Yes/No]
How does PPNR ensure that the logging of data is stored for 5 years, cf. Section 24(4) of the PNR Act?	[Specify how PPNR ensures that the logging of information is stored]

8. Documentation and guides

TECHNICAL QUESTIONS	
Search user guide	[Enclose copy or state location of existing user guides for searching the system]
User guide for IT system	[Enclose copy or state location of existing user guides for use in connection with the system]
Other system documentation	[Enclose a copy or provide the location of existing documentation regarding the system's structure and functionality]

9. General questions regarding security of processing

LEGAL QUESTIONS

Which documentation does PPNR store regarding the processing system and its related procedures, cf. Section 23 of the PNR Act, including 1) name and contact details of the staff in the PNR unit that processes PNR data, see Annex 1, 2) the different levels of authorisations regarding access to data for the staff of the PNR unit, 3) requests submitted by the competent agencies listed in Annex 3 or the Danish Security and Intelligence Service and the Danish Defence Intelligence Service, respectively, and any competent agencies or PNR units in other EU Member States; and 4) requests for and transfers of PNR data to non-member countries and international organisations?	[Specify what documentation PPNR stores regarding the processing system and corresponding procedures]

If PPNR has prepared documentation that answers the above questions regarding processing security, PPNR is requested to submit such documentation as well.

TO BE COMPLETED BY TET

Any follow-up questions for the start-up meeting

NUMBER	QUESTION	ANSWER
1		
2		
3		

Review of [agency] in [year] ([review subject])

1. Background and purpose

Description of TET's decision (date of the meeting), the purpose of the review as well as TET's overall risk assessment of the review area

"At the meeting held on [date], TET decided to perform a compliance review of [review subject]."

"The purpose of the review is to [...]."

"TET's risk assessment of [DSIS / DDIS / CFCS / PPNR] in [year] showed a [low / limited / medium / high] risk of non-compliance in terms of [DSIS' / DDIS' / CFCS' / PPNR's] [obtaining of information / internal processing of information / disclosure of information / processing of information regarding legal political activity] when using [review subject]"

2. Description of the review subject

Description of the review subject (system, database, process, etc.) and a brief objective description thereof and/or reference to where more detailed information may be found; emphasising the parts of the review subject which are particularly relevant for the review

"[The review subject] is [DSIS' / DDIS' / CFCS' / PPNR's] [system / database / process] for [...]."

"[The review subject] includes [...], of which [...] [is/are] deemed particularly relevant to TET's review."

3. Initial analysis/specific risk assessment of the review subject

Brief description of the volume of data and identified processes as well as the risk assessment thereof, including on the basis of any start-up meeting held with DSIS, DDIS, CFCS or PPNR and any previous reviews about similar matters. Furthermore, a description of the initial considerations about the method for the review, description of any amended focus of the review since TET's decision as a result of the initial analysis.

Based on a [start-up meeting with the intelligence service / previous reviews], it has been determined that [...]"

"In the light of these [...]".

4. Review method

Description of final area of review focus and method (system-based, complete or sampling, etc.); overall description of the file selection in the review and/or reference to enclosed selected sheet; overall description of any challenges involved in achieving completeness in the review, i.e. assurance that the oversight elements (the reviewed data as well as the review form) provide a sufficient basis for an assessment of the area. Followed by a brief description of the review having been performed.

"Based on the above, the focus of TET's review is [...]"

The review is performed by [full review / sampling / content screening / inspection / interview-based review / review of decentralised data management], where [system / process is reviewed through discussions with DSIS' / DDIS' / CFCS' / PPNR's employees and/or technical investigations] / [the selection of [cases/records, etc.] has been made on the basis of [random/targeted selection]."

"The population of [cases/records/individuals] reviewed were in total [number]. On this basis, TET has randomly selected [30 cases/records/individuals / 10 percent], which have been reviewed by [...]"

It is TET's assessment that [completeness of the review has been ensured / it has not been possible to ensure completeness of the review] since [...]"

5. Experience

On completion of the review, experience gained from the review is stated, including a general description of the relevant parts of the review and methodical experience, and whether the risk assessment proved correct compared to the result of the review. It is stated whether a similar review is recommended in the future or any suggestions for alternative review methods.

"The review showed that [...]"

"On this basis, it is TET's assessment that [a similar review is not required next year / a similar review is required next year / a similar review should be performed next year, but that the review method should be adjusted so that [...]."

Approved on [date] / [initials]

[Danish Security and Intelligence Service /
Danish Defence Intelligence Service /
Centre for Cyber Security /
PNR Unit of the Danish Police]

Danish Intelligence Oversight Board

Date:
Caseworker: [Name 1] [Name 2]
File no.: [Case no.]
Doc.: [Document no.]

Follow-up on TET's compliance review of [review subject] in [year] / Briefing regarding TET's planned review of [review subject] in [year] [1]

The Danish Intelligence Oversight Board (TET) has in its compliance review of [the Danish Security and Intelligence Service (DSIS) / the Danish Defence Intelligence Service (DDIS) / Centre for Cyber Security (CFCS) / the PNR Unit of the Danish Police] in [year] carried out reviews of [review subject] focusing on [DDIS' / DDIS' / CFCS' / PPNR's] compliance with the rules on [obtaining of information / internal processing of informatoin / disclosure of information / processing of information regarding lawful political activities].

The compliance review was carried out by [Description of TET's oversight methodology]. / [DSIS / DDIS / CFCS / PPNR] stated at the briefing of [date] that [...]. Accordingly, TET has decided that the review will not be carried out.

[The review did not give rise to any consultation. / The review gave rise to a consultation regarding [...]. By form / e-mail / letter to this effect, [DSIS / DDIS / CFCS / PPNR] was consulted on [date].

[DSIS / DDIS / CFCS / PPNR] responded to TET's consultation by letter of [date].

[DSIS / DDIS / CFCS / PPNR] provided [consultation response and any comments].

TET [finds that the review does not give rise to any comments. / finds no grounds on the existing basis for assessing [...] / finds it striking [...] / finds it problematic [...] / has identified [...] / finds it criticisable [...] / finds it highly criticisable [...]. In case of any comments by [DSIS / DDIS / CFCS / PPNR] as to the information that may be included in TET's annual

1 NB! "Briefing" is only used in cases where the review subject has been found to fall outside the competence of TET

Borgergade 28, 1
DK-1300 Copenhagen K
t +45 25 50 10 34
www.tet.dk

report in terms of the description of the review area or if [DSIS / DDIS / CFCS / PPNR] has any information concerning the follow-up review, TET requests to receive such comments no later than [date] for purposes of TET's internal process for preparing the annual report for the year [year]. TET will include any comments from [DSIS / DDIS / CFCS / PPNR] in the assessment of how to describe the review area and any follow-up review in TET's annual report for [year].

Reference is made to [DSIS' / DDIS' / CFCS' / PPNR's] reference no. [...] and TET's review number [see review plan].

Yours sincerely,
Danish Intelligence Oversight Board

by/[name]
Chair of TET

Standards for Danish intelligence oversight activities
Published by the Danish Intelligence Oversight Board, February 2024

Layout + illustrations: Eckardt ApS

The publication is available on TET's website at www.tet.dk

Danish Intelligence Oversight Board
Borgergade 28, 1st floor, 1300 Copenhagen K
www.tet.dk