tet

Danish Intelligence Oversight Board

Standards for Danish intelligence oversight activities

- Risk and materiality assessment (v.2.0)
- Selection of method of oversight and performance of compliance checks (v.1.1)
- Mapping of IT infrastructures (v.1.1)

Content

Introduction **2**

1. Standard for risk and materiality assessment **4**
1.1 Risk and materiality assessment process 5
1.2 Risk assessment of oversight subjects 6
1.3 Ranked risk analysis and oversight plans 9

2. Standard for selection of method of oversight and performance of compliance checks **11**
2.1 Oversight type 11
2.2 Oversight methods 12
2.2.1 Full check 14
2.2.2 Random check 14
2.2.2.1 Random check 14
2.2.2.2 Targeted check 15
2.2.3 Content screening/non-verifiable area 15
2.2.4 Inspection/interview-based check 16
2.2.5 Decentralised data processing check 16
2.2.5.1 Screenshots 17
2.2.5.2 Camera 18
2.2.5.3 Written confirmation 18
2.3 Detailed process description 18
2.3.1 Clarification of the framework and method of the check (oversight type A) 19
2.3.2 Performance of checks (oversight types A and B) 23
2.4 Reporting to TET 25
2.4.1 Oversight memorandum 25
2.4.2 Submission of check at oversight meeting 26
2.4.2.1 Oversight results for discussion and/or approval 26
2.4.2.2 Submission of appendices 26
2.4.2.3 TET's internal compliance checks 26
2.5 Reporting to DSIS, DDIS, CFCS and RPNR 27

3. Standard for mapping of IT infrastructures **29**
3.1 Annual process for IT infrastructure mapping 30
3.2 Preparation and use of the infrastructure list 30
3.3 Analysis and assessment of data in the infrastructure list 31
3.4 Preparation and use of the system list 32
3.5 Detailed process description 33
3.6 Verification of data in the infrastructure list 37

APPENDIX

Glossary **38**
TET's organisation **38**
Scale of TET's comments to DSIS, DDIS, CFCS and RPNR **40**

Appendix 1 Template for schematic risk assessment 42
Appendix 2 Template for oversight plans 44
Appendix 3 Template for technical information sheet and system flowchart 46
Appendix 4 Template for oversight memorandum 50
Appendix 5 Template for follow-up letter to DSIS, DDIS, CFCS and RPNR 52
Appendix 6 Template for infrastructure list 53
Appendix 7 Template for system list 54

Versions since publication of TET's standards

Standard for risk and materiality assessment

VERSION	PUBLISHED	CHANGES
2.0 (current)	2 june 2022	Extensive update of TET's risk and materiality assessment model for DSIS, DDIS, CFCS and RPNR
1.0	24 june 2021	Original version

Standard for selection of method of oversight and performance of compliance checks

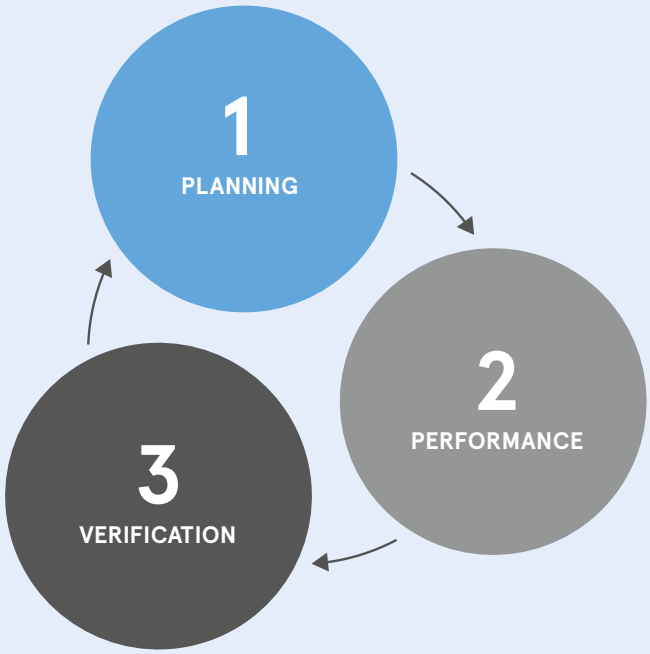
VERSION	PUBLISHED	CHANGES
1.1 (current)	2 june 2022	Minor changes as a result of annual update
1.0	24 june 2021	Original version

Standard for mapping of IT infrastructures

VERSION	PUBLISHED	CHANGES
1.1 (current)	2 june 2022	Minor changes as a result of annual update
1.0	24 june 2021	Original version

Introduction

Overall, TET's checks of the Danish Intelligence Service (DSIS), the Danish Defence Intelligence Service (DDIS), the Danish Centre for Cyber Security (CFCS) and the Danish National Police PNR unit (RPNR) consist of three elements:



TET's **1)** planning of the following year's compliance checks is based on an annual risk and materiality assessment of DSIS, DDIS, CFCS and RPNR processes and systems. The purpose of the risk and materiality assessment is to assess the risk of non-compliance with legislation in relation to the activities of DSIS, DDIS, CFCS and RPNR falling within TET's scope of competence. On that basis, risk analyses are prepared which form the basis of the selection of the following years' checks. On that basis, TET approves oversight plans for the following year's compliance checks of DSIS, DDIS, CFCS and RPNR.

The purpose of the risk analyses is to ensure that TET's checks are focused on the areas with the highest risk of errors and, furthermore, that other relevant factors are taken into account, e.g. areas where TET's checks are given special weight by the legislature such as the rules on legal political activity.

Areas deemed to have a low risk of errors are generally checked once every five years in order to achieve completeness in the oversight of DSIS, DDIS, CFCS and RPNR and ensure that the assessment of risks of errors in the area still holds.

The standard for TET's risk and materiality assessment of DSIS, DDIS, CFCS and RPNR is described in more detail in section 1.

TET's checks **2)** are performed regularly throughout the year based on the oversight plans approved by TET for DSIS, DDIS, CFCS and RPNR. Methods for individual checks are not determined by TET in connection with the preparation of risk assessments and analyses. As such, the selection of method is determined prior to initiating a specific check.

TET uses various methods to check the individual subjects, including full checks, random or targeted checks, content screenings, inspections and interview-based checks.

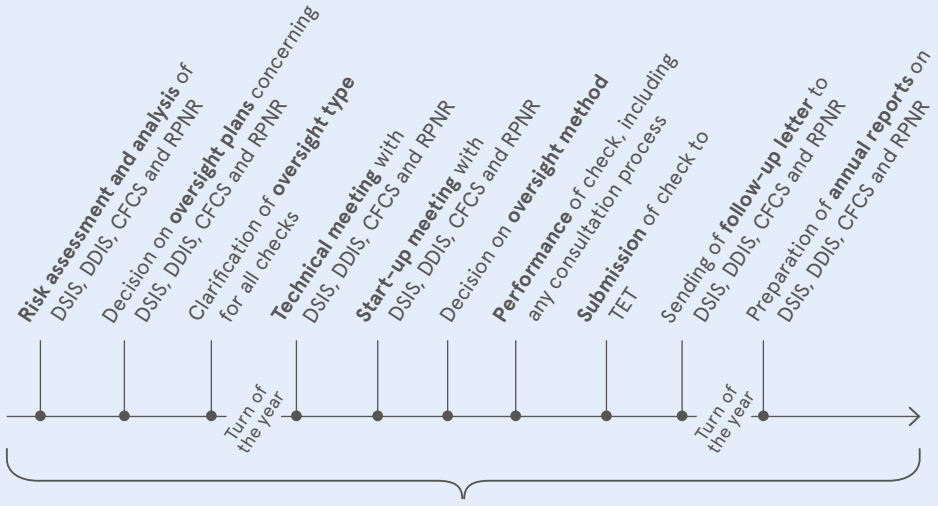
TET's selection of oversight method is based on a specific risk assessment of the oversight subject, experience from previous checks and TET's findings in connection with the specific check. In that connection, prior to checking subjects not previously checked, TET holds technical meetings and start-up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

The standard for TET's method selection and performance of compliance checks of DSIS, DDIS, CFCS and RPNR is described in more detail in section 2.

Finally, TET **3)** performs verification by continuously mapping DSIS', DDIS', CFCS' and RPNR's IT infrastructures at the server, component and application level in order to be able to make complete risk assessments of all processes and systems of DSIS, DDIS, CFCS and RPNR. The purpose of the verification is to ensure that TET's checks are based on data from DSIS, DDIS, CFCS and RPNR the accuracy of which has been verified by TET.

The standard for TET's verification by mapping DSIS, DDIS, CFCS and RPNR IT infrastructures is described in more detail in section 3.

The process for TET's **1)** planning, **2)** performance and **3)** verification of its checks of DSIS, DDIS, CFCS and RPNR is illustrated in the below figure.



Continuous verification and mapping of IT landscapes with feedback to risk assessments and analyses as well as clarification of oversight method for the individual checks

In addition to the version management contained in this document, TET keeps previous versions of its standards on file as it should be possible by comparison to see when and to what extent the standards have been revised.

1. Standard for risk and materiality assessment

The purpose of TET's risk and materiality assessment of DSIS, DDIS, CFCS and RPNR, respectively, is to compile and assess risks to create the proper basis for decisions on TET's own motion checks and checks 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 method is inspired by the Danish Agency for Digitisation's "Guide to IT risk management and assessment" from 2015, but is essentially developed by TET. TET performed its first annual risk assessment of DSIS, DDIS and CFCS in 2016. The method for TET's risk assessment of DSIS, DDIS, CFCS and RPNR has been updated three times (most recently in 2022).

The reason for TET's need to develop its own method is that the target field of TET's risk and materiality assessments is not internal processes in own activities but rather an assessment of other agencies' processes, systems and data processing practices.

This implies, among other things, that the different impact types[1] used by the Danish Agency for Digitisation do not apply in TET's assessments as, considering TET's function, it is only deemed relevant to analyse risks in relation to non-compliance with legislation.

TET's risk and materiality assessment method applied in relation to DSIS, DDIS, CFCS and RPNR is to ensure comparability – both within a given year and over time – and 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 oversight areas.

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

- *Process guide* concerning TET's risk and materiality assessment of DSIS, DDIS, CFCS and RPNR (this standard).

---

1 The Danish Agency for Digitisation's "Guide to IT risk management and assessment" operates with the assessment of different impact types, including strategic, financial, political and administrative/procedural impacts.

- Schematic *risk assessments* of the individual oversight areas, intelligence gathering disciplines, systems, etc. ("oversight subjects") of DSIS, DDIS, CFCS and RPNR, containing risk scores for the individual oversight subjects and stating to what extent in relation to DSIS, DDIS, CFCS and RPNR a given system is checked based on indirect subject access requests (see the relevant template in Appendix 1).

- Ranked *risk analyses* of DSIS, DDIS, CFCS and RPNR concerning TET's own motion checks.

- Ranked *risk analyses* of DSIS and DDIS concerning indirect subject access requests.

- Draft *oversight plans* for next year's compliance checks of DSIS, DDIS, CFCS and RPNR.

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

1.1 Risk and materiality assessment process

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

AUGUST-SEPTEMBER: TET prepares risk assessments of DSIS, DDIS, CFCS and RPNR. The risk assessments contain the risk scores for the individual oversight subjects and state to what extent a given system is checked based on indirect subject access requests.

SEPTEMBER-NOVEMBER: On the basis of the risk assessments, TET prepares ranked risk analyses of DSIS, DDIS, CFCS and RPNR concerning TET's own motion checks and ranked risk analyses of DSIS and DDIS concerning indirect subject access requests. Finally, draft oversight plans are prepared for the following year's checks of DSIS, DDIS, CFCS and RPNR.

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

DECEMBER-JANUARY: TET meets with DSIS, DDIS, CFCS and RPNR to discuss TET's oversight plans for the following year.

The aim is to continuously involve DSIS, DDIS, CFCS and RPNR in this process in relation to the management of DSIS', DDIS', CFCS' and RPNR's internal compliance checks and the preparation of risk and materiality assessments. This provides for the mutual exchange of experience that will strengthen the risk-oriented selection as well as the effect of TET's compliance checks.

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

1.2 Risk assessment of oversight subjects

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

TET's risk assessment of oversight areas is based on TET's accumulated knowledge about DSIS, DDIS, CFCS and RPNR, including in particular the performance and results of previous years' compliance checks as well as the ongoing dialogue with relevant employees of DSIS, DDIS, CFCS and RPNR. This ensures a high degree of validity in the risk assessment and the subsequent ranking and selection of oversight subjects.

As a basis for TET's ranked risk analyses of DSIS, DDIS, CFCS and RPNR, TET has produced a risk score calculation model for the individual oversight areas. The risk score expresses the overall risk/likelihood of a given statutory rule being violated within an oversight area.

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

- *The quality of the data* contained in the given oversight 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 oversight subject.*
- *The method of data processing* within the given oversight subject, i.e. whether this takes place by fully automated processes or fully/partial manual processes.
- *The location of the data processing* for the given oversight subject, i.e. whether the processing takes place on a centralised basis whereby the supervisor has independent access or whether it takes place on a decentralised basis.
- *Logging and rights management* in relation to the data processing within the given oversight subject, i.e. whether all relevant user actions are correctly recorded, 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 oversight subject are able to do so.

- The extent of DSIS', DDIS', CFCS' and RPNR's *internal legal compliance checks* of the given oversight subject, including an assessment of

  - whether DSIS, DDIS, CFCS and RPNR 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 oversight subject, including whether such training is based on introductory training or ongoing dialogue.

- The extent of DSIS', DDIS', CFCS' and RPNR's *internal compliance checks* of the given oversight subject, including

  - whether DSIS, DDIS, CFCS and RPNR subsequently conduct a legal compliance check of a given oversight subject and, if so,
  - whether this internal compliance check 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 check has revealed any errors.

- Whether *TET has conducted any checks in the past* of the oversight subject, including stating

  - the date of TET's most recent check;
  - whether TET's checks within the last three years have revealed any errors;
  - whether TET's checks within the last three 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 RPNR includes the following variables and potential values:

VARIABLES	VALUES	
Data quality?	Structured	0
	Unstructured	2
	Unknown	3
	N/A	0
Extent of personal data?	Minor extent	0
	Material extent	2
	Unknown	3
	N/A	0
Method of data processing?	Automated	0
	Semi-automated	1
	Manual	2
	Unknown	3
	N/A	0
Location of processing?	Central, and TET has independent access	0
	Central, but TET has no independent access	1
	Decentralised	2
	Unknown	3
	N/A	0
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
Internal legal compliance checks?	Yes, including established practice in place for legal approval	0
	Yes, but no established practice in place for legal approval	1
	No	3
	Unknown	3
	N/A	0
Internal compliance checks?	Yes, satisfactory	0
	Yes, but ad hoc/decentralised/not satisfactory	1
	No	3
	Unknown	3
	N/A	0
Any errors revealed in connection with internal compliance checks?	Yes, non-compliance with legislation	2
	Yes, minor errors	1
	No	0
	N/A	0
Any compliance checks performed by TET?	Yes	0
	No	2
	N/A	0
TET's most recent compliance check?	≥ 4 years	3
	3 years	2
	2 years	1
	≤ 1 year	0
	N/A	0
Any errors revealed by TET's compliance checks?	No	0
	Yes, minor errors in connection with most recent compliance check	2
	Yes, non-compliance with legislation in connection with most recent compliance check	5
	Yes, minor errors in connection with previous compliance check (≤ 3 years)	1
	Yes, non-compliance with legislation in connection with previous compliance check (≤ 3 years)	3
	N/A	0
Any comments by TET?	No	0
	Yes, minor comments in connection with most recent compliance check	2
	Yes, material comments in connection with most recent compliance check (criticisable/highly criticisable)	5
	Yes, minor comments in connection with previous compliance check (≤ 3 years)	1
	Yes, material comments in connection with previous compliance check (criticisable/highly criticisable) (≤ 3 years)	3
	N/A	0

TET's assessment of the above variables is entered into a spreadsheet (see Appendix 1) which calculates a risk score for the individual oversight subject on the basis of a weighted model. The risk score is initially stated relative to the risk of non-compliance with the individual statutory provisions within the oversight subject and then as a total score for the relevant process/system.

The risk score is stated on a scale from 0-26 as follows:

Risk score 0-6,5	**Low risk** of non-compliance with legislation
Risk score 6,6-13,0	**Limited risk** of non-compliance with legislation
Risk score 13,1-19,5	**Medium risk** of non-compliance with legislation
Risk score 19,6-26	**High risk** of non-compliance with legislation

In addition to entering the above assessments in the risk assessment, it is possible to make comments concerning the nature and number of errors revealed by TET's or DSIS'/DDIS'/CFCS'/RPNR's previous checks, including whether the errors were in the nature of non-compliance with statutory provisions or internal guidelines, or whether the past checks have given rise to further comments from TET which did not specifically relate to non-compliance with statutory rules or internal guidelines, etc.

It is essential that the additional comments field is used systematically in order to ensure comparability between the risk score and the factors which the model does not specifically take into account. In that way, it will be possible to differentiate and weight the individual risk scores when ranking the given oversight subject in the subsequent risk analysis.

1.3 Ranked risk analysis and oversight plans

On the basis of the risk assessments and the individual risk scores, TET prepares risk analyses of DSIS, DDIS, CFCS and RPNR concerning TET's own motion checks and on that basis a draft oversight plan for the following year as well as separate risk analyses of DSIS and DDIS concerning TET's checks based on indirect subject access requests.

The risk analyses concerning TET's own motion checks rank the oversight subjects by emphasising relevant factors in terms of whether a given oversight subject should be included, upgraded or downgraded in TET's oversight plan for the following year.

While the prior risk assessments of the oversight subjects are used as a basis for the ranking of oversight subjects, it must be possible to include supplementary factors in the risk analysis, including information stated in the comment field of the risk assessments, and in that way differentiate between and rank the risk scores stated in the risk assessment.

Moreover, the risk analyses must specify the subjects for which it is not possible to calculate a specific risk score on the basis of the above model, including TET's detailed assessment of the agency's internal compliance checks as well as a general assessment of the IT systems of the DSIS, DDIS, CFCS and RPNR, and whether it is necessary to revise TET's mapping thereof.

Finally, draft oversight plans for the following year's oversight of DSIS, DDIS, CFCS and RPNR are prepared on the basis of the risk analyses (see Appendix 2). The expected period for the individual oversight is stated in these oversight plans.

In the risk analyses of TET's checks 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 checks of DSIS and DDIS are adequate considering the risks identified and assessed in the risk assessments. On this basis, it is for TET to decide whether the checks are sufficient or whether they are to be supplemented or downgraded with specified systems.

2. Standard for selection of method of oversight and performance of compliance checks

TET uses various methods to check DSIS, DDIS, CFCS and RPNR, including full checks, random or targeted checks, content screenings, inspections and interview-based checks.

The selection of method is based on a specific risk assessment of the oversight subject based on any technical meetings and start-up meetings held with DSIS, DDIS, CFCS or RPNR and on TET's findings in connection with the specific check, and experience from previous checks.

Thus, before an oversight method 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.

2.1 Oversight type

When TET has approved the oversight plans for the following year's checks of DSIS, DDIS, CFCS and RPNR (see section 1), it must initially be assessed whether the individual checks concern:

OVERSIGHT TYPE A

A new oversight subject or a subject where the assumptions on which the check is based have or may have changed. As such, there is a need to clarify the framework and method of the check, including by way of a start-up meeting with DSIS, DDIS, CFCS or RPNR.

OVERSIGHT TYPE B

A known oversight subject with a (fairly) fixed framework for the check, which can be performed according to an already fixed method without a start-up meeting with DSIS, DDIS, CFCS or RPNR.

Any decision to that effect is stated in the oversight plans (see Appendix 2) concerning DSIS, DDIS, CFCS and RPNR next to the individual checks.

It is TET's caseworker in charge who is responsible for any changes to the assessment of the oversight type by ad hoc inclusion of new oversight subjects or, if it turns out

that a given check cannot be performed anyway, according to an already known method.

A change of the assessment must be approved by the relevant Section Leader and Deputy Head of Secretariat of TET and be updated in the oversight plan.

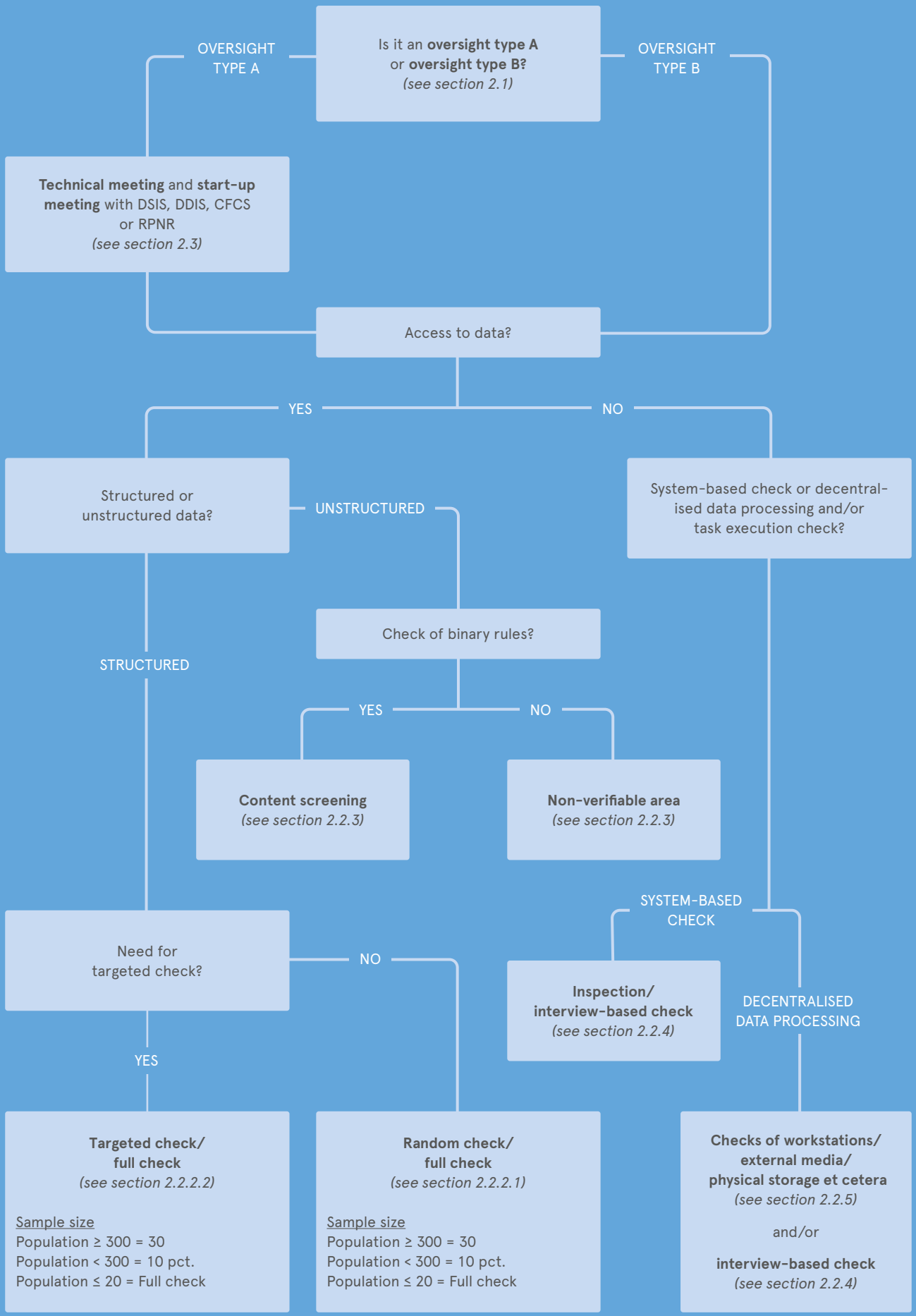
2.2 Oversight methods

When the oversight type for a given oversight subject has been clarified, the method for the check must be determined. As mentioned above, the method is selected after a specific risk assessment of the oversight subject based on any technical meetings and start-up meetings held with DSIS, DDIS, CFCS or RPNR and on TET's findings in connection with the specific check, and experience from previous checks.

Thus, before any oversight 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 oversight methods applied by TET are discussed below. It is the responsibility of the responsible caseworker to arrange for a discussion of suitable oversight methods for a given oversight subject in close dialogue with the relevant Section Leader and other relevant section employees. On this basis, a proposed oversight method is prepared which is subject to the approval of the Deputy Head of Secretariat of TET in all cases.

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


Is it an **oversight type A** or **oversight type B?** *(see section 2.1)*
OVERSIGHT TYPE A
OVERSIGHT TYPE B
Technical meeting and **start-up meeting** with DSIS, DDIS, CFCS or RPNR *(see section 2.3)*
Access to data?
YES
NO
Structured or unstructured data?
UNSTRUCTURED
System-based check or decentralised data processing and/or task execution check?
Check of binary rules?
STRUCTURED
YES
NO
Content screening *(see section 2.2.3)*
Non-verifiable area *(see section 2.2.3)*
SYSTEM-BASED CHECK
Need for targeted check?
NO
Inspection/ interview-based check *(see section 2.2.4)*
DECENTRALISED DATA PROCESSING
YES
Targeted check/ full check *(see section 2.2.2.2)*
Sample size
Population ≥ 300 = 30
Population < 300 = 10 pct.
Population ≤ 20 = Full check
Random check/ full check *(see section 2.2.2.1)*
Sample size
Population ≥ 300 = 30
Population < 300 = 10 pct.
Population ≤ 20 = Full check
Checks of workstations/ external media/ physical storage et cetera *(see section 2.2.5)*
and/or
interview-based check *(see section 2.2.4)*

2.2.1 Full check

A full check of a given oversight subject may be a very resource-intensive method. Full checks 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 check 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 oversight period, DDIS has only made 20 or fewer raw data searches directed at persons resident in Denmark. In this situation a full check is required.

The category "exceptional cases" contains TET's special check 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, random checks must generally be made (see section 2.2.2), unless, because of exceptional circumstances, full checks should continue to be made.

2.2.2 Random check

In a random check, a small number of records/files/individuals, etc. are sampled from a larger population of data. A random check is thus a subset of a population and provides TET with an estimate of the population properties.

Random checks are an efficient method to check 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 check may be extrapolated to the full data set. By using simple random sampling, i.e. a *random check* (see section 2.2.2.1), it is possible to generalise a finding observed in the sample to the whole population (extrapolation).

However, in TET's checks, it will often be necessary to make random checks based on prior modelling/division of the data (the population) using methods applied in relation to stratification, i.e. dividing the population into mutually exclusive groups (strata), or cluster sampling. In this process guide, these methodical concepts are included in a broad sense under *targeted check* (see section 2.2.2.2).

2.2.2.1 Random check

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

TET uses a dedicated spreadsheet to generate random samples by entering the size of the population and the ideal sample size.

The sample size depends on the population size:

- Population ≥ 300 = 30 records/files/individuals, etc.
- Population < 300 = 10% of records/files/individuals, etc.
- Population ≤ 20 = Full check

If TET's sample size standards are adhered to, it is possible based on a random sample to extrapolate the finding observed in a sample to the entire population. However, TET does not use this approach in practice in its communication about the result of a given oversight subject as only the number of errors or the rate of error of the sample is mentioned.

2.2.2.2 *Targeted check*

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

Like random samples, the sample size depends on the population size:

- Population ≥ 300 = 30 records/files/individuals, etc.
- Population < 300 = 10% of records/files/individuals, etc.
- Population ≤ 20 = Full check

2.2.3 Content screening/non-verifiable area

If the data for a check 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 checking options are substantially limited.

In such situations, the only check option available to TET is to perform its check based on binary rules, i.e. rule-making provisions that do not enable discretionary assessments – e.g. provisions on time limits for erasure, which may be checked 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 erasure, 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 checks of transit systems used by DSIS or other checks of DSIS', DDIS', CFCS' or RPNR's erasure of information on file drive structures.

Where TET's checks are not focused on binary rules and where the data are characterised by unstructured data, the oversight subject will be classified as a "non-verifiable area" and then submitted to TET for approval (see section 2.4).

If an oversight subject is classified as a "non-verifiable area", DSIS, DDIS, CFCS or RPNR will be notified according to the applicable procedure in this respect (see section 2.5).

In this connection, DSIS, DDIS, CFCS and RPNR is requested to put in place as soon as possible pathways for efficient checks of the oversight subject and the general public will be made aware of this in the annual reports of TET on its oversight activities.

2.2.4 Inspection/interview-based check

If TET does not have access to the relevant data in its own right in relation to a given oversight subject, it must be clarified whether a system-based check (this section) or a decentralised data processing check and/or task execution check (see section 2.2.5) – or a combination of the two – is required.

A system-based check 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 automatic erasure of information.

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

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

When preparing the question frame for the interview-based check, focus must be on ensuring effective communication between TET and DSIS, DDIS, CFCS or RPNR. It is important in this connection to prepare clear and unambiguous questions the purpose of which is to establish facts and, similarly, where a complex issue is addressed, it is important to ask control questions by using the same question in a new context (supplementary questions).

Data collected from the inspection/the interview-based check are then to be compared against the previously collected data in the form of the technical clarification of the oversight subject and/or data from previous years' checks.

2.2.5 Decentralised data processing check

Checks of decentralised systems include workstations, transit media and the like where it may be difficult to secure documentation of the results of the check. Thus, in connection with this type of check, special focus must be on securing the proper documentation, for which purpose the following methods are used:

- Check form
- Screenshot
- Camera

- Written confirmation

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

- the individual questions in the check 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 check will be discussed.

2.2.5.1 *Screenshots*

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

1) The DSIS, DDIS, CFCS or RPNR 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, subject field and the date of receipt/sending of the email. Where necessary for the check, 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 identification of the emails containing personal data.

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

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

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

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

5) Immediately after the check 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.

2.2.5.2 *Camera*

If it has been agreed with DSIS, DDIS, CFCS or RPNR and if it is necessary in connection with a decentralised data processing check to document a finding which is *not* stored

electronically (e.g. in safety cabinets), documentation of the finding must be secured using the following procedure:

1) TET's employee takes a photo of the finding.

    a. The photo must clearly show a heading, document date, file no., serial no. and other data of importance to the check.

    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 RPNR employee is requested to estimate for how long the document has been stored at the given location and the answer is noted in the check form.

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

4) Immediately after the check, 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 check.

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.

2.2.5.3

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 RPNR.

2.3 Detailed process description

In the following sections, the process of TET's checks is described:

- Section 2.3.1 concerning clarification of the framework and method of the check of DSIS, DDIS, CFCS or RPNR (only relevant for oversight type A)

- Section 2.3.2 concerning performance of checks according to a fixed method (relevant for oversight types A and B)

PREPARATION OF THE CHECK | TECHNICAL CHECK OF THE OVERSIGHT AREA | INTERNAL PRE-MEETING | START-UP MEETING WITH DSIS, DDIS, CFCS OR RPNR | INTERNAL DISCUSSION ON OVERSIGHT METHODOLOGY | APPROVAL OF OVERSIGHT METHOD

PROCESS	DEADLINE	RESPONSIBLE
1. Preparation of the check		
Meeting planning a. *Convening of technical meeting and start-up meeting* with DSIS, DDIS, CFCS or RPNR in coordination with the relevant IT Specialist b. *Convening of internal pre-meeting* with Section Leader, IT Specialist and any other relevant employees c. *Convening of method discussion meeting* with Deputy Head of Secretariat, Section Leader and any other relevant employees d. *Create file* for the check and send link to Section Leader, IT Specialist and any other relevant employees	No later than two months before the check is scheduled to take place	TET's caseworker
2. Technical check of the oversight area		
Own checks a. *Check* whether TET has access and relevant user rights to the oversight subject b. *Examine* how the oversight subject is accessed (application, web or the like) and works (client and system), including functions, types of data and interfaces c. *Request access/user rights* if TET does not have the relevant access to the oversight subject d. *Retrieve existing information* on the oversight subject, including, for example, previous oversight memoranda, IT landscape, detail form, own notes and DSIS, DDIS, CFCS or RPNR documentation, etc. e. *Record and file* all relevant documentation	No later than eight weeks before scheduled start-up meeting	TET's IT Specialist

PROCESS	DEADLINE	RESPONSIBLE
Technical consultation process, if relevant a. *Identify need for additional information* and, where relevant, initiate a consultation with DSIS, DDIS, CFCS or RPNR with a 4-week response deadline (see Appendix 3)	No later than seven weeks before scheduled start-up meeting	TET's IT Specialist
Preparation of technical meeting a. *Review the technical material* received based on the technical consultation. Write down points requiring special attention for use in connection with internal planning and selection of oversight method b. *Draw up the technical question frame* and send it to responsible caseworker and relevant Section Leader c. *Record and file* the technical material and the draft technical question frame	No later than three weeks before scheduled start-up meeting	TET's IT Specialist
Holding of technical meeting a. *Print and bring* the technical question frame and other relevant material for meeting b. *Sum up* briefly to the participants the material and question frame c. *Use question frame and minutes template* for noting down the answers to all technical questions as well as follow-up points and tasks from the meeting	No later than two weeks before scheduled start-up meeting	TET's IT Specialist (with the participation of responsible caseworker and Section Leader)
Follow-up a. *Go over* the results of the meeting with the other participants b. *Note down* any relevant information from the meeting c. *Note down* any unresolved issues d. *Send* follow-up list, if any, of derived tasks to DSIS, DDIS, CFCS or RPNR	Immediately after technical meeting	TET's IT Specialist (as well as relevant employees and Section Leader)
3. Internal pre-meeting	**To be held no later than one week before start-up meeting**	**TET's caseworker**
Preparations a. *Review* any material received from DSIS, DDIS, CFCS or RPNR b. *Review* notes from the technical meeting with TET's IT Specialist c. *Prepare* draft question frame for the check d. *Prepare* a presentation of initial assessment of the oversight subject e. *Consider* the need to consult with DSIS, DDIS, CFCS or RPNR as well as any other relevant preparations	No later than the day before internal pre-meeting	TET's caseworker

PROCESS	DEADLINE	RESPONSIBLE
f. *Record and file* draft question frame, descriptions of the oversight subject as well as other relevant case material and *send* link to the participants in the check		
Presentation at internal pre-meeting a. *Present* all relevant material, including the caseworker's impression and initial assessment of the oversight subject, to the other participants at the meeting	At the meeting	TET's caseworker
Discussion and clarification at the meeting The following is discussed and clarified: a. Draft question frame and any need for supplementing thereof b. Need to collect additional information c. Need to consult with DSIS, DDIS, CFCS or RPNR prior to the start-up meeting d. The need to prepare any forms or other material for purposes of the start-up meeting e. Other subjects or questions of relevance to the check	At the meeting	TET's caseworker (as well as relevant employees and Section Leader)
Follow-up (as relevant) a. *Revise* the question frame b. *Collect* additional information c. *Prepare* forms for purposes of the check	No later than the day before the start-up meeting	TET's caseworker

4. Start-up meeting with DSIS, DDIS, CFCS or RPNR

Preparations a. *Print* relevant material to all participants b. *Sum up* briefly to the participants in the check the material and question frame	The day of the start-up meeting	TET's caseworker
Holding of start-up meeting		TET's Section Leader
Follow-up a. *Review* the results of the meeting with the other participants b. *Note down* any relevant information from the meeting c. *Note down* any unresolved issues	Immediately after the start-up meeting	TET's caseworker (as well as relevant employees and Section Leader)
Draft point-form minutes of the meeting	To be completed the same day, if possible, and no later than on the day before the method discussion meeting	TET's caseworker

PROCESS	DEADLINE	RESPONSIBLE
5. Internal discussion on oversight methodology		**TET's caseworker**
Preparations a. *Prepare* recommendation for oversight method by filling in sections 1-4 of oversight memorandum (see Appendix 4) with the involvement of the Section Leader b. *Record, file* and *send* link to oversight memorandum, point-form minutes of meeting and any additional relevant material to the participants in the meeting	No later than the day before the meeting	TET's caseworker
Presentation/discussion of oversight method a. *Present and discuss* the results of technical meeting and start-up meeting with DSIS, DDIS, CFCS or RPNR with the participants as well as the recommended oversight method	At the meeting	TET's caseworker
Follow-up a. If relevant, *revise* recommendation for oversight method (sections 1-4 of oversight memorandum) and *inform* TET's Deputy Head of Secretariat when the recommendation is ready for final approval	Immediately after the meeting	TET's caseworker
6. Approval of oversight method		
Approval a. *Approve* sections 1-4 of oversight memorandum	No later than one day after the oversight method meeting	TET's Deputy Head of Secretariat

PREPARATION AND APPROVAL OF OVERSIGHT METHODOLOGY

PERFORMING THE CHECK

COMPLETION OF CHECK

PROCES	DEADLINE	ANSVARLIG
1. Preparation and approval of oversight methodology		
a. *Check* whether the factual or legal assumptions on which the check is based have changed. It is particularly important to be critical of whether the annual risk assessment of the oversight subject still holds. If relevant, discuss this with Section Leader b. *Check* whether there is the required access to the oversight subject c. *Create* file on shared drive d. *Create* template for check form e. Ensure *approval* of oversight methodology by Deputy Head of Secretariat f. *Draw* samples, if relevant g. *Inform* the section that the check may be performed on the existing basis.	To be completed no later than one week before the check	TET's caseworker
2. Performing the check		
a. *Perform* the check according to the fixed method		TET's caseworker
Approval of check forms etc.		TET's Section Leader *and* in case of consultation with DSIS, DDIS, CFCS or RPNR, TET's Head of Secretariat
Consultation of DSIS, DDIS, CFCS or RPNR, if relevant a. *Prepare* draft consultation, if relevant		TET's caseworker

PROCES	DEADLINE	ANSVARLIG
Approval of any draft consultation		TET's Section Leader and Head of Secretariat
Receipt of any consultation responses from DSIS, DDIS, CFCS or RPNR *Assess* together with TET's Section Leader whether a. DSIS, DDIS, CFCS or RPNR provides full and satisfactory answers to all questions b. the responses provided by DSIS, DDIS, CFCS or RPNR give rise to additional questions which should be clarified in connection with the check c. a new consultation with DSIS, DDIS, CFCS or RPNR should be prepared (go to the heading "Consultation of DSIS, DDIS, CFCS or RPNR, if relevant").	No later than one week after receipt	TET's caseworker

3. Completion of check

Oversight memorandum a. *Complete* draft oversight memorandum and any check forms and send them to TET's Section Leader for approval	No later than one week before the oversight meeting or one month after the last response received from DSIS, DDIS, CFCS or RPNR	TET's caseworker
Approval of oversight memorandum, final check forms and draft follow-up letter at section level	No later than one week after receipt from caseworker	TET's Section Leader
Approval of oversight memorandum at executive level	No later than three days after receipt from Section Leader	TET's Deputy Head of Secretariat
Approval of final check forms and draft follow-up letter at executive level	No later than three days after receipt from Section Leader	TET's Head of Secretariat
Approval of check result and follow-up letter at oversight level (apply section 2.4 of this process guide)	At the next oversight meeting	TET's members
Check forms a. *Insert* TET's decision in all check forms	No later than one week after the oversight meeting	TET's caseworker
Approval of any adjusted follow-up letter at oversight level	By agreement with the Chair of TET	Chair of TET
Sending of follow-up letter to DSIS, DDIS, CFCS or RPNR	No later than three days after TET's or the Chair's approval	TET's Section Leader
Enter the check in the follow-up check form	No later than three days after TET's or the Chair's approval	TET's caseworker

2.4 Reporting to TET

The required decision-making basis must be available before a check 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 RPNR;
- TET's specific risk assessment of the oversight area;
- TET's selection of oversight method;
- TET's performance of checks, including log lists, check forms, etc.;
- TET's consultations; and
- a consolidation of the above in the form of an oversight memorandum (see section 2.4.1).

A check may not be submitted to TET's members for discussion and/or approval until the above has taken place.

2.4.1 Oversight memorandum

Oversight memoranda are a consolidation of all material information concerning an oversight subject, including

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

The template for the preparation of oversight memoranda is provided in Appendix 4.

Before submission of a check to TET's members, relevant documentation must be recorded and filed on the oversight case and TET's Deputy Head of Secretariat must approve the oversight memorandum.

The check may then be submitted to TET's members for discussion and/or approval, including for inclusion in TET's internal compliance checks (see section 2.4.2.3).

2.4.2 Submission of check at oversight meeting

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

Before a recommendation for the CA is prepared, it must be clarified whether the oversight result is to be recommended for discussion by TET or approval without further discussion at the meeting (see section 2.4.2.1).

When preparing the recommendation for TET, it is important to ensure that only relevant descriptions/details are included in the CA. This will 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.

2.4.2.1 *Oversight results for discussion and/or approval*

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

If a check is recommended to be submitted to TET for discussion, this is indicated in the CA next to the recommendation by a note stating *"(to be discussed at the meeting)"*.

2.4.2.2 *Submission of appendices*

As a general rule, appendices (technical mappings, check forms, consultations, consultation responses, etc.) are only submitted to TET's members where the check has shown non-compliance with the rules or the check otherwise gives rise to comments on DSIS, DDIS, CFCS or RPNR which are subsequently to be addressed in a follow-up letter (see section 2.5).

2.4.2.3 *TET's internal compliance checks*

TET's members perform internal compliance checks of TET's oversight activities. The reason for this is that a substantial amount of TET's oversight material is not submitted to TET's members as the material does not show processing in violation of legislation and therefore does not give rise to consultation with DSIS, DDIS, CFCS or RPNR.

TET's checks are submitted to TET's members at oversight meetings for the purpose of their discussion and completion thereof, and in that connection oversight material is generally only submitted which gives rise to consultation with DSIS, DDIS, CFCS or RPNR (see section 2.4.2.2).

The procedure for TET's internal compliance checks is as follows:

- TET's internal compliance checks are performed on oversight material concerning the checks that are expected to be completed at the next oversight meeting.

- The oversight material comprised by the internal compliance checks has not given rise to consultation with DSIS, DDIS, CFCS or RPNR and the material is thus not appended to the meeting material.

- The DSIS, DDIS, CFCS or RPNR checks comprised by TET's internal compliance checks will be divided into individual numerical groups and a single number will be assigned to each individual check (e.g. DSIS-1, DDIS-3, CFCS-2, RPNR-2).

- A designated member of TET will select one check from each of the agencies subject to oversight by randomly selecting a number without knowing which check the number relates to.

- The designated member of TET will receive a check form for each randomly selected check.

- The designated member of TET will also receive an oversight memorandum as well as other relevant documentation for each randomly selected check so that TET member attains background knowledge for the checks, including about the selection of method and evaluation of result. This will provide TET members with more detailed knowledge about TET's considerations in relation to the specific check as well as the consequences of the check for future checks.

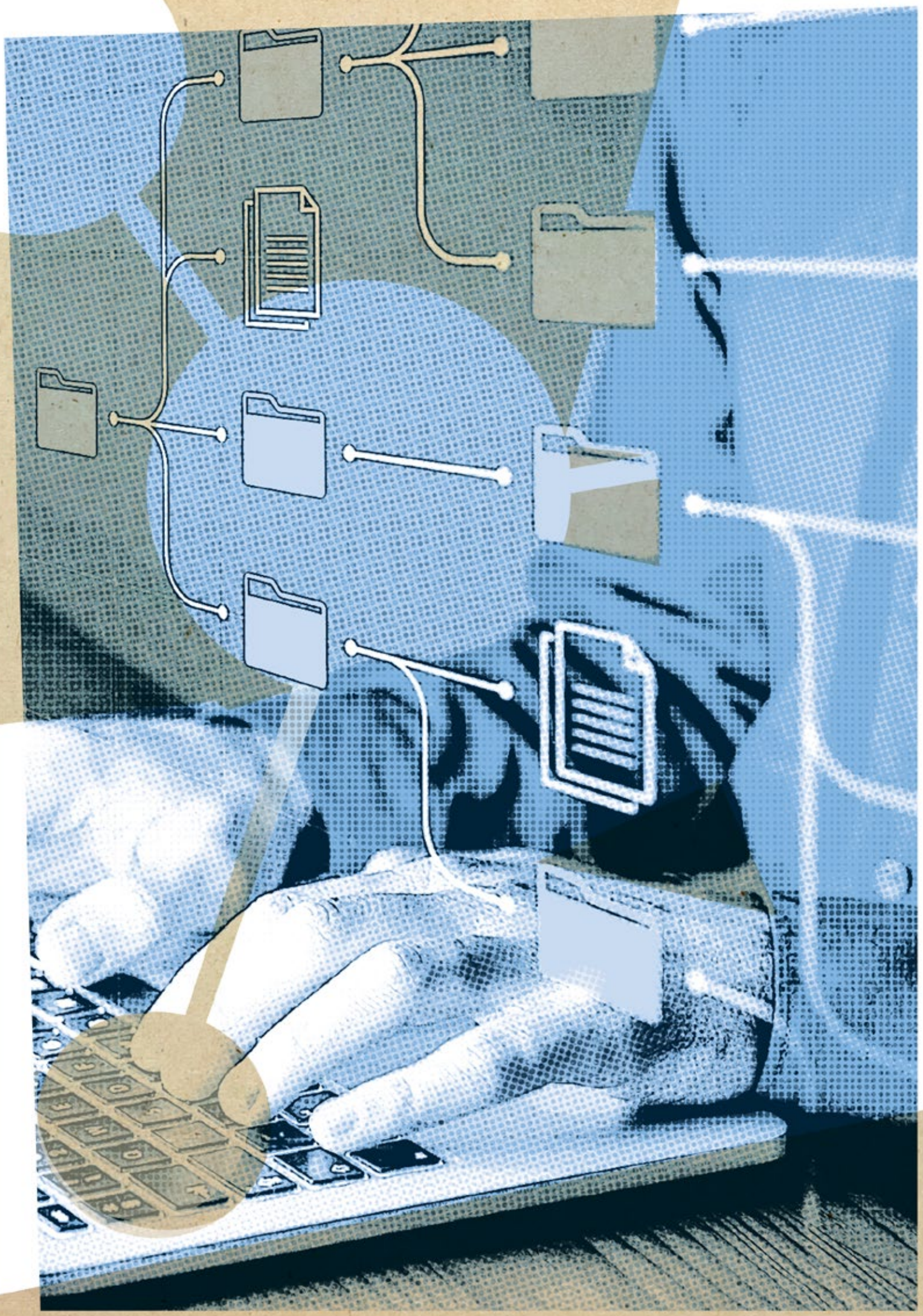
- Finally, the designated member of TET will receive a check form showing the checks, including the check forms, which TET member has checked. The member will be allowed to write down comments on the checks in the check form. The check form will be signed by the member when the internal compliance check is completed.

- The designated member of TET will present the results of the internal compliance check to the other members of TET at the next meeting.

2.5 Reporting to DSIS, DDIS, CFCS and RPNR

When the members of TET have approved a check, a follow-up letter will be sent to DSIS, DDIS, CFCS or RPNR. A template for the draft follow-up letter is provided in Appendix 5 (reference is also made to section 2.3.2 for a detailed process description thereof).

When the members of TET have approved the follow-up letter, it is signed by the Chair of TET and then, without undue delay, sent to DSIS, DDIS, CFCS or RPNR.



3. Standard for mapping of IT infrastructures

The purpose of TET's mapping of the IT infrastructure of DSIS, DDIS, CFCS and RPNR is to compile and assess information about the central, server-based parts in order to create the proper basis for TET's annual risk and materiality assessments of DSIS, DDIS, CFCS and RPNR.

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, which has prompted a need to adjust, structure, and formalise the method.

The selection of method thus reflects a balancing of the need for a technical degree of mapping detail to be able to support TET's checks, the level of IT resources and the IT governance maturity level within TET as well as DSIS, DDIS, CFCS and RPNR.

As an external agency, TET is very much dependent on which IT tools DSIS, DDIS, CFCS and RPNR already have and use as well as the types of system access being available. TET endeavours to use view-only access to the systems and data of DSIS, DDIS, CFCS and RPNR.

TET's method for mapping of IT infrastructures is developed in order to ensure comparability – both within a given year and over time – and 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 factors 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 RPNR 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 RPNR (this standard).
- Schematic template for an *infrastructure list* for collection of relevant information about DSIS, DDIS, CFCS and RPNR IT infrastructures concerning all networks and servers put into operation (see Appendix 6).
- Schematic template for TET's internal *system list*, which is prepared based on an analysis and assessment of the collected data (see Appendix 7).

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 where it is easy to sort and filter data.

In order to ensure optimum utilisation of the IT resources of TET as well as DSIS, DDIS, CFCS and RPNR, 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 RPNR as well as TET.

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

3.1 Annual process for IT infrastructure mapping

The overall IT infrastructure mapping process starts at the beginning of January with TET requesting relevant information from DSIS, DDIS, CFCS and RPNR and 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 RPNR 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 overall ranking of checks. The mapping process stretches throughout the year as follows:

JANUARY–APRIL: TET sends consultation notice to DSIS, DDIS, CFCS and RPNR containing a template for the infrastructure list and requesting that relevant data for all DSIS, DDIS, CFCS and RPNR servers be entered in the list. After having sent the consultations, TET enters into a dialogue with DSIS, DDIS, CFCS or RPNR in case of any questions to the process or the templates.

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

AUGUST–DECEMBER: TET updates its graphic IT landscapes of the DSIS, DDIS, CFCS and RPNR IT infrastructures as well as evaluates and updates processes and templates for the following year's mapping activities.

3.2 Preparation and use of the infrastructure list

TET has decided to structure its checks so that within an oversight subject, the individual IT systems are used as a basis. This method contributes to ensuring completeness in TET's checks. Thus, TET's mapping of the IT infrastructure at DSIS, DDIS, CFCS and RPNR uses the individual IT systems as a basis. The connection between operational matters, systems

and procedures, including data flow mapping, is subsequently mapped in connection with TET's individual checks.

TET has decided to map DSIS', DDIS', CFCS' and RPNR's IT infrastructures each year in a template, which comprises 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 for TET's check.

The infrastructure list contains the following:

- Server name
- System name
- Network/context
- DNS domain
- Primary software
- Short description of the function/role of the server/system

A more elaborate explanation of the individual points in the infrastructure list is available in the template (see Appendix 6). The content of the infrastructure list is adjusted and updated annually as needed.

3.3 Analysis and assessment of data in the infrastructure list

In TET's analysis and assessment of data concerning DSIS', DDIS', CFCS' and RPNR's IT infrastructure it is the system name that is the primary key in the infrastructure list and system list. The system name binds the two lists together and functions as input to TET's annual risk and materiality assessments.

The infrastructure list ties the individual servers to an IT system and may thus be used for crosschecking and validating 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 list.

The infrastructure list enables TET to cross-check and validate whether servers appearing on the infrastructure list correspond to the servers which in practice run in DSIS', DDIS', CFCS' and RPNR's IT environments. This is checked in part by means of inspection checks of DSIS', DDIS', CFCS' and RPNR's virtualisation layers (hypervisor administration tools) and by physical servers in server rooms. At the same time, it is checked whether there are any servers that have been turned off or taken out of service.

TET also screens and assesses the relevance of the individual servers for the check 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 as, 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

The primary software of the server in particular 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 thus normal to place critical or central functions in an IT system on a separate server.

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

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

3.4 Preparation and use of the system list

TET's system list is prepared based on the above-mentioned infrastructure list, available DSIS, DDIS, CFCS and RPNR system documentation and TET's accumulated knowledge. The system list is an internal tool for TET, which is continuously updated with relevant technical information. The system list is important for TET's understanding of systems used by DSIS, DDIS, CFCS and RPNR, 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 checked or which in TET's assessment have undergone extensions or changes which may affect TET's risk and materiality assessment of the system.

The system list contains the following:

- System name
- Short description of the system
- Specification of network/context/environment
- Year of the most recent check
- Relevance score
- Relevance assessment

A more elaborate explanation of the individual points in the system list is available in the template (see Appendix 7). The system list columns are adjusted and updated annually.

3.5 Detailed process description

The annual timetable for preparation of TET's updated system lists is provided in the process description below. The system list updates is finalised before TET's annual risk assessments of DSIS, DDIS, CFCS and RPNR.

The process results in complete infrastructure lists and, on that basis, system lists. The infrastructure lists are prepared by DSIS, DDIS, CFCS and RPNR using a template, while TET prepares the system lists internally.

Initially, TET will send a consultation notice to DSIS, DDIS, CFCS and RPNR containing TET's infrastructure list template, which DSIS, DDIS, CFCS and RPNR must fill in with information about all servers from all IT environments, physical and virtual, including host servers exclusively used to run virtual servers (hypervisor software).

For each server, DSIS, DDIS, CFCS or RPNR must note selected metadata of special interest to TET – for example, what operational system the server is part of and in what IT environment it is installed.

Based on this information, TET will subsequently, using different sorting functions, be able to create a number of different lists of, for example, operational systems, IT environments, networks, contexts, etc.

SENDING OF CONSULTATION NOTICE

DIALOGUE MEETING WITH DSIS, DDIS, CFCS OR RPNR

RECEIPT AND REVIEW OF FILLED IN INFRASTRUCTURE LIST

POSSIBLE FOLLOW-UP MEETING WITH DSIS, DDIS, CFCS AND RPNR

RECEIPT AND REVIEW OF UPDATED INFRASTRUCTURE LIST

PREPARATION OF SYSTEM LIST

EVALUATION OF INFRASTRUCTURE LIST TEMPLATE

PROCES	DEADLINE	ANSVARLIG
1. Sending of consultation notice		
a. Consultation accompanied by infrastructure list (template or last year's list) is sent to DSIS, DDIS, CFCS and RPNR. The consultation period is 15 weeks.	Beginning of January	TET's IT Specialist Consultation to be approved by relevant Section Leader before sending.
2. Dialogue meeting with DSIS, DDIS, CFCS or RPNR		
a. If relevant, dialogue meeting with DSIS, DDIS, CFCS and RPNR about the infrastructure list template and its columns..	End of January	DSIS, DDIS, CFCS and RPNR
3. Receipt and review of filled in infrastructure list		
a. The infrastructure list is returned by DSIS, DDIS, CFCS and RPNR and then reviewed in order to determine whether there are any unresolved issues or points that need to be clarified. Any resolved issues are summarised in a supplementary consultation and sent to DSIS, DDIS, CFCS or RPNR. Consultation period: two weeks. Supplementary consultation questions are summarised in such a way that DSIS, DDIS, CFCS and RPNR can answer them by updating the infrastructure list.	End of April	TET's IT Specialist
4. Possible follow-up meeting with DSIS, DDIS, CFCS and RPNR		
a. Meeting if TET has sent supplementary consultation.	Beginning of May	DSIS, DDIS, CFCS and RPNR
5. Receipt and review of updated infrastructure list		
a. If TET has sent a supplementary consultation with DSIS, DDIS, CFCS or RPNR, an updated infrastructure list is returned which is then reviewed for purposes of verifying that questions from the supplementary consultation have been answered and that the infrastructure list now contains the relevant information.	End of May	TET's IT Specialist

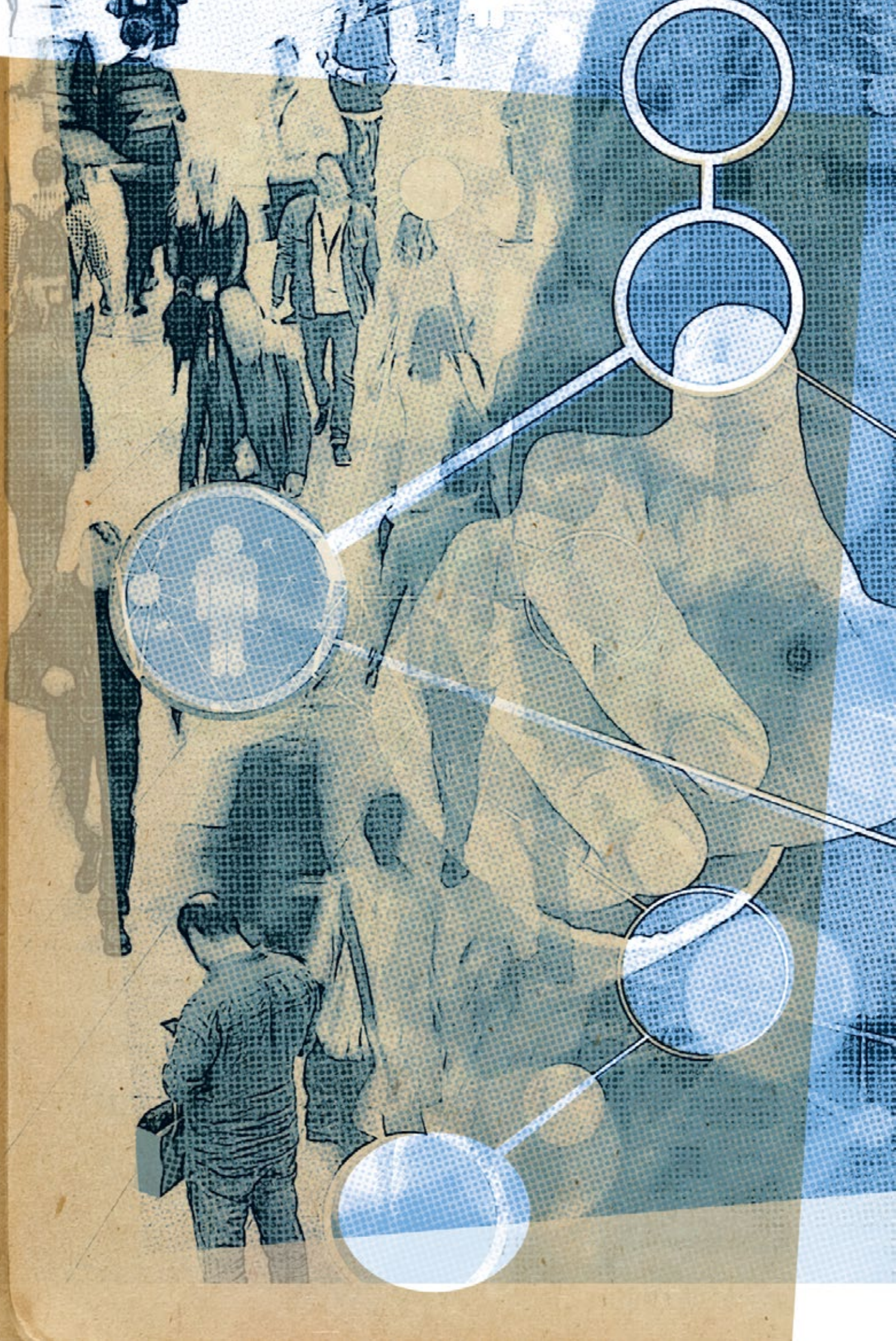
PROCES	DEADLINE	ANSVARLIG

6. Preparation of system list

TET's system lists are subsequently prepared on the basis of the infrastructure lists filled in by DSIS, DDIS, CFCS and RPNR: a. *Sort* the infrastructure list according to the systems column (expand to apply to the rest of the sheet) b. *Copy* the individual system names to the system list so that they occur only once for each network/context/environment in the system list. Remember to fill in the column network/context/environment when entering the system. sheet) c. The fields in the description column to be filled in based on the information in the infrastructure list and documentation previously received from DSIS, DDIS, CFCS and RPNR. The column "relevance score" in the system list denotes a technical assessment of which systems it would be relevant to make a risk assessment of, including a technologically based ranking of such systems. The individual systems are divided into three categories: 1) Relevant system (ranked) 2) Relevant system 3) Non-relevant system Re 1) *Relevant system (ranked)* is a system which from a technical point of view should have special focus in TET's risk and materiality assessment. This usually includes systems that have not been selected for checks in the past and which are technically deemed so complex that there is an increased risk of accumulation of personal data. A system of this type may be selected for mapping with a view to subsequently performing a more relevant check. The number 1 is assigned to systems of this type. Re 2) *Relevant system* is a system that processes personal data but which TET already knows of and which have not undergone major changes since the last mapping. This category is assigned to the vast majority of systems. The number 2 is assigned to this type of systems. Re 3) *Non-relevant system* typically means systems that support the IT infrastructure, for example hypervisor servers, DNS servers, domain services, etc. The number 3 is assigned to this type of systems. The column "relevance assessment" is used where TET's IT Specialist wishes to elaborate on or add information to the relevance score. Finally, system lists are provided as input for TET's annual risk and materiality assessments of DSIS, DDIS, CFCS and RPNR (see section 1).	Mid-June	TET's IT Specialist

7. Evaluation of infrastructure list template

a. The infrastructure list is reviewed with a view to incorporating any experience gained from last year's use of the list. Relevant TET caseworkers are involved in this process.	Beginning of December	TET's IT Specialist



3.6 Verification of data in the infrastructure list

The information entered by DSIS, DDIS, CFCS and RPNR in the infrastructure lists is verified against the existing servers by cross-checking server names on the infrastructure list with the current servers appearing in DSIS', DDIS', CFCS' and RPNR's user and object directory and/or server administration consoles (e.g. hypervisor administration modules). This requires view-only access to the mentioned administration modules or printouts from DSIS, DDIS, CFCS and RPNR, which may be printed out during an inspection meeting.

Checks of context and network grades are cross-checked against configuration lists from network equipment and firewalls, including lists of the networks (including VLAN) that have been set up.

Appendix Glossary

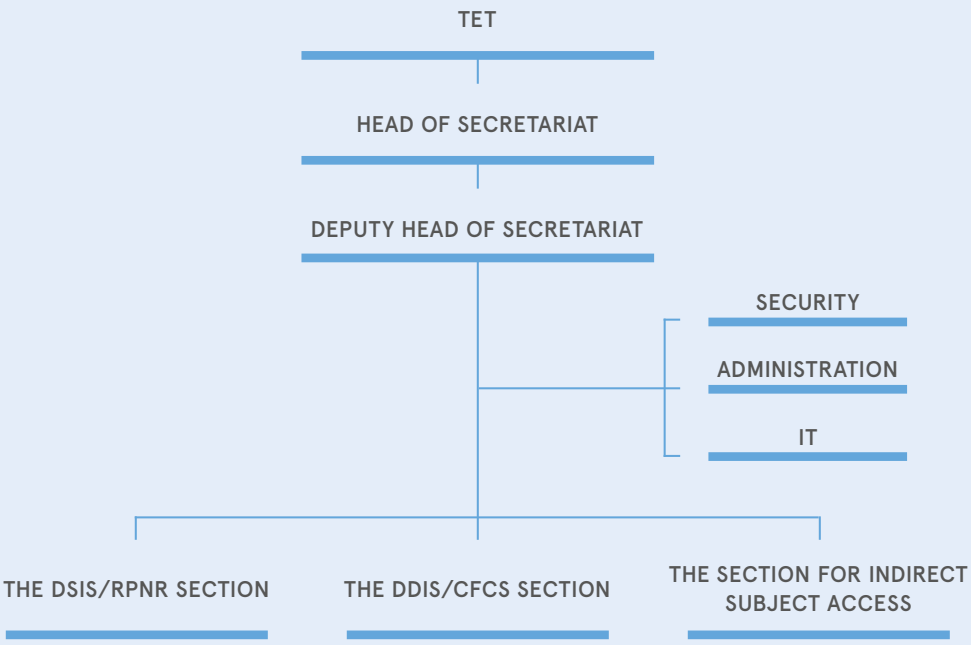
This is a glossary of the most important concepts used in this process guide.

CONCEPT	EXPLANATION
Binary rules	Rule-making provisions that do not enable discretionary assessments – e.g. provisions on time limits for erasure, which may be checked by way of simple look-ups.
Oversight subject	The subject of TET's oversight, i.e. system/process/area, which TET has decided to check.
Oversight type A	A new area or an area where the assumptions on which the check is based have or may have changed and there is a need to clarify the framework and method of the check, including by way of a start-up meeting held with DSIS, DDIS, CFCS or RPNR.
Oversight type B	A known oversight subject with a (fairly) fixed framework for the check which can be performed according to an already fixed method without a start-up meeting being held with DSIS, DDIS, CFCS or RPNR.
Population	The overall data being subjected to a specific check.
Sample	A smaller set of data from a larger population. A sample may be selected randomly or based on targeted parameters (see section 2.2.2).
Unstructured data	Data with no fixed metadata, no efficient retrieval methods and/or no user event logging system being available.

Appendix

TET's organisation

TET 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 is supported by a secretariat, which is subject solely to the instructions of TET 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 secretariat is divided into sections which are concerned with DSIS/RPNR, DDIS/CFCS and indirect subject access requests. In order to ensure subject-matter coordination and experience sharing, TET's staff works across sections.

Appendix

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

TET's comments to DSIS, DDIS, CFCS and RPNR, forwarded to DSIS, DDIS, CFCS and RPNR in a follow-up letter (classified) (see Appendix 5) and subsequently published in TET's annual reports on its activities (unclassified), are based on the following scale:

COMMENTS	BACKGROUND TO COMMENTS
»[...] **does not give rise to any comments**«	Used when TET agrees with DSIS, DDIS, CFCS or RPNR on how they are generally or specifically administering the law.
»TET **finds no grounds for criticizing [...]**«	Used when TET's review is limited by either factual or legal circumstances.
»TET finds it **striking** [...]«	Used for situations in DSIS, DDIS, CFCS, RPNR or 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 RPNR having demonstrated a willingness to ensure the necessary remedial action.

COMMENTS

OVERALL RISK SCORE

0-6,5 = Low risk
6,6-13 = Limited risk
13,1-19,5 = Medium risk
19,6-26 = High risk

RISK SCORE ACCORDING TO LEGAL BASIS

0-6,5 = Low risk
6,6-13 = Limited risk
13,1-19,5 = Medium risk
19,6-26 = 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 Uknown = 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 Uknown = 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
Uknown = 3

METHOD OF DATA PROCESSING?

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

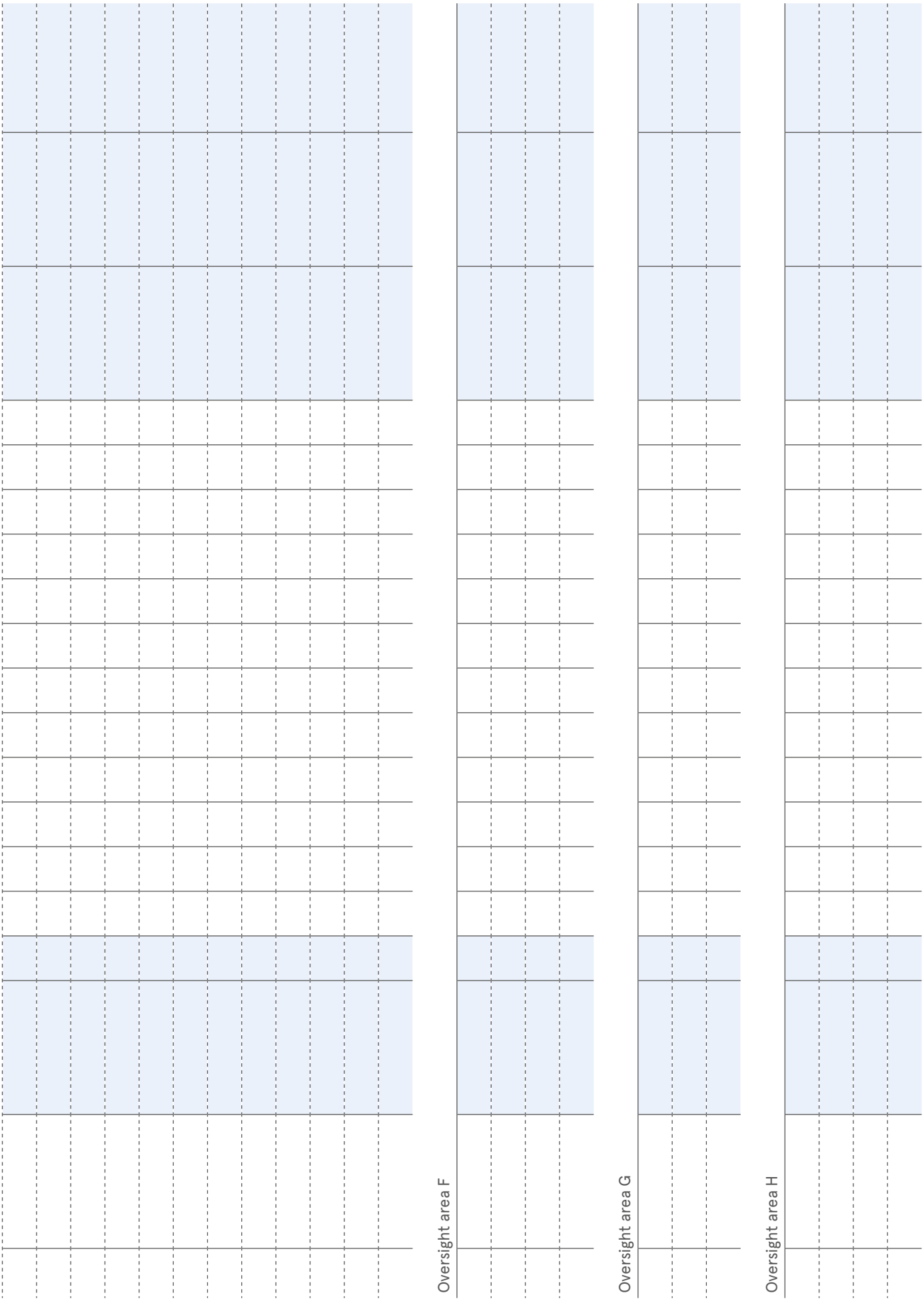
STATUTORY RULES	Statutory provision A	Statutory provision B	Statutory provision C	Statutory provision D	Statutory provision E	Statutory provision A	Statutory provision B	Statutory provision C	Statutory provision D	Statutory provision E	Statutory provision A	Statutory provision B	Statutory provision C	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						
OVERSIGHT AREA	Oversight area A										Oversight area B											

Oversight 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															
Oversight 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 checks but only TET's technical checks of access rights etc.)

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

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


Oversight area F
Oversight area G
Oversight area H

Technical information sheet for [IT system]

TO BE FILLED IN BY TET

Date of sending to [DSIS/DDIS/CFCS/RPNR]	Date of technical meeting	Participants from TET	Participants from [DSIS/DDIS/CFCS/RPNR]
Date of receipt from [DSIS/DDIS/CFCS/RPNR]	Caseworkers with TET		
Date of sending of consultation	Date of receipt of consultation responses		

Guide to filling in form (Word) and related system flowchart (Visio)

The bracketed text in the below form serves as a guide and is to be deleted in connection with the form filling process. Enter N/A for fields 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 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 gathered to being stored or transferred to other IT systems. Thus, the chart drawing must state the following:

- The data flowing to, being processed 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 through the system

TO BE FILLED IN BY [DSIS/DDIS/CFCS/RPNR]

Overall description of the system

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

System master data

System name(s)	[State the system call name or names if the system has more than one name]
Products/producers 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, other 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 name]
Data owner	
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]

IT infrastructure of the IT system

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, state web link or explain how the IT system is accessed/the client is commissioned]
Data sources to the IT system	[E.g. IT system with other 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 other IT systems	[Estimate in relevant format, e.g. records, MB, GB, number of documents, etc.]
Recipients of data from the system	[E.g. IT system with other agency, other departments, EDMS, internal database, etc.]
Data formats being transferred from the system	[E.g. PCAP, ZIP, XML, CSV, etc.]
Data volumes being transferred from the system	[Estimate in 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]

User and rights management

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 which 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 more systems, etc.]
Rights management	[Who grants and revokes user rights in the system?]

Routine erasure of data

Initiation of erasure	[Who ensures routine erasure/cleansing of data in accordance with any time limits for erasure?]
Erasure	[Are data in the system erased manually or automatically, e.g. via scripts? In manually, who does it?]
Frequency	[How often are data routinely erased/cleansed in the system?]

Backup og restore

Backup of data	[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?]

Logging of user activities

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

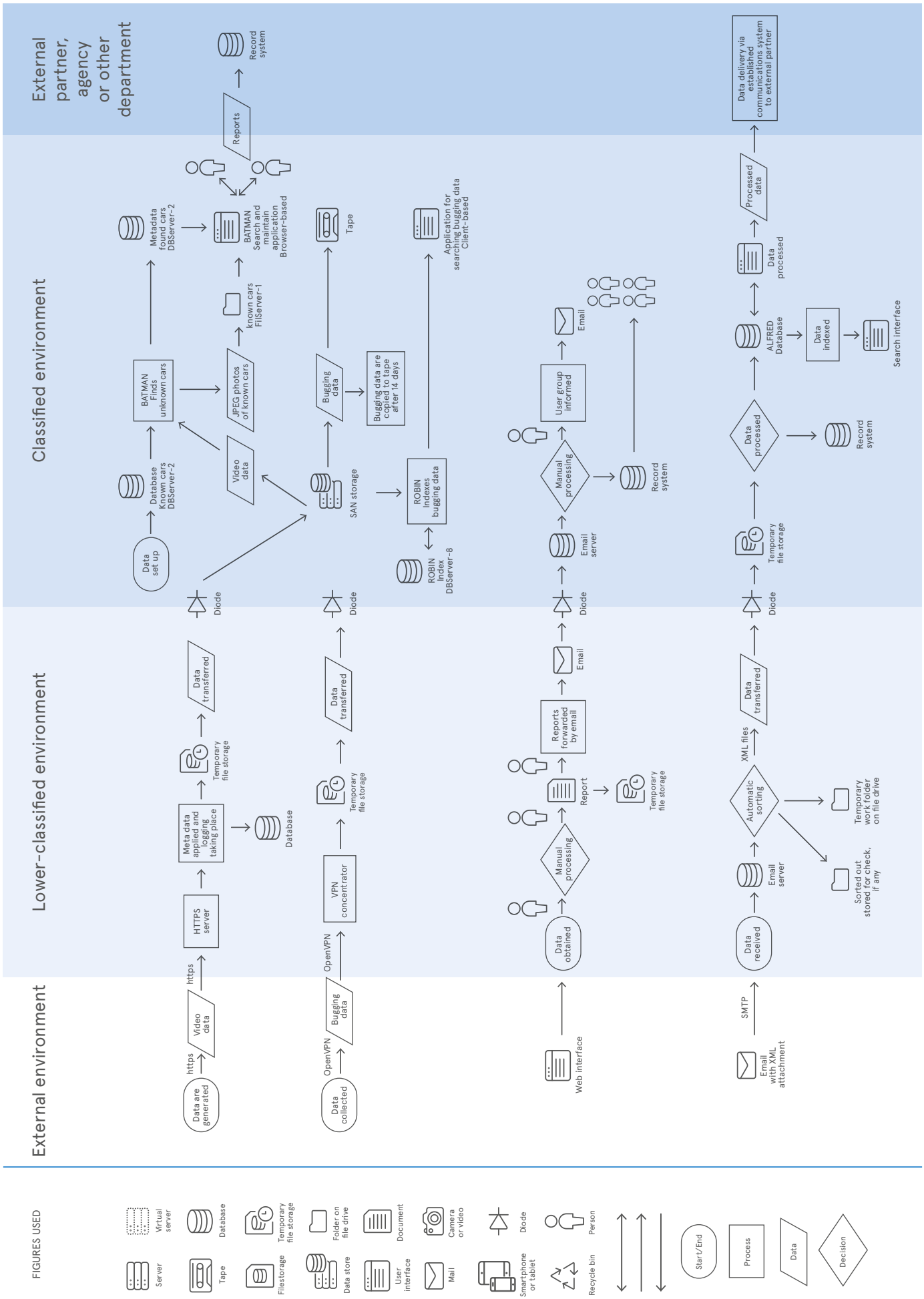
Documentation and guides

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]

TO BE FILLED IN BY TET

Any follow-up questions to technical meeting

NUMMER	QUESTIONS	ANSWER
1a		
1b		
2		


External environment
Lower-classified environment
Classified environment
External partner, agency or other department
Data are generated
https
Video data
https
HTTPS server
Meta data applied and logging taking place
Database
Temporary file storage
Data transferred
Data collected
OpenVPN
Bugging data
OpenVPN
VPN concentrator
Temporary file storage
Data transferred
Diode
Data set up
Database Known cars DBServer-2
BATMAN Finds unknown cars
Video data
JPEG photos of known cars
known cars FilServer-1
Metadata found cars DBServer-2
BATMAN Search and maintain application Browser-based
Reports
Record system
Diode
SAN storage
Bugging data
Tape
Bugging data are copied to tape after 14 days
ROBIN Index DBServer-8
ROBIN Indexes bugging data
Application for searching bugging data Client-based
Web interface
Data obtained
Manual processing
Report
Temporary file storage
Reports forwarded by email
Email
Diode
Email server
Manual processing
Record system
User group informed
Email
Email with XML attachment
SMTP
Data received
Email server
Automatic sorting
XML files
Data transferred
Diode
Temporary file storage
Data processed
Record system
ALFRED Database
Data processed
Data indexed
Search interface
Processed data
Data delivery via established communications system to external partner
Sorted out stored for check, if any
Temporary work folder on file drive
FIGURES USED
Server
Virtual server
Tape
Database
Filestorage
Temporary file storage
Data store
Folder on file drive
User interface
Document
Mail
Camera or video
Smartphone or tablet
Diode
Recycle bin
Person
Start/End
Process
Data
Decision

Danish Intelligence Oversight Board

Date:
Caseworker:
File no.:
Doc.:

Check of [agency] in [year] ([oversight subject])

1. Background and purpose

[*Description of TET's decision (date of the meeting), the purpose of the check as well as TET's overall risk assessment of the oversight area*]

"At the meeting held on [date], TET decided to perform a compliance check of [oversight subject] in [year]."

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

"TET's overall risk assessment of [DSIS / DDIS / CFCS / RPNR] in [year] showed a [low / limited / medium / high] risk of non-compliance with legislation. Specifically, TET found that there is a [low / limited / medium / high] risk of non-compliance with the rules on [procurement / internal processing / disclosure / legal political activity et cetera]."

2. Description of the oversight subject

[*Description of the oversight subject (system, database, process et cetera) and a brief objective description thereof and/or reference to where more detailed information may be found; emphasising the parts of the oversight subject which are particularly relevant for the check*]

"[The oversight subject] is [DSIS / DDIS / CFCS / RPNR] [system / database / process] for [...]."

"[The oversight subject] includes [...], of which [...] [is/are] deemed particularly relevant for TET's check."

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

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

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

"Against this background [...]".

4. Oversight method

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

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

The check was in the form of a [full check / sample check / content screening / inspection / interview-based check / decentralised data processing check] where [system / process has been examined through discussions with DSIS / DDIS / CFCS / RPNR employees and/or technical checks] / [the [cases / records et cetera] have been selected using [random/targeted sampling].]"

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

In TET's assessment, [completeness in the oversight has been achieved / it has not been possible to achieve completeness in the oversight] as [...]"

5. Experience

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

"The check showed that [...]"

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

Approved on [date] / [initials]

[Danish Security and Intelligence Service (DSIS)/
Danish Defence Intelligence Service (DDIS)/
Danish Centre for Cyber Security (CFCS)/
Danish National Police PNR unit (RPNR)]

Danish Intelligence Oversight Board

Date:
Caseworker:
File no.:
Doc.:

Follow-up on TET's compliance check of [oversight subject] in [year]

In the course of its oversight of [the Danish Security and Intelligence Service (DSIS) / the Danish Defence Intelligence Service (DDIS) / the Danish Centre for Cyber Security (CFCS) / the Danish National Police PNR unit (RPNR)] in [year], TET performed a check of, among other things, [oversight subject], focussing on [DSIS' / DDIS' / CFCS' / RPNR's] compliance with the rules on [procurement / internal processing / disclosure of information / legal political activity et cetera].

[Description of TET's oversight method, including the consultation date and the time allowed for consultation responses as well as any comments].

TET's check of [oversight subject] verified [DSIS' / DDIS' / CFCS' / RPNR's] [compliance with the legislation on procurement, internal processing and disclosure of information / showed that DSIS / DDIS / CFCS / RPNR has [...] in violation of the legislation.

In case of any comments by [DSIS / DDIS / CFCS / RPNR] as to the information that may be included in TET's annual report in terms of the description of the oversight area or whether [DSIS / DDIS / CFCS / RPNR] has any information concerning the follow-up check, TET requests to receive such comments within four weeks for purposes of TET's internal process for preparing the annual report for [year]. TET will include any comments from [DSIS / DDIS / CFCS / RPNR] in the assessment of how to describe the oversight area and any follow-up check in TET's annual report for [year].

Reference is made to [DSIS' / DDIS' / CFCS' / RPNR's] reference no. [...]].

Yours faithfully
Danish Intelligence Oversight Board

by/[name]
Chair

NAME	SYSTEMNAME	NETWORK/CONTEXT	DNS DOMAIN	PRIMARY SOFTWARE	BRIEF DESCRIPTION OF SERVER FUNCTION/ROLE
Server name (NETBIOS or DNS)	Business system(s) which the server forms part of	State the network/ context which the server forms part of	State if the server form part of a DNS domain. If not, state N/A or work group	Primary server software	Comments and/or explanations concerning server function, data or other relevant matters that may contribute to understanding the server role

SYSTEM NAME	DESCRIPTION	NETWORK/CONTEXT/ ENVIRONMENT	MOST RECENT CHECK	RELEVANCE SCORE	RELEVANCE ASSESSMENT
State system name	Brief description of the system	State the environment, context or network on which the system is being operated. If the system is being operated on multiple environments, state which.	State the year in which the system was most recently checked, state whether oversight type A or B was applied	Systems are broken down into the following categories: 1. Relevant system (ranked) 2. Relevant system 3. Not relevant system	Where relevant, written explanation of or comment on category breakdown.

Standards for Danish intelligence oversight activities
Published by TET, June 2022

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