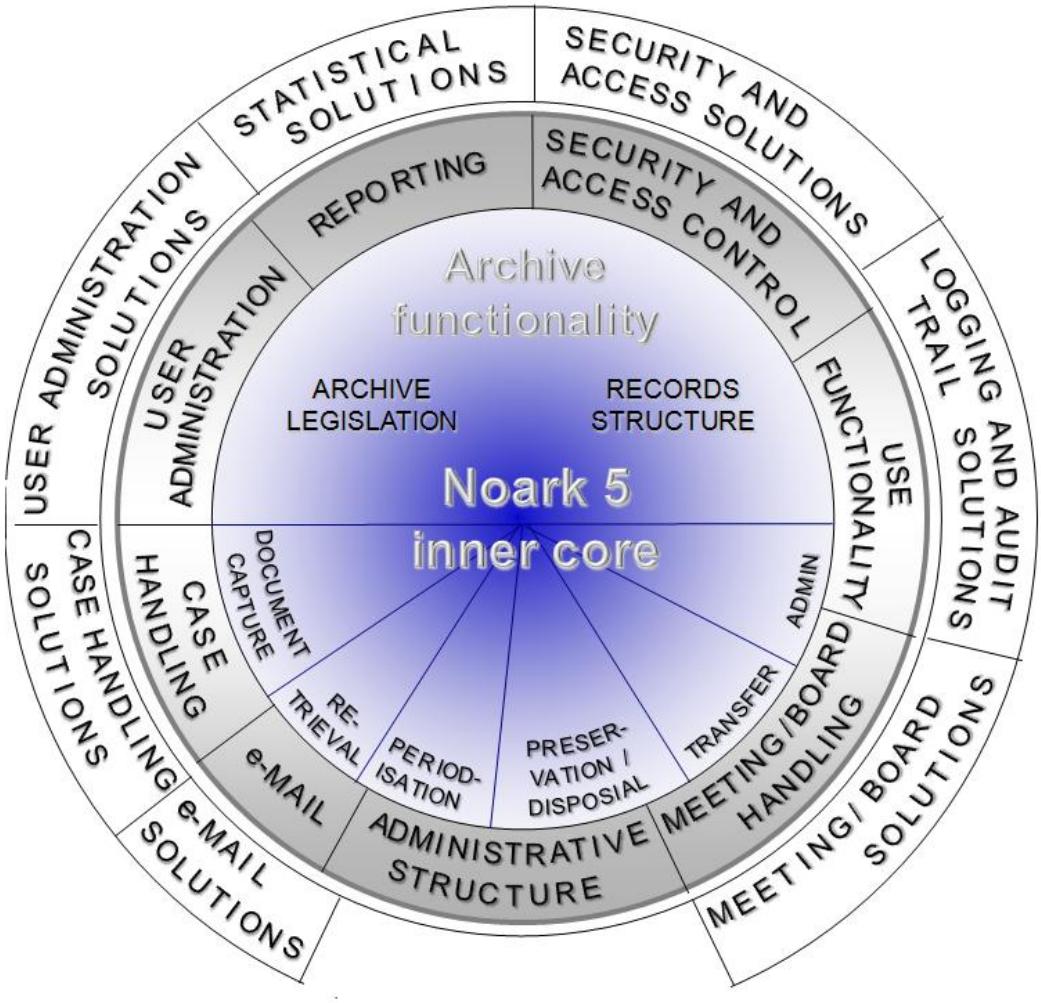
Noark 5
Standard for Records Management



Version 2.0

03.04.2009

CONTENTS

Part I: General

1 Introduction

1.1 History

Noark is a Norwegian abbreviation for *Norsk arkivstandard*, or "Norwegian Archive Standard". Noark was developed as a specification of requirements for electronic recordkeeping systems used in public administration in 1984 and quickly became established as the de facto standard. The standard was developed further with new reports in 1987 (Noark 2) and 1994 (Noark 3). This further development covered both modernisation in line with technological advances and expansions to the systems' information content and functionality.

In 1995, a corresponding specification of requirements was developed for the municipal sector, Koark. Koark was based on the same principles as Noark, but had a number of additions specifically adapted to the needs of the municipal sector, e.g. political case handling.

Noark 4, which arrived in 1999, included the specifications in Koark and became a common standard for public sector administration. Noark 4 took the standard a major step further by specifying a complete electronic records management system, integrated with e-mail and general case handling systems. Noark 5 further develops the principles from Noark 4.

When the Archives Regulation was introduced on 1 January 1999, it became mandatory for public bodies to use a Noark-based system, approved by the Director General of the National Archival Services of Norway, for electronic recordkeeping. Since 1 October 2002, Chapter IX of the National Archival Services of Norway's Regulation on the electronic archiving of case documents has stipulated that the recordkeeping of electronic case documents should generally be carried out in a system that fulfils the requirements of the Noark standard and is approved by the National Archival Services of Norway. This applies regardless of whether a simple recordkeeping and archive system is used or recordkeeping functions are integrated in a case handling system or other similar system. When case documents are archived electronically, the system must meet the requirements for electronic archiving in the Noark standard and be approved for this purpose by the Director General of the National Archival Services of Norway.

1.2 Background to the project

Since Noark 4 arrived in 1999, there have been significant changes on several fronts: organisational, work- and cooperation-related and technological.

There are many reasons why work began on Noark 5, but a key factor was strong pressure from both the public sector and suppliers to bring about good solutions for integration between Noark-based systems and task systems.

Since 1999, national and international standards of relevance to electronic recordkeeping and archiving have also been formulated. These areas are not covered adequately in Noark-4.

The Director General of the National Archival Services of Norway therefore considered it necessary to establish a project to draw up a standard which covers these areas up to a level

which ensures that all documents and transactions are handled in line with the Norwegian Archives Act. This project was established in September 2005.

1.3 Project organisation

The project consisted of a steering group, a project group and a number of reference groups. *The Project Manager* was Anne Mette Dørum of the National Archival Services of Norway.

The Steering Group consisted of:

- Ivar Fonnes, National Archival Services (chairman)
- Trond Sirevåg, National Archival Services
- Ingvar Engen, Ministry of Culture and Church Affairs
- Katarina de Brisis, Ministry of Modernisation (September 2005–September 2006)
- Henrik Linnestad, Ministry of Government Administration and Reform (September 2006–March 2007)
- Christer Gundersen, Norwegian Association of Local & Regional Authorities (September 2005–September 2006) and Ministry of Government Administration and Reform (March 2007–May 2007)
- Kristian Bergem, Ministry of Government Administration and Reform (from May 2007)
- Line Richardsen, Norwegian Association of Local & Regional Authorities (from September 2006)
- Anne Mette Dørum (project manager and secretary of the Steering Group)

The Project Group consisted of:

- Herbjørn Andresen, Department of Informatics, University of Oslo (from November 2006)
- Martin Bould, National Archival Services (to November 2006)
- Tor Anton Gaarder (from January 2007)
- Jon Atle Haugen, National Archival Services
- Synnøve Hellevik, National Archival Services (to February 2008)
- Øivind Kruse (from January 2007)
- Anthony Lærdahl, National Archival Services (to June 2007)
- Birgitte Olafsen, National Archival Services (to December 2006)
- Petter Svendsen, National Archival Services

The Working Group that worked on the chapter concerning meeting handling consisted of:

- Kari Remseth, Inter-Municipal Archive in Trøndelag (chairman of the group)
- Elin Harder, Directorate for Nature Management
- Jan Tore Helle, Inter-Municipal Archive in Hordaland
- Rolf Petter Waage, Inter-Municipal Archive in Møre og Romsdal.
- Astrid Øksenvåg, Norwegian Association of Local & Regional Authorities.
- Ståle Prestøy, Inter-Municipal Archive in Trøndelag (secretary of the group).

The reference group consisted of many players from both the private and public sectors. Specific problems linked to personal privacy issues were discussed with the Norwegian Data Inspectorate where necessary. Similarly, specific problems linked to security issues were

discussed with the National Security Authority when necessary. The Norwegian Press Association was also contacted when necessary.

Special thanks go to hired consultant Paul Hoseth of Mesan AS, who with great patience and inestimable expertise assisted the project to realise the vision of a Noark 5 core Thanks must also go to Heidi Einarsen of the National Archival Services for her considerable writing efforts on the home straight.

1.4 Requirement types in Noark 5

Noark 5 sets out requirements concerning record structure, metadata and functionality, but does not contain any requirements concerning how these requirements should actually be met in system development. Noark 5 therefore does not define a system, but facilitates for different solutions.

The requirements are stricter for depositing, transfer and migration. Obligatory metadata must be included in the export, and the export must have a defined structure.

The standard does not contain a description of procedures or the way in which different requirements can be met. Where it is necessary in order to understand the requirements, some introductory text has nevertheless been included before the tables of requirements. The tables of requirements set out all applicable requirements. The tables of requirements have been set up in the following way:

Req. no.	<area covered by requirements>	Type	Remarks

Req. no.: Requirement numbering is divided into <chapter no.>. <serial number within chapter>
(for example, 4.11 means chapter 4, requirement no. 11).

<area covered by requirements>: This specifies the area for which requirements are imposed in the table.

Type: Specifies the type of requirement. The following are used here:
- O (Obligatory)
- B (Conditional obligatory)
- V (Optional)

Remarks: Remarks concerning the requirement, e.g. conditions for when the requirement becomes obligatory.

Obligatory and conditional obligatory requirements are indicated by “must” in the description of the requirement. Optional requirements are indicated by “should” in the description of the requirement. Conditional obligatory requirements are obligatory under certain conditions. These conditions are described in more detail in the remarks field.

It will be appropriate to give Noark 5 approval for three main types of system:

- Case record systems
- Task systems with correspondence documents
- Task systems without correspondence documents

All these systems will be electronic document management systems, although they may also contain references to physical documents. Task systems without references to documents fall outside the type of system for which it is appropriate to give Noark 5 approval.

Case record systems are general case handling and records management systems. This is the only type of system so far to have been given Noark approval. *Task systems with correspondence documents* (also known as task systems with recordkeeping functionality) are specialised case handling systems which handle incoming and outgoing documents. Task systems without correspondence documents do not handle such documents and will often be extremely simple records management systems[1].

The obligatory requirements are obligatory for all three main types of system. Some conditional obligatory requirements will only be obligatory for case record systems. Other conditional obligatory requirements may be obligatory for systems that contain documents which must be retained for more than 10 years. In other cases, such a requirement may be obligatory if a previous optional requirement is to be fulfilled.

Noark 5 approval will not cover the optional requirements, but suppliers must state the optional requirements that they fulfil. Most requirements concerning case handling, security and access, user administration, etc. are optional. This does not of course mean that these requirements are less important and can therefore be omitted. In many cases, the way in which the optional requirements are met will be decisive for the system that a user chooses. This could therefore be a competitive advantage for suppliers. Users must decide which optional requirements they need and then require the supplier to fulfil them.

1.5 Relationship to Nordic standardisation

The project has regularly kept in contact with environments that are involved in national standardisation work, such as the Norwegian Standards Council, the Semantics Register for Electronic Collaboration (SERES) and the Coordination Body for e-Administration (*Koordineringsorganet for eForvaltning* (KoeF), and work relating to open standards, electronic signatures and identification.

Many Norwegian projects were taken into consideration during the formulation of the requirements. These include:

- Specification of requirements for PKI in the public sector
- ELMER 2 – Guidelines for user interfaces in official forms on the internet
- Proposed strategy for the use of eID and e-signatures in the public sector
- Report to the Storting no. 17 (2006-2007) *Eit informasjonssamfunn for alle* (An Information Society for All)
- Shared ICT architecture in the public sector

[1] Within a case record system, there may also be series without correspondence documents, e.g. a series which contains meeting documents.

The project has had interesting and productive exchanges of views and experiences with the FESD project (*Fælles systemer til elektronisk sags- og dokumenthåndtering i den offentlige sektor* – Shared Systems for Electronic Case and Document Management in the Public Sector) in Denmark. The FESD project has established a common technical standard for recordkeeping and case handling systems, based on Noark 4.

In Sweden, the Long-term Digital Preservation project was an important source of input in formulating the Noark 5 transfer requirements.

The project has drawn on experience from the Sähke project in Finland, a project relating to the long-term preservation of electronic documents.

1.6 Relationship to international standardisation

The work relating to Noark 5 was based on international standards where relevant. These include:

- ISO 15489-1 and 2: 2001 Information and documentation - Records management (Part 1: General, Part 2: Guidelines). This is an international standard for records management design.
- MoReq - Model Requirements for the management of electronic records (European Commission 2002). This is an EU standard for records management design based on ISO 15489. MoReq2 was released in February 2008.

- ISO 23081-1: 2004 Information and documentation - Records management processes - Metadata for Records. This is an international standard for metadata for records.
- ISO 14721: 2002 Reference Model for an Open Archival Information System (OAIS). This is an ISO standard for the preservation of archival records.

- Data Dictionary for Preservation Metadata: Final Report of the PREMIS Working Group (OCLC and RLG 2005). PREMIS stands for "Preservation Metadata: Implementation Strategies". The PREMIS Working Group describes a model – a core of metadata – which can be used for digital preservation, irrespective of the type of documents or preservation strategies.

The international standards for archive design and archival repositories are directly linked to Noark 5 in the sense that where the requirements in the standards have a strong relevance to Norwegian circumstances, we have used the requirements almost directly translated. Where the relevance has been weaker, we have ensured that the requirement formulations in Noark 5 take the requirements into consideration wherever possible, giving special consideration to Norwegian administrative practice and law.

During the project period, the project manager was involved in the work relating to the development of MoReq2 as a participant on the Editorial Board. To ensure that Noark 5 is in line with MoReq2, the project primarily related to MoReq2's requirements, as they were completed.

Many of the project participants have been involved in an international training scheme, which is a follow-up to the report from the PREMIS Working Group.

2 Legal framework conditions

2.1 Introduction

A recordkeeping and archive system must be in line with the requirements set out in laws and regulations. This chapter considers the general legal requirements with which a Noark 5-based system must comply. In this context, "general legislation" is used in particular to refer to administrative, confidentiality, recordkeeping and personal privacy legislation, but other special legislation may also apply.

Noark 5 must enable an individual organisation to comply flexibly and effectively with general legislation. However, it is also important that the organisation is aware of other special legislation which could be of significance to the archive. Other regulations may affect archive-related circumstances, and in certain contexts these regulations will have consequences for archive-related work performed by public bodies.

The key legal framework conditions for the Noark 5 standard are set out in the following legislation and regulations:

- Act of 4 December 1992 No. 126 on archives (*the Archives Act*).
- Regulation of 11 December 1998 No. 1193 on official archives (*the Archives Regulation*).
- Regulation of 1 December 1999 No. 1566 on supplementary technical and archive provisions concerning the management of official archives (*the Director General of the National Archival Services of Norway's provisions concerning official archives*).
- Act of 10 February 1967 on the processing method in administrative cases (*the Public Administration Act*).
- Regulation of 25 June 2004 No. 988 on electronic communication with and within public bodies (*the e-Administration Regulation*).
- Act of 19 May 2006 No. 16 on right of access to documents held by the public administration and public undertakings (*Freedom of Information Act*), which supersedes the Act of 19 September 1970 No. 69 on right of access within the public administration (*Freedom of Information Act*).
- Act of 14 April 2000 No. 31 on the processing of personal data (*the Personal Data Act*).
- Regulation of 15 December 2000 No. 1265 on the processing of personal data (*the Personal Data Regulation*).
- Act of 15 June 2001 No. 81 on electronic signatures (*the e-Signature Act*).
- Act of 20 March 1998 No. 10 on preventive security services (*the Security Act*).
- Decree of 17 March 1972 No. 3352 on the processing of documents requiring protection for reasons other than those referred to in the Security Act and regulations (*the Protection Decree*).

2.2 Relationship to public bodies' archive function

An archive system is a tool for managing the archive function of an organisation. For Noark, this is particularly a question of the archive function within the public administration, and the specifications must therefore be adapted to the framework and requirements that apply to this.

The archive function within the public administration consists of maintaining an overview of documents for
handling (case documents), placing the documents in their handling
context (cases), distributing documents to the handling link, following up with respect to the handling link, archiving documents that have been handled, responding to internal and external enquiries concerning case handling status and concerning the content of documents, searching for/retrieving documents on request, lending documents or distributing copies, etc. After a number of years, the archive material must be set aside and subsequently delivered to an archival repository as documentation of the activity where it occurred.

The recordkeeping and archive functionality must be a tool for every area of the archive function. For the organisation as a whole, the recordkeeping and archive functionality will often be integrated in an associated case handling system or task system. The recordkeeping and archive functionality will be used to register and archival documents and other information and to search for and retrieve this information and distribute it. The solution must of course be designed to perform the tasks involved in both the archive function and in the organisation's collective document management as effectively as possible. Consideration must also be given to the fundamental framework established through applicable laws and regulations, including the definition of what kind of documents the archive is to cover. The system must also facilitate satisfactory quality assurance in the archive function.

2.3 Laws and regulations

The regulations help to ensure the documentation of the public administration's actions and decisions, partly for administrative and legal purposes and partly for knowledge and research purposes in the future. Pivotal provisions concern the obligation to maintain fonds, organisation of the recordkeeping function, the type of material to be stored in the archive, what is to be retained for the future and how it is to be stored. However, relatively detailed provisions are also set out concerning archive procedures, linked to areas such as document handling, recordkeeping, lending, the setting aside of older material and transfer to an archival repository.

It is however not just the archive regulations and the Archives Act that affect the archive functions. A number of other laws and provisions must also be taken into consideration. This particularly concerns the *Freedom of Information Act*, which is of importance for recordkeeping, the presentation of official records and the screening of information. *The Public Administration Act* sets out general rules concerning case handling, in addition to specialised provisions concerning confidentiality obligations and special access for involved parties. It is important to be aware of the *e-Administration Regulation* pursuant to the e-Signature Act and the Public Administration Act. This regulation sets out more specific rules concerning electronic communication with and within the public administration. *The Personal Data Act*

and the associated Regulation (*the Personal Data Regulation*) regulates the processing of personal data.

It is also necessary to take into consideration the written and unwritten rules implied by the term *good administrative practice.* This covers keywords such as equality (precedence), complete decision-making basis, the requirement for enquiries made to the public administration to be answered within a reasonable period of time (cf. back log control), etc.

Special legislation of relevance includes the *Security Act* and the *Protection Decree,* which set out provisions concerning information which must be protected for national security or other reasons. Another law is the *e-Signature Act*, which facilitates the use of electronic signatures in connection with electronic communication with and within the public administration.

Noark 5 must support other archive functions which fall within the framework of the regulations, and it must avoid building in functionality that is not permitted. Within the various areas, a series of examples of requirements which the standard must fulfil is presented below. It should be noted that these examples do not exhaustively describe the legal requirements for the individual areas of legislation, but are intended solely as illustrative examples.

2.4 The Archives Act and associated regulations

The public administration's archive function has been regulated for many years through specific regulations. The Act of 4 December 1992 No. 126 on archives (the Archives Act) entered into force on 1 January 1999. The same date saw the entry into force of the Regulation of 11 December 1998 No. 1193 on official archives (the Archives Regulation). The Regulation of 1 December 1999 No. 1566 on supplementary technical and archive provisions concerning the management of official archives (management of official archives) was introduced as a result of a need for further regulation, partly to regulate the electronic archiving of archive material. Collectively, the Archives Act, Archives Regulation and Regulation on the management of official archives form the core of the regulations that regulate the management of official archives.

The Archives Act sets out a number of general and fundamental provisions concerning archives and, in particular, archives within the public administration. With few exceptions (cf. Section 5 of the Archives Act), these provisions apply to all activities within the public administration.

The purpose of the Archives Act is to secure archives that are of significant cultural or research value, or which contain legal or important administrative information, so that they can be managed and made available for use in the future; cf. Section 1 of the Archives Act. Furthermore, Section 6 of the Archives Act states that public bodies are obliged to have archives and that these archives must be organised and set up in such a way that the documents are secured as sources of information for both the present and the future.

Together with the supplementary regulations, the Act represents a complete legal framework relating to all archive-related issues in the public administration, right from the initial creation of a document in the course of everyday operations, via archive limitation and the transfer of

important archive material to archival repositories, and during the storage and making available of the material for use in the future.

2.4.1 Records management design

To ensure authentic documentation, it is important that solutions are established for optimal document capture, i.e. that documents that are to be archived are identified, "captured" and archived. This involves the documents being linked to metadata (registered) and archived in a way which ensures that they can be retrieved in unaltered form. The document capture can be anything from the manual processing of hard copy documents to a fully automated process for electronic documents.

Regardless of the method used, document capture leads to archiving, and there should basically be no limitations on this capture. When establishing both self-service solutions for industry and the public and solutions for case handling and cooperation within or between public bodies, there are major efficiency gains to be had from incorporating automated document capture, i.e. functions for capturing and freezing documents. Ensuring good document capture meets the needs of enterprises to establish solutions for good knowledge management and decision-making support, the legal rights of the parties involved, openness within the public administration and future cultural and research-related needs.

2.4.2 Archiving obligation and archive weeding

The Archives Act and associated regulations mean that any public body will normally be subject to an express *archiving obligation*, i.e. an obligation to *archive all documents that are created as part of the operations that the body conducts*, regardless of whether this concerns a document that is sent to the body or a document that the body itself produces. This follows from Section 6 of the Archives Act. The definition of document in the Archives Act is technology-neutral and extremely broad; a document is defined as "a logically delimited quantity of information that is stored on a medium for subsequent reading, listening, presentation or transfer".

Exempt from the archiving obligation are those documents that are covered by the provisions relating to *archive limitation* in accordance with Sections 3-18 and 3-19 of the Archives Regulation. "Archive limitation" means that documents which are created as part of the operations conducted by the body but which are neither subject to case handling nor of value as documentation, will be kept outside or removed from the archive. Each individual body must continuously carry out archive limitation.

Section 3-19 of the Archives Regulation contains five groups of material that are covered by archive limitation, i.e. meaning either that the material is not to be archived at all or that it should subsequently be removed from the archive once it has been archived. Note however that there are important exemptions in the first four of these groups.

2.4.3 Recordkeeping obligation

The Archives Regulation also introduces a *recordkeeping obligation* for all public bodies. The obligation to register documents has been narrowed down in relation to the obligation to archive documents. The documents that are covered by this recordkeeping obligation are set out in Section 2-6 first paragraph of the Archives Regulation:

- Firstly, it is a requirement that the document must be considered a *case document for the body,* as defined in the freedom of information legislation. A case document for the body is a document that has been received by or submitted to a body, or which the body has itself created, and which concerns the body's area of responsibility or operations. A document is created when it is dispatched by the body. If this does not take place, the document is considered to be created when it is finalised.
- Secondly, a document must *form part of correspondence,* i.e. it has been received or sent out by the body.
- Thirdly, the document must have *substantial content,* i.e. it must both be subject to case handling and be of value as documentation.

When all three of these criteria are met, there is therefore *an obligation* to enter the document into a journal. Documents covered by the rules concerning archive limitation should not however be recorded. Beyond this, it is largely up to the body itself to decide what should or should not be entered into a journal.

In other words, the body has an *obligation* to archive documents that have been received or dispatched by the body. A body's internal documents are entered into a journal as and when the body deems it appropriate.

2.4.4 Disposal and deletion

Disposal means that archive material that has been subject to case handling or been of value as documentation is removed from the archive and deleted or destroyed.

Section 9(c) of the Archives Act sets out provisions which state that archive material cannot be disposed of except pursuant to regulations or with the specific consent of the Director General of the National Archival Services. The ban on disposal in the Archives Act takes precedence over provisions concerning disposal in or pursuant to other laws. Notwithstanding this, the Norwegian Data Inspectorate may make decisions concerning the deletion of personal data pursuant to Section 29 of the Personal Data Act. However, such deletion can only be carried out after a statement has been obtained from the Director General of the National Archival Services.

Material covered by provisions concerning preservation cannot be discarded without the permission of the Director General of the National Archival Services. 'Preservation' means that archive material is retained for the future and transferred to an archival repository. Section 3-20 of the Archives Regulation sets out specific obligatory requirements concerning preservation.

Disposal is an irreversible action. No form of deletion or other disposal may take place without special thorough case preparation, in order to eliminate the possibility of material that should have been retained being unintentionally disposed of.

It is stressed that disposal must not be confused with archive limitation.

2.5 Freedom of Information Act

The new Freedom of Information Act of 19 May 2006 No. 16 will have an expanded scope in relation to the Freedom of Information Act of 1970. This means that more types of activity must comply with the new Freedom of Information Act.

The purpose of the Act is to ensure that public bodies are open and transparent, in order to enhance freedom of information and free speech, democratic participation, the legal rights of the individual, confidence in the public sector and public control. The Act is also intended to facilitate the re-use of official information.

The principal rule in the Act is that the body's case documents, fonds and other similar registers are open to inspection unless otherwise follows from a law or a regulation pursuant to a law. Anyone can request access to case documents, fonds and registers that are similar to case documents that are archived by the body concerned.

Anyone may also request access to a summary of information that is electronically stored in the body's databases if the summary can be prepared using simple procedures.

Public bodies that are covered by the Act are obliged to maintain fonds in accordance with the rules in the Archives Act and associated regulations. Public bodies that maintain electronic registers must make the register publicly available on the internet in the manner that is set out in the Regulation pursuant to the Freedom of Information Act.
Documents may be made publicly available on the internet, with the exception of information that is subject to a confidentiality obligation in a law or pursuant to a law.

2.6 Public Administration Act

The Act of 10 February 1967 on the method of processing in administrative cases (*the Public Administration Act*) regulates certain types of archive material through provisions concerning the rules that apply to case handling and concerning the rights that the Public Administration Act accords the individual. The purpose of the Act is to regulate the rights of citizens when they come into contact with public bodies. The Public Administration Act is intended to protect the legal rights of citizens and ensure appropriate case handling. The Act is a general law which applies to case handling provided that no other law is applicable under special legislation.

Most exemptions under the Freedom of Information Act on the basis of a statutory confidentiality obligation are based on Sections 13 to 13 f of the Public Administration Act. Involved parties' right of access to information in accordance with the Public Administration Act is regulated in Section 18, which is the main rule concerning a person's right to access documents that concern themselves. In addition, many special laws contain similar provisions concerning access to information concerning yourself.

2.6.1 e-Administration Regulation

The Regulation on electronic communication with and within the public administration entered into force on 1 July 2002. This Regulation has been revised and the revised Regulation on

electronic communication with and within the public administration was adopted on 1 July 2004.

The purpose of the Regulation is to prepare a common set of regulations which set out the framework for the secure and effective use of electronic communication with and within the public administration. The Regulation is intended to promote predictability and flexibility and to facilitate for the coordination of secure and appropriate technical solutions, including e-signatures.

The e-Administration Regulation contains provisions which set out guidelines for routines and procedures linked to recordkeeping. Chapter 2 includes provisions which state that any individual who contacts an administrative body can in principle use electronic communication, that the administrative body must confirm that the communication has been received and how requirements concerning access should be handled. The chapter also covers how confidential information and personal information should be distributed and how parties should be notified of individual decisions that have been taken. Chapter 6 sets out provisions for the administrative body's handling of messages that are encrypted or signed with an electronic signature. Of particular importance here is Section 26, which sets out provisions concerning the archiving of advanced electronic signatures, etc.

2.7 Personal Data Act

The Act of 14 April 2000 No. 31 on the processing of personal data (*the Personal Data Act*) entered into force on 1 January 2001. The Act supersedes the Personal Data Registers Act from 1978.

The Act covers the processing of personal data using electronic tools and the manual processing of personal data which involves the creation of a personal register.

The purpose of the Act is to protect the individual from having personal information about them misused through the handling of data. The intention of the Act is to help ensure that personal data is handled in accordance with fundamental considerations relating to personal privacy, including the need for personal integrity and personal privacy and to ensure that personal data is of adequate quality.

The Personal Data Act focuses on the "processing of personal data". The term therefore indicates the scope of the Act. The Act does not cover the processing of personal data that an individual carries out solely for personal or other private purposes.

The processing of personal data covers any and all use of personal data: collection, record, collation, storage and distribution or a combination thereof.

2.8 E-Signature ACt

The Act of 15 June 2001 No. 81 on electronic signatures (*the e-Signature Act*) entered into force on 1 July 2001. The Act is intended to ensure that providers of certificate services and products on the Norwegian market fulfil a specific higher security level. The security requirements must be balanced between commercial, consumer and social considerations.

An electronic signature can be used to verify that electronically transmitted information has not been altered during sending, to provide confirmation of who sent the information and as verification that the sender will not be able to deny that he sent it. These functions are referred to as the securing of integrity, authenticity and non-repudiation.

Electronic IDs and electronic signatures are necessary preconditions for the greater use of electronic services which require the communicating parties to identify themselves and bind themselves to the content of the communication in a way which can be traced or which requires confidentiality protection.

The use of standardised electronic signatures paves the way for the digitalisation of many public services. Users can reuse a particular ID for many services. This makes life simpler and easier for the individual when they interact with the public sector.

The Act does not confer a general right to communicate electronically. If a requirement for a signature is imposed, the use of a qualified electronic signature will always fulfil such a requirement, providing it is possible to perform the action electronically. This means that such an electronic signature is accorded the same legal effect as a handwritten signature. However, the Act does confer the right to impose additional requirements in connection with communication with and within the public administration.

The Act implements the EU Directive on a Community framework for electronic signatures and Noark 5 establishes a framework for the use of electronic signatures.

2.9 Security Act

The Act of 20 March 1998 No. 10 on a preventive security service (*the Security Act*) entered into force on 1 July 2001. The Act supersedes the Security Decree and contains a separate chapter on information security.

The purpose of the Act is to protect national security and vital national security interests against espionage, sabotage and terrorism through the use of preventive measures, and applies to the entire public administration. The Act also aims to protect the legal rights of the individual and ensure trust in and simplify control of the service. The measures must be implemented within the government, municipal authorities and private enterprises covered by the Act.

Regulations have been prepared concerning information security, personnel security, industrial security and security administration. The archive-related processing of documents classified under the Security Act is covered by a special Regulation on information security.

2.10 Protection Decree

The Decree of 17 March 1972 No. 3352 on the processing of documents requiring protection for reasons other than those referred to in the Security Act and associated regulations (*the Protection Decree*) cover documents irrespective of the media on which they are available.

The protection of a document in accordance with the Protection Decree must only be carried out when the document can be classified as confidential under the Freedom of Information Act and harmful effects could result.

3 Noark 5: National standard for recordkeeping

3.1 Applications for Noark 5

Noark 5 is to be used for all types of recordkeeping, irrespective of the technological solution or type of public body. All activities that generate documents which need to be stored and retrieved in authentic form should in principle be covered by a recordkeeping function. This is completely independent of whether the documents are dealt with by traditional case handling, the number of years that they are to be archived for and whether they are to be transferred to an archival repository.

Noark 5 has therefore been written with regard to both the public and the private sector, as well as organisations which are planning to procure a new system or which wish to assess the system that they have already introduced. Although the Noark standard is only obligatory within the public sector, it should also be possible to use the standard in connection with the procurement of solutions for handling archival documents within the private sector.

The standard has been prepared from a holistic perspective, based on the archive's function in an electronic environment. The principal focus has always been to establish a set of requirements which can ensure that the functions that are developed lead to the appropriate handling of an electronic archive.

There are many types of case handling that have traditionally not been recorded in an archive, and within archive terminology, this has been known as *batch case handling.* This could for example be an application for a municipal childcare place, an application for the deferment of a regular vehicle check or the submission of various form-based information. As this type of case often involves large volumes of documents, it has for resource reasons been decided not to register the case documents in an archive, even though they largely come under the archiving obligation. Through the use of solutions based on the core requirements in Noark 5, integration with case handling and form handling systems and automated recordkeeping, archiving and document distribution, it will also be possible to maintain control over documents in such cases. A precondition is that archive-related requirements and conditions must be included when systems, processes and routines are planned and specified.

Noark 5 is a technology-independent standard. Specific requirements concerning technologies, such as approved archival formats for electronic documents, have been removed from the standard and placed in the regulations issued pursuant to the Archives Act. The requirements are technology-neutral and not based on or formulated with regard to any particular technological solutions.

3.2 The requirement structure in Noark 5

An *archival document* consists of the elements: content, structure, context and presentation. The content is contained in one or more electronic or physical documents which reproduce the archival document's "message". The documents must be stored in such a way as to enable future users to understand both the message itself and the original context of the message. This implies that, in addition to its content, the archival document contains information (metadata) concerning content, context and structure.

The presentation is dependent on a combination of the archival document's content, structure and (for electronic records documents) the software in which the archival document is being viewed. The content of an archival document must be unalterable and protected from access by unauthorised persons. "Unalterable" means that it must be protected from change and deletion (unauthorised disposal). The archival document and associated metadata must therefore be "frozen" so that it cannot be altered. It is important to link integrity protection to archival documents, i.e. any changes can be detected. The requirement for readability (presentation) means that it must be possible to recreate appearance and content over time.

Recordkeeping is the core of all disciplines that consider case documents to be part of the organisation's collective information resources. Through systematic and controlled recordkeeping, the archived documents will demonstrably be genuine, credible, retrievable and readable. Linking the documents to metadata and storing them in an unalterable form ensures that any document you are to use is, in terms of its content, identical in every way to the document that was originally prepared or received.

The point of view above does not just apply to traditional, correspondence-based case handling within government ministries for example. It is also at least as important to document what an organisation has received and generated in terms of documents in cases where automated case handling is used to some degree in specialised task systems or decision-support systems.

Document capture, the provision of metadata and the archiving of documents must be possible in widely varying environments, from organisations which make extensive use of automated case handling and advanced case handling support, to organisations that need to manage simple post routines and archive individual files. One of the very simplest forms of recordkeeping will for example be the handling of photographs in photoboxes when vehicles pass a road tollbooth.

In order to avoid creating two sets of Noark 5 (one set of functionality requirements for an archive which can be used in any environment and one set of requirements for a complete, independent system), Noark 5 specifies three layers or levels – requirements for the inner core, requirements for the outer core and requirements for a complete Noark 5.

Inner core contains requirements for basic functionality for recordkeeping and archiving. The principal functions lie within record structure, metadata and requirements for systems which are set out in the regulations concerning archives. There are also requirements concerning the modules that the core must contain, i.e. data capture, searching, retrieval and viewing, administration of the core, preservation and disposal and transfer.

The requirements for the inner core must be met in order for the system to be approved as a Noark 5 solution.

Outer core defines the core's requirements concerning external, optional modules/systems. In order for the core to function in an integrated archive system environment, the core must impose some requirements concerning the relevant "optional" systems that are used in the environment. Between the Noark 5 core and peripheral systems, there is a "grey zone", which is Noark 5's requirements for external modules/systems.

The requirements for the outer core form part of the Noark 5 core and must be fulfilled in order for the system to be approved as a Noark 5 solution.

Complete Noark 5 specifies requirements and recommendations for some of the optional task and administration systems that will form part of a "complete" Noark 5 solution, i.e. a solution that is close to the current Noark 4 system. These are specifications which concern certain given task systems, which form part of a complete Noark 5 solution. This constitutes the outer layer of functionality in Noark 5. The requirements for the outer task systems do *not* form part of the mandatory requirements for the Noark 5 core.

The areas where Noark 5 deviates from Noark 4 are discussed separately after each section.

3.3 Transition from Noark 4 to Noark 5

Noark 5 will supersede Noark 4 (which in turn superseded Noark 3), but be backwards-compatible with Noark 4 in the sense that it will be possible to migrate archives from systems based on the older standard to the new one. This has been taken into consideration as regards both the construction of the record structure and the metadata that are defined. An example of this is that the units *fonds* and *series* are still retained in the record structure.

The public administration's case documents that are stored electronically must be linked to a recordkeeping system or some other electronic system for registering documents. The system must control all archiving of and access to the case documents.

The recordkeeping of electronic case documents must as a general rule take place in a system which follows the requirements in Noark and which has been approved by the Director General of the National Archival Services. This applies regardless of whether a pure recordkeeping and archive system is used or functions for archiving are integrated in a case handling system or similar. In connection with the electronic archiving of case documents, the system must meet the requirements for electronic archiving in Noark and be approved for this purpose by the Director General of the National Archival Services. If the system does not satisfy the requirements in Noark, the administrative body must apply to the Director General of the National Archival Services for dispensation. Dispensation must be granted before the system can be taken into use.

If case documents are to be exchanged by e-mail in connection with the electronic archive, the system should also satisfy the basic requirements for integrated e-mail.

If documents are to be signed by electronic signature, the system must also satisfy the basic requirements for the integrated use of digital signatures in Noark.

In connection with the development of new systems or functionality for recordkeeping and archiving, the development must be based on Noark 5, not Noark 4. For task systems and other systems where there is a need to establish defined, pure recordkeeping and archive functionality, the core requirements in Noark 5 must be fulfilled. In cases where a Noark 5 supplier wishes to "loosen" the system in relation to the requirements imposed in Noark 4, the new system/version of the system must at least satisfy the core requirements in Noark 5.

All recordkeeping and archive systems used within the public administration must therefore satisfy the Noark requirements in principle and be approved by the Director General of the National Archival Services. All Noark 5-based solutions must therefore be approved by the Director General of the National Archival Services before they can be brought into use. This also covers ordinary "off-the-shelf" solutions:

- Recordkeeping and archive functionality in task systems, where the public body itself develops the solution.
- Recordkeeping and archive functionality for task systems, where the recordkeeping and archive functionality is developed as an "off-the-shelf" product.
- Recordkeeping and archive functionality that is defined as a common component for one or more public bodies or one or more systems.
- Noark 4 systems that are "remoulded" into Noark 5 systems, as the extraction for transfer format has been altered considerably in Noark 5 compared with Noark 4.

The public administration will not be required to switch from Noark 4-based to Noark 5-based systems from a particular date. The Director General of the National Archival Services' view is that public bodies must choose the tools for recordkeeping and archiving which, within the framework of the Archives Act, are most appropriate for the body concerned at any time. Behind this lies the consideration that for certain administrative or case areas it may still be appropriate to use paper-based records and archives, while others will need to use task systems with functionality based on the core requirements in Noark 5.

3.4 Maintenance of Noark 5

The Director General of the National Archival Services will ensure the continual updating and maintenance of Noark 5, in the form of new versions of the standard.

Minor changes in the form of corrections, the harmonisation of requirements that are contradictory, the clarification of text and the reformulation of text which could be misunderstood or interpreted incorrectly will be implemented on an ongoing basis. These intermediate versions will retain the main version number and have consecutive numbering after the main version number. Noark 5 version 1.0 was released on 4 July 2008. Versions during the autumn of 2008 with corrections, etc. will have the version number 1.1, 1.2, 1.3, etc.

Major changes where additions have been made to the requirements or texts have been heavily reworked will be published with new main version numbers. This will for example take place through the completion of (sections of) requirements that are incomplete in the current version and the introduction of new laws or regulations which must be reflected in Noark 5.

New main versions will be released at fixed times: before the end of the first and third quarters every year.

3.5 Noark 5: Applicable for both the private and public sectors

MoReq2 is a general standard for electronic records management. This is intended to cover both large and small organisations, the public and private sectors, all EU Member States (and countries outside the EU). This means that MoReq is extremely general. It does not contain requirements linked to functions in order to satisfy laws and regulations (not even for the EU), take account of country-specific administrative practices or traditions or other country-specific considerations. The standard is also only in English. Within the EU, emphasis is placed on each country translating MoReq2 into its own language and preparing a "Chapter 0", which contains the country-specific requirements. The requirements in "Chapter 0" must not contradict the other requirements in MoReq2.

MoReq2 will not become an EU Directive. It will continue to be a recommendation and each EU Member State must decide whether, and if so how, MoReq2 will be implemented in the country concerned.

In Norway, the Director General of the National Archival Services has decided that replacing the Noark standard with MoReq2 would not be appropriate. However, it has been a goal to bring Noark 5 as close to MoReq2 as possible. In a number of areas, MoReq2 is more advanced than Noark and contains many requirements with no equivalent in Noark 5. However, the fundamental requirements are largely common, as is the record structure and many of the metadata. It has been a goal for the project that Noark 5 should not contain requirements that are incompatible with MoReq2.

Noark 5 should be considered the official Norwegian version of MoReq2. The Noark 5 core is a technical and functional implementation of the general requirements for appropriate archiving, as they are formulated in MoReq2, ISO 15489 and elsewhere. This ensures that authenticity and integrity are maintained over time. Solutions that are based on Noark 5 core will ensure appropriate archiving regardless of the rules that apply to this archiving. Solutions based on Noark 5 core should therefore also be able to serve as electronic records management solutions for the private sector in Norway.

Solutions that are based only on ISO 15489 and MoReq will not be accepted as Noark 5-compatible. The archive legislation contains provisions which require an administrative body that is to introduce solutions for electronic document management (and archiving) to use Noark-based systems which have been approved by the Director General of the National Archival Services. This applies regardless of whether a pure recordkeeping and archive system is used, or whether functions for archiving are integrated in a case handling system or similar. In connection with the electronic archiving of case documents, the system must meet the specific requirements for electronic archiving in the Noark standard and be approved for this purpose by the Director General of the National Archival Services.

3.6 Recordkeeping as part of added value

Bringing order to document management and recordkeeping within an organisation is increasingly being seen as a necessity in order to improve efficiency and increase added value within the organisation. In an electronic environment, systematic and controlled records

management may be even more difficult than in a paper-based system, as it can be impossible to know whether a document has been altered or which of all the versions that have been created is the "original". Alternatively, the document may simply be deleted or impossible to recreate.

To ensure that the document is authentic and has its integrity maintained, it is a requirement that authenticated metadata is linked to the document. That a document is *authentic* means that the document is what it claims to be, e.g. by the fact that the identities of the parties in an electronic communication are correct. That the *integrity* of the document is maintained means that data has not been altered or destroyed in an unauthorised manner or erroneously; it is therefore a property associated with data which makes it possible to detect whether data has been altered in an unauthorised manner or erroneously.
Authenticated metadata means metadata which is intended to support the document's authenticity and credibility, partly by giving the recipient information which can be utilised in connection with checks on the document's content and sender.

It is important to be aware that recordkeeping and document management are organised differently. MoReq defines the differences as follows:

Solutions for document management	**Solutions for recordkeeping**
Allows documents to be altered and/or stored in several versions without there being any control over which version is the final version.	Prevents fonds documents from being altered and has version control.
Can allow the documents to be deleted by the document owner.	Prevents documents from being deleted without them being subject to controlled, authorised disposal.
May contain some control over how long a document should be retained for and whether it can be deleted.	Rigorous retention control, i.e. the solutions must have functions to manage the preservation, migration and disposal of fonds documents in accordance with established plans.
May contain structured document storage, which can be user-controlled.	Must contain a rigorous record structure with a classification system, which is maintained by an authorised administrator.
Performs the primary function of supporting the daily production and the use of documents in ongoing case handling.	Supports the daily use of documents in ongoing case handling, but must also be a secure and credible archive for fonds documents.

Solutions for document management can therefore give no guarantee in the future that a document can still be retrieved or that it is readable or that the document that you do retrieve has not been altered. Solutions that have been developed specifically for recordkeeping, as the Noark standard facilitates, will ensure that the document can be retrieved, that it is readable and that it is authentic and has had its integrity maintained.

Part II: Noark 5 Inner and Outer core

In the longer term, the system architecture within government bodies will also tend towards a more service-oriented architecture. This is a stated goal of the Ministry of Government Administration and Reform (FAD). The subdivision of Noark 5 into a structure where inner core functionality is specified in order to ensure good archive management, with "optional" systems outside this – integrated, in order to meet the special task-related needs of the individual organisation is a step towards this goal.

4 Introduction to the Inner and Outer cores

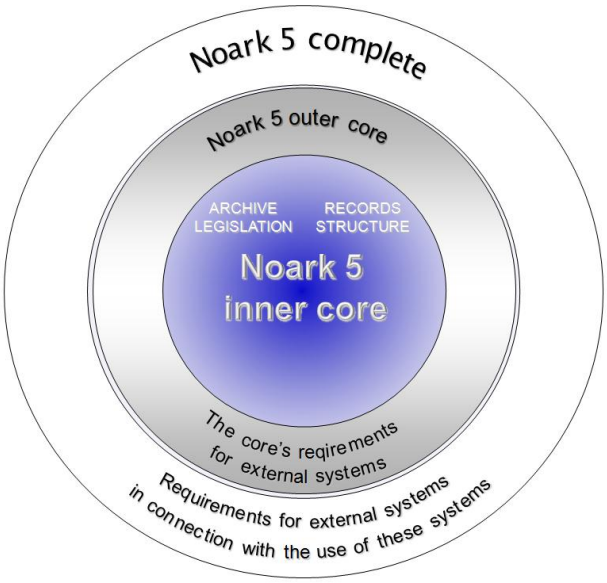
Documentation of the requirement structure in Noark 5 provides an introduction to this chapter, Here, the term core is explained and the content of the various layers is defined.

4.1 Noark 5 core and Noark 5 complete

The specification of requirements in Noark 5 is arranged in three layers or levels. Noark 5 inner and outer core and Noark 5 complete.

Noark 5 inner core

The starting point for the definition of requirements for the inner layer of the core is the i1dentification and definition of the fundamental functions which must be present in order for the core to act as an independent "service" in an archive system environment. Within its domain - archiving - the core must be capable of functioning independently and without any dependency on external functions, programs or similar in order to perform its defined part of the job.



Noark 5 outer core

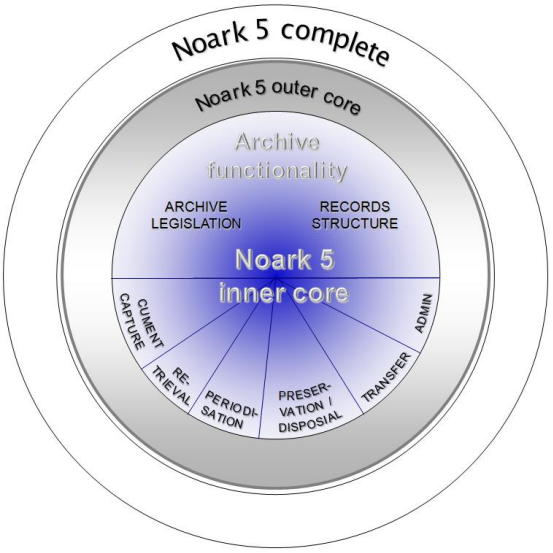
In order for the inner core to function in an archive system environment, a number of requirements must be imposed concerning the functionality of "external" modules. These are requirements formulated on the basis of the archive core's needs and can be defined as the outer layer of the core itself - the core's requirements with respect to external systems. Both the inner and the outer "layer" of requirements in the core must be fulfilled in order for a system to be approved as a Noark 5-based archive system. Certain requirements only need be fulfilled under certain conditions, e.g. that it contains case documents.

Noark 5 complete

The third "layer" of requirements consists of requirements that Noark 5 has concerning freestanding modules or systems which constitute a complete case, recordkeeping and archive solution in a given user environment. These are task systems and pre-systems which each organisation has a need to use and which can be supplied by different suppliers. Together with Noark 5 core (inner and outer), this constitutes Noark 5 complete. Noark 5's requirements for external systems or modules have been organised into separate (independent) sections.

4.1.1 Requirements for modules in Noark 5 inner core

This section presents an overview of the modules that make up the "inner" core in a Noark 5 system.



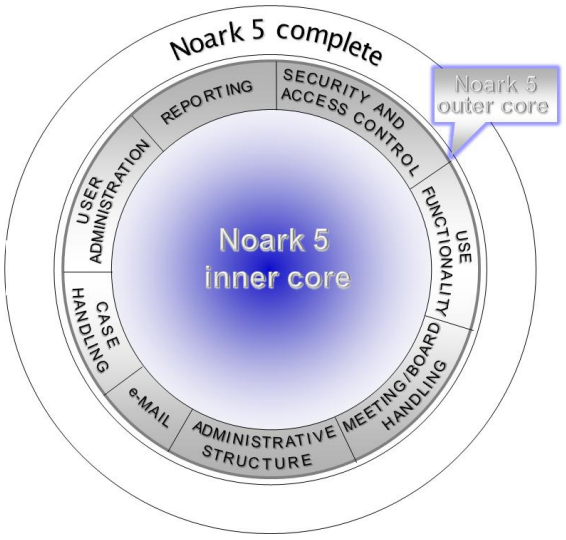
The requirements in the inner core of Noark 5 consist of the fundamental archive functionality, requirements based on the laws and regulations for appropriate archiving, plus a number of important function areas for operation and administration of the core. The outline diagram show the modules in Noark 5's inner core.

The archive area itself, subdivided into record structure and archive regulations, contains the basic requirements for archiving. In addition, the inner core must contain the modules Document capture, Retrieval, Preservation and disposal, Periodisation, Transfer and Administration of the core.

4.1.2 Requirements for modules in Noark 5 outer core

The outer core covers requirements for external (optional) systems. Noark 5's core is dependent on working together with various pre-systems implemented according to the individual organisation or supplier's needs.

In order for Noark 5 to function in a holistic archive system environment, it must be possible to integrate Noark 5 with the pre-systems/task systems which must be implemented in order to supplement a recordkeeping and archive solution.



The core's outer section (the so-called "grey zone") contains Noark 5's requirements for these external, optional systems and/or modules based in the laws and regulations relating to the archive field.

These are systems or modules which are considered to be free solutions in relation to the core. This means that suppliers and customers (users) of Noark 5 can freely select system solutions and integrate them with the Noark 5 core provided that the solutions concerned satisfy the requirements imposed by the core for such a solution.

> *Example of understanding of the figure:*
> *It is not intended that the system for "Security and access control" for example must be a separate module in the Noark 5 core, but the Noark 5 core has a number of specific requirements for security and access control which the external system solution for this area must fulfil.*

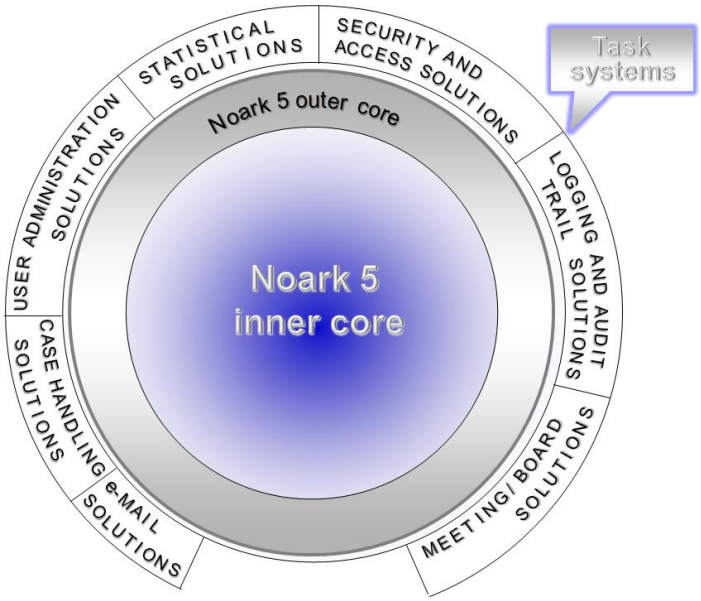
This section therefore sets out guidelines and requirements for the various task systems or pre-systems which can be freestanding systems in relation to Noark 5. However, these requirements must be considered to constitute part of the Noark 5 core requirements and must be fulfilled in order for a system solution to be approved as a Noark 5 solution.

4.1.3 Noark 5 complete

Within the public administration, needs and requirements for task systems can vary widely from body to body. Noark 5 complete contains requirements for functions, content and the use of external system solutions which are naturally used integrated with Noark 5 core functionality. This will concern independent task systems/subject modules which a body can freely choose to introduce from different suppliers. It must be up to the individual body to decide how strictly it wishes to impose these requirements in relation to the system supplier concerned.

Requirements described in Noark 5 complete are requirements which are based more on good practice (compared with recordkeeping and archiving), and routine- and process-based requirements for the task system concerned than on requirements based on specific archive-related laws and regulations.

The following sections contain requirements for the use of external optional functions which naturally form part of a complete Noark 5 archive solution.

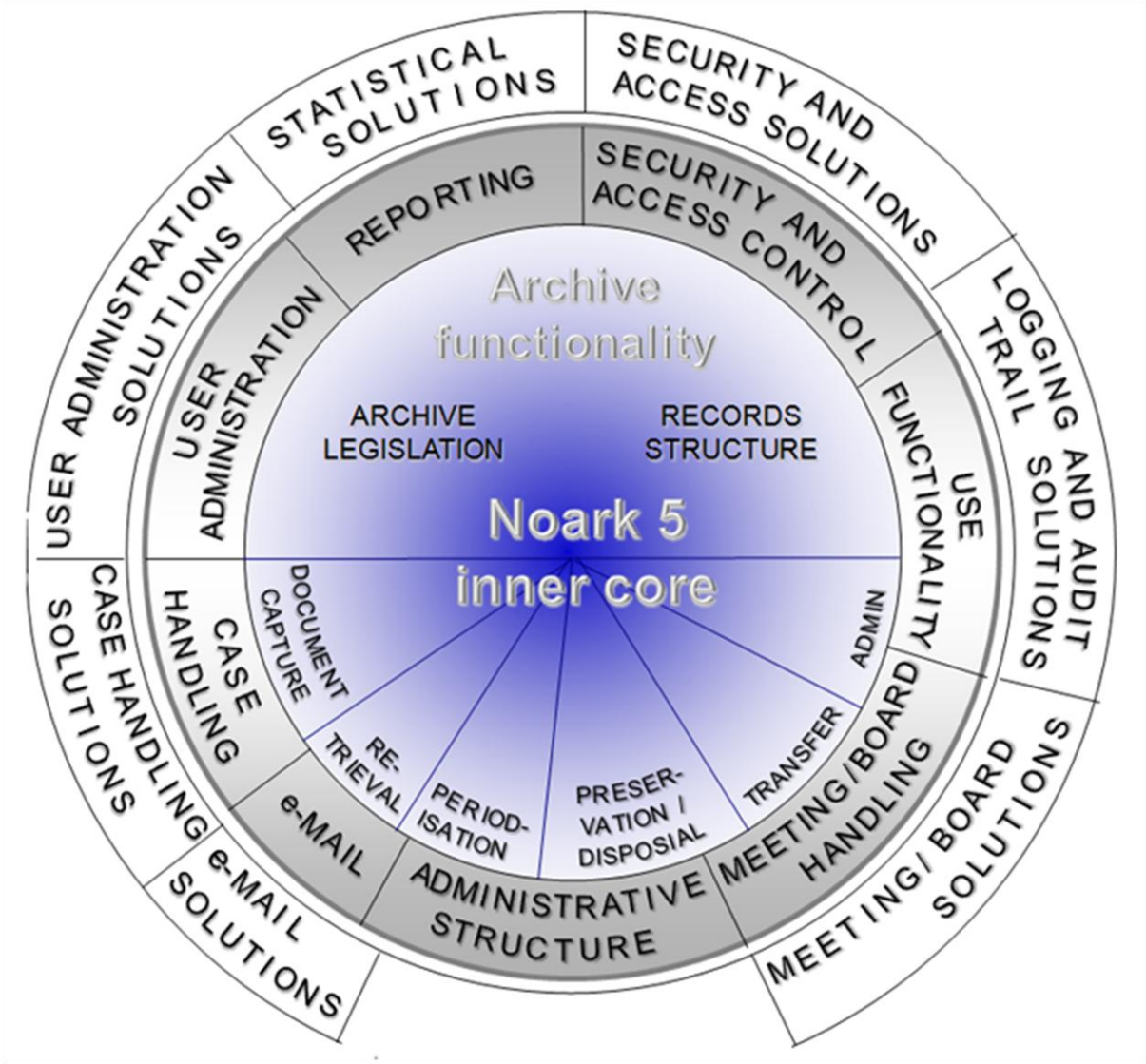


The systems/modules covered by the requirements which form part of Noark 5 complete comprise systems for:

- case handling
- e-mail
- meeting and board handling
- logging and audit trails
- security and access
- statistics and reporting
- user administration

These are expanded requirements in relation to Noark 5 inner and outer core and will act more as guidelines than requirements which shall/must be fulfilled in order to achieve Noark 5 status for the system solution.

The overall picture of Noark 5 complete can be illustrated as shown in this outline diagram.



4.2 The record structure

We can call the record structure the inner arrangement of the archive. This structure is largely hierarchical with several levels from top to bottom. The term *record unit* is used as a common designation of the main classes in these levels.

In a physical archive, the archive structure will largely be reflected in the paper documents' sorting and physical arrangement in folders, files, archive boxes, cabinets, etc. In an electronic archive, the documents can also be presented as if they were in files and a hierarchical archive structure can be represented through files being placed in other files at several levels.

In an electronic archive, the files do not of course exist as physical units. The archive structure in an electronic archive is only built up from various metadata. Each unit in the structure has its own particular metadata, and the various levels are also linked by metadata. Metadata is

aggregated at several levels, so that metadata at the top level will be linked to all documents in the archive, while metadata at the lowest level will only be linked to an individual document.

Electronic and physical archive

It is becoming increasingly common for archives to consist of electronic documents. However, many organisations still keep parts of their archive on paper. Noark 5 focuses on electronic archiving, but can also be used for physical archiving and for a mixture of electronic and physical archiving.

Many metadata are relevant to both electronic and physical archives, but there are also metadata which only concern one type of archiving.

Different types of archive

Traditionally, archives from general case handling – case records – which came under the registry's area of responsibility and therefore received most attention in connection with the formulation of regulations and standards. Noark 4 was only aimed at this type of archive.

An important difference between Noark 4 and Noark 5 is that the standard can now cover most types of archive. If the inner core is integrated with a *task system*, this will in many cases not be necessary to have full case record functionality. In some cases, it may also make integration difficult. Typical of many task systems is specialised case handling, where a few activities are repeated according to fixed routines. The number of documents that are received and generated in such task systems can often be extremely high. In such cases, there may be a need for a simpler archive structure and fewer metadata than is appropriate for case records.

4.3 Metadata

Metadata is information which describes the documents in the archive, both physical and electronic documents. The documents is first and foremost assigned metadata during document capture. Some of this will take place manually, but much also takes place automatically. In certain task systems, almost all metadata capture will be automated. Some metadata will be frozen as soon as it is registered, and after the documents have finally been archived, most metadata will only be alterable by specially authorised users.

Metadata has a number of important functions. Metadata bind the document to the context in which it was created. Metadata ensure the electronic documents' authenticity and therefore their value as evidence. Without metadata, documents will not be *fonds documents* – or *records.* Another important function for metadata is to act as a means of retrieval. Metadata can also control access to the documents and screen other metadata which are not publicly available (e.g. national identification numbers). Metadata can also control preservation and disposal, i.e. the controlled deletion of all documents that have a limited retention period.

Metadata for archives can be subdivided into different categories. An example of such a subdivision is presented below:

1. Unique identifiers
2. Information on who archived ("captured") the document and assigned ("registered") metadata, and when this took place.

3. Metadata concerning *structure*, i.e. information on the document's form and on the document's link to other documents and to the various levels in the archive structure.
4. Metadata concerning *context*, i.e. which function, process and activity created the document, which people and organisations were involved in this activity, the dates on which the document was generated, sent, received, etc.
5. Metadata on *content*, e.g. titles and descriptions.
6. Metadata for retrieval, including keywords and index terms.
7. Place of storage and format of physical documents.
8. Archive responsibility if a system is shared by several organisations.
9. Access rights and screening of information.
10. Preservation and disposal provisions.

Metadata in Noark 5

In Noark 5, metadata are defined for all levels in the archive structure. These metadata are specified in more detail in a separate appendix, as a *metadata directory.* Many of the same metadata will occur at different levels in the archive structure, but will only be specified once in the directory.

Metadata in Noark 5 cannot be compared with the attribute lists in Noark 4. The basis for the definition of metadata was the requirement as to what must be included in a transfer export. However, consideration has also been given to metadata which can be exchanged electronically together with documents, metadata which can be shared in connection with integration with task systems, and metadata which can be migrated to other systems together with associated documents.

Metadata will be named in an unambiguous way, which is explained in more detail in the metadata directory. The metadata names are mandatory in connection with the export and exchange of data, i.e. in XML format.

All metadata do not need to be stored as attributes (fields) in the database either. In some cases, metadata will only be generated when data is exported or exchanged.

Metadata can be *inherited* by a subordinate unit from a superior unit.

There is no requirement for all metadata in the directory to necessarily be stored in the inner core. In some solutions, it is more appropriate to store some of the metadata in the task system. However, it is a requirement that when exporting or exchanging, all mandatory metadata are included in a common structure. Such structures will be described in the form of an XML form in Noark 5.

In the ongoing text, the metadata elements are grouped into objects, which can for example correspond to a record unit (a level in the archive structure). A fixed form is used for this:

No.	Name	Type	Occ.	Trans.	Remarks

No.: Refers to the unique number in the metadata directory (separate appendix).
Name: Name to be used in connection with transfer and where applicable other export.
Type: Here, the same code types as in the Noark 5 requirements are used:
O (obligatory), must always contain a value.
B (conditional obligatory), must contain a value when certain conditions are met.
V (optional), does not need to contain a value.
Occ.: Occurrence, i.e. how many times the metadata element can be repeated within the same object. Values: **One** and **Many**.
Trans.: Code **A** indicates that the metadata element should be included in a transfer if it contains a value. **Blank field** means that, although it does not have to be transferred, it has still been included because it may be appropriate to export it in other contexts.
Remarks: Specifies any remarks, e.g. conditions when the metadata element must have a value.

The number of occurrences is therefore dependent on the type, as shown in the following table:

	Obligatory	**Conditional**	**Optional**
One	1	0..1	0..1
Many	1..N	0..N	0..N

The metadata elements will also be repeated in the appendix "Metadata grouped according to object".

4.4 Relationship to Noark 4 and MoReq2

Noark 5 will be backwards-compatible with Noark 4 in the sense that it will be possible to migrate archives from systems based on the older standard to the new one. This has been taken into consideration as regards both the construction of the archive structure and the metadata that are defined. An example of this is that the units *fonds* and *series* are still retained in the archive structure.

Bringing Noark 5 as close as possible to MoReq2 has also been a goal. MoReq2 is more advanced than Noark in a number of areas and contains many requirements with no equivalent in Noark 5. However, the fundamental requirements are largely common, as is the archive structure and many of the metadata.

5 Noark 5 inner core

The inner core will handle the organisation's *archive*, i.e. the *fonds documents* that are received or produced as a result of the activities carried on by the organisation.

Fonds documents come into the archive, i.e. they are archived, through *document capture.* The documents must be organised in a *record structure* which shows the link between the documents. This means that documents must be placed in the correct place in the archive. When documents are archived, they must be frozen for all further editing.

Document capture also involves the documents being assigned *metadata*, i.e. information on the documents' *content, context* and *structure.* An important function of metadata is to maintain trust in the documents' *authenticity* over time. There must be no doubt that a document is genuine and that it was created by the person who claims to have created it.

It must be possible for the archive structure to be *administered* by those who have the necessary rights. It must for example be possible to move documents that have been incorrectly archived.

It must be possible for documents that have been archived to be *retrieved* quickly and securely, and it must be possible for both the documents and their context to be presented to users in a clear manner.

The inner core must also contain functions for *preservation and disposal.* Organisations are neither required nor permitted to retain all their fonds documents for the same length of time, and it must therefore be possible to add rules for when such documents must be removed from the archive.

The archival authorities will also take decisions concerning the retention of particular fonds documents by public bodies without any time restriction. It must be possible to *transfer* these documents to an archival repository.

5.1 The archive structure

This section contains a description of an overall model for the archive structure in Noark 5.

The section is subdivided below according to the structure model, i.e. for every level in the structure, an associated section is created which documents the structure level with a separate sub-model and the requirements for this sub-model.

In addition, metadata for functionality that applies to all levels in the model will be described in separate subsections.

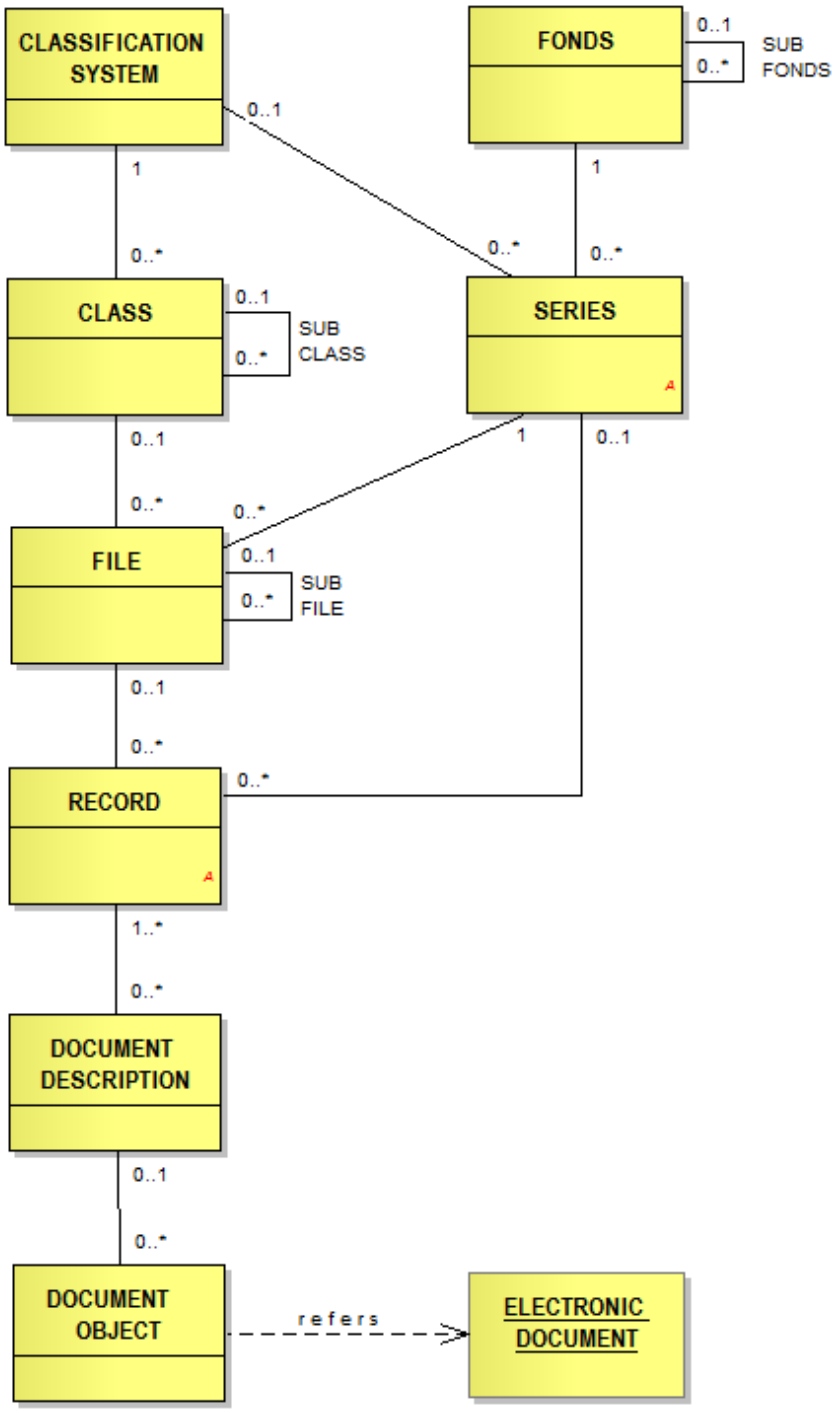
Main model for the archive structure

The models in Noark 5 are *conceptual models* which are intended to show the link between different metadata, and between metadata and physical or electronic documents. The conceptual models in Noark 5 state something about how the information should be organised

in principle. They will also form the basis for the definition of data structures in connection with electronic communication, integration with other systems, migration from one system to another and for transfer.

Overall sketch[2] of the conceptual model for Noark 5:

[2] *Note: Under the description of the conceptual model for each level (subsection), the main classes in the level will be indicated by a yellow colour. Key associated classes will be shown in grey. These are documented under their respective levels (subsections).*



The levels for FILE and RECORD have been built up with the aid of specialisation of the classes.
The archive structure outlined through the conceptual model in this section represents the main structure in Noark 5 and is obligatory for case records.

Simplified structure

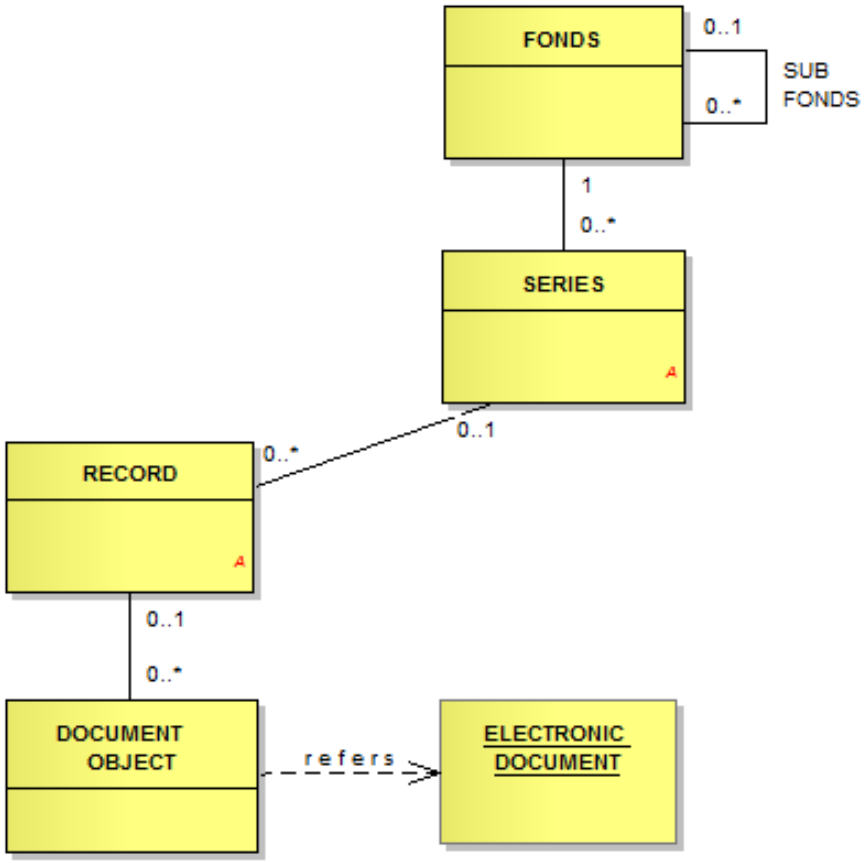
In some task systems, there may be a need for a simplified structure in relation to case records. If there is no need to group records into files in a task system (e.g. a drawing archive), the file level can be omitted. Similarly, the document description level can be omitted if a record always consists only of a single document and if this document will not occur in other records.

The sequence of documents in a classification system is also not obligatory for task systems. If the classification system is included, it must nevertheless be possible to omit the file level. This means therefore that records can be directly linked to a class.

It is stressed that such a simplified structure will only be of relevance to a few task systems. It must not be interpreted as indicating that classification systems, files and document descriptions can be omitted from functions that are aimed at case records. Many task systems, i.e. task systems which contain correspondence, will also require the same complete record structure as case records.

If you look at the structure of the record structure in the various conceptual models for each level in the record structure, you will see that there is a simplified structure built-in through the use of constraints such as “either/or”. This gives an opportunity to establish an archive without having to use the levels for File and/or Document description.

A simplified version of the conceptual model could look like this:



<FORENKLET STRUKTUR NOARK 5>

The definitions of the individual levels/archive elements can be found in the respective sections for the archive level.

Req. no.	General requirements for the archive structure	Type	Remarks
5.1.1	In order for a system to be approved in accordance with the Noark 5 standard, it must be possible to implement the conceptual model of the archive structure and the functional opportunities in the relevant system's (physical) data structures.	O	

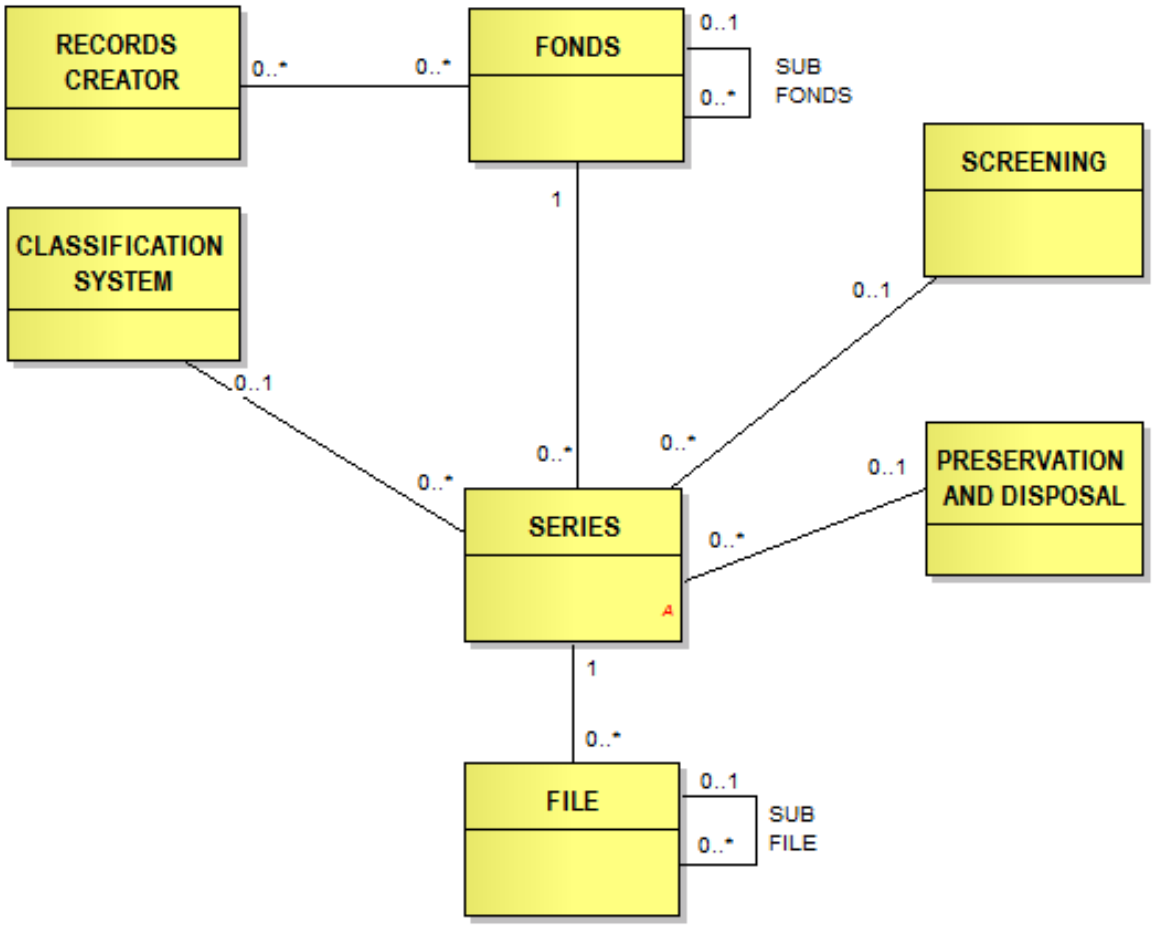
Req. no.	General requirements for the archive structure	Type	Remarks
5.1.2	Fonds documents that belong to a case record must form part of an archive structure which must contain the following record units: *Fonds*, *Series*, *Classification system*, *Class*, *File* [1)], *Record*[2)], *Document description* and *Document object*. [1)] *File* is a common term for the record units Basic file, including the specialisations Case file and Meeting file. [2)] *Record* is a collective term for the record units Simplified record, including the specialisations Basic record, Registry entry and Meeting record.	B	Obligatory for case records.
5.1.3	Fonds documents that do not belong to a case record (e.g. a task system) can be included in a "simplified" archive structure which must at least contain the following record units: *Fonds*, *Series*, *Record*[1)] *and Document object*. [1)] *Record* is a collective term for the record units Simplified record, including the specialisations Basic record, Registry entry and Meeting record.	O	Replaced by requirement 0 for case records. This is a minimum solution. Task systems can consist of the same record units as case records.
5.1.4	Noark 5 must have services/functions for *storing, retrieving, altering and deleting data and selections*[1)] *of data* in accordance with the metadata descriptions in all *record units* (see requirement 0) and associated classes which are documented in the conceptual models and metadata tables in Noark 5. *Note:* Individual functional requirements in the various sections may override this requirement. [1)]*Selections of data* means selections within a from/to designation of obligatory metadata for the record unit concerned.	O	This is a general requirement, which covers a lot of functionality in Noark 5 core.
5.1.5	It must be possible to identify a record unit (see requirements 0 and 0) uniquely.	O	In connection with transfer, a unique ID for all record units must be called systemID.

5.2 Fonds and Series

This section concerns requirements for fonds and series. It is subdivided into three underlying sections: Fonds, Subfonds and Series.

Different organisations will have different needs here. MoReq2 does not contain anything which corresponds to record and series; in it, the classification system handles all grouping of documents at the uppermost levels. However, in Noark 5 both record and series are obligatory. This is because of the consideration concerning backwards compatibility with Noark 4 and the fact that important functionality is linked to series.

Conceptual model for *Fonds* and *Series*



<Conceptual model Record/Series>

In certain cases, there is a need for an additional level between record and series. It is particularly important to be able to subdivide fonds into a number of (physical) sections for physical fonds within the municipal sector. This is overcome by introducing so-called "subfonds" into the conceptual model. A subrecord is a hierarchical structure within the fonds and can therefore be defined at a number of levels. In practice, there will normally be one level.

Fonds

Fonds consist of documents that are created as part of an activity, i.e. documents that are received or produced by an individual fonds creator and collated as a result of this person's work. A Noark solution can cover one or more fonds entities.

Series

An arbitrarily defined section of a fonds entity in which all material is subdivided and arranged according to a single primary classification system. A fonds section will often be defined identically to a record series, but need not necessarily be defined in this way.

Fonds creator

An organisational unit or person who creates fonds as part of his or her work. A fonds creator may be a public body, a company, an organisation, a foundation, etc. or a part of such a unit. A public agency may be one fonds creator and thus have one fonds entity (central registry), or it could have several fonds creators (departments, services, etc.), each of which create their own fonds entities (partial fonds).

Screening

Screening is used to screen registered information or individual documents. The screening takes effect when an access code is applied to the individual file, record or individual document. (See separate section: *6.6.1 Screening*
)

Preservation and disposal

Codes which indicate decisions concerning disposal. Disposal decisions determine which fonds are to be removed from the archive and destroyed. (See separate section: *5.10 Retention and disposal*
)

Classification system

(See separate section: *0 Remarks: Requirements for.*
)

5.2.1 Fonds

Fonds

Fonds form the highest level of the records structure. Most users will only need to create one fonds entity in their Noark 5 solution. However, it must be possible to create several fonds entities. This may be appropriate if several bodies share the same solution. This may be appropriate if several bodies share the same solution. Here, a head office and several regional offices could each be set up with their own fonds entity. However, in the case of electronic recordkeeping, there is also nothing to prevent the entire service from sharing the same fonds entity.

Fonds creator

Traditionally, a fonds entity has been defined according to *organisation*. An organisation creates a fonds entity, i.e. the organisation is the fonds creator. However, electronic information technology has resulted in it becoming increasingly common for several fonds

creators to create one fonds entity. The fonds entity will then be defined according to *function*, not organisation[3].

In a Noark 5 solution, it must therefore be possible to link one or more fonds creators to a fonds entity. Information on fonds creators is obligatory in transfer exports.

Metadata for *Fonds*

No.	Name	Type	Occ.	Trans.	Remarks
M001	systemID	O	One	A	
M020	title	O	One	A	
M021	description	V	One	A	
M050	fonds status	B	One	A	Obligatory for case records.
M300	documentmedium	V	One	A	
M301	storagelocation	V	Many		For physical fonds.
M600	createdDate	O	One	A	
M601	createdBy	O	One	A	
M602	finalisedDate	B	One	A	Obligatory when the fonds have been finalised.
M603	finalisedBy	B	One	A	Obligatory when the fonds have been finalised.
M200	referenceParent	B	One	A	Obligatory for subfonds.
M201	referenceChild	O	Many	A	Reference to series or possibly subfonds. In connection with transfer, there will only be a reference to one fonds section.

Metadata for *Fonds creator*

Fonds creator is obligatory, and may occur once or many times in a Fonds entity.

No.	Name	Type	Occ.	Trans.	Remarks
M006	fondscreatorID	O	One	A	

[3] Example: The immigration administration (which is a function) could constitute a records entity where the organisations – the Directorate of Immigration, the Immigration Appeals Board, the Directorate of Integration and Diversity, the embassies and consulates and the police - are collectively records creators.

No.	Name	Type	Occ.	Trans.	Remarks
M023	fondscreatorName	O	One	A	
M021	description	V	One	A	

Requirements for *Fonds*

Req. no.	Structural requirements for *Fonds*	Type	Remarks
5.2.1	It must be possible for a Noark 5 solution to consist of one or more independent *Fonds.*	O	
5.2.2	It must be possible to create no, one or more *Fonds* for a *Fonds creator* (activity) and it must be possible to specify that several fonds creators together create a *Fonds entity.*	O	
5.2.3	A *Fonds entity* must consist of one or more fonds sections and a *Fonds section* must form part of (only) one *Fonds entity.*	O	

Req. no.	Functional requirements for *Fonds*	Type	Remarks
5.2.4	If a *Fonds entity* is registered as "Finalised", it must not be possible to add more underlying *Fonds sections.*	B	Obligatory if fonds status is used.
5.2.5	When a service/function deletes an entire *Fonds entity* with all underlying levels, this must be logged.	O	
5.2.6	It must not be possible to alter the date of creation of the *Fonds entity.*	O	
5.2.7	It must not be possible to delete the date of creation of the *Fonds entity.*	O	
5.2.8	It must not be possible to delete the date of closure of the *Fonds entity.*	O	
5.2.9	It must be possible to define status values for *Fonds entities.* The following values are recommended: • Created • Finalised	B	Obligatory for case fonds.

5.2.2 Subfonds

In the case of physical recordkeeping, an organisation may have placed the documents in several different places, e.g. linked to the departments that create the documents. This may be the case for larger organisations with many different functions, e.g. municipal authorities. In a

Noark 5 solution, it should therefore be possible to subdivide the fonds into subfonds, if the users need such a subdivision[4].

In the case of electronic recordkeeping, there is little need for subfonds.

Subfonds occur in the conceptual model as a self-relation to Record. This means that Fonds can be built up in a hierarchy. In most cases, this will concern one level which lies between Fonds and Series. Subfonds are not obligatory in the fonds structure.

Metadata for *Subfonds*

See "Metadata for *Fonds".*

Requirements for *Subfonds*

Req. no.	Structural requirements for *Subfonds*	Type	Remarks
5.2.10	It should be possible for a *Fonds entity* to be subdivided into a hierarchy (outlined in the model by using a self-relation) of *Subfonds.* Remarks: Using one or more levels under *Fonds entity*, it should be possible to represent physical subfonds for example. This may be relevant for organisations that have fonds physically located in several different places.	V	

Req. no.	Functional requirements for *Subfonds*	Type	Remarks
5.2.11	The system should have a service/function for specifying a *Fonds entity* as a *Subrecord* of a *Fonds entity.*	V	
5.2.12	A *Subrecord* must only be created and altered through the Administration system for Noark 5.	B	Obligatory if subfonds are used.

5.2.3 Series

It must be possible to subdivide a fonds entity into series in order to group the records according to overall criteria. The most important criteria for subdividing into series are:

- Distinguish between active records entities and closed records periods. Important functions in connection with periodisation and production of transfer exports are linked to this.
- Distinguish between files (cases if the files are case files) that are to be periodised according to different principles. Many organisations wish for example to retain personnel files in an active records entity for as long as a person is an employee of the organisation.

[4] Traditionally, these have been called *subrecords.* Because this term could easily be confused with series, it is not used in Noark 5.

- Distinguish between cases that are classified according to different principles. This is most relevant in connection with physical recordkeeping, in which case files and personnel files for example are stored in difference places. In the case of electronic archiving, subdivision into different classification systems will meet this need.
- Distinguish between electronic records and physical records. The general rule is that entire files must be either physical or electronic. However, dispensation from this rule can be given, so that some records can be physical and others electronic in the same file. If a large appendix (e.g. a printed document) is not scanned, physical documents can also occur together with electronic documents in the same record (registry entry).
- Distinguish between the case records and other types of records, e.g. records linked to task systems. Some organisations will need to distinguish clearly between administrative cases and task cases. There will also be a need to separate out meeting documents.
- Distinguish between document types that are to be preserved and documents that are to be disposed of.

Metadata for *Series*

No.	Name	Type	Occ.	Trans.	Remarks
M001	systemID	O	One	A	
M020	title	O	One	A	
M021	description	V	One	A	
M051	recordssectionstatus	B	One	A	Obligatory for case records.
M300	documentmedium	B	One	A	Obligatory for mixed physical and electronic records.
M301	storagelocation	V	Many		For physical records.
M600	createdDate	O	One	A	
M601	createdBy	O	One	A	
M602	finalisedDate	B	One	A	Obligatory when the series has been finalised.
M603	finalisedBy	B	One	A	Obligatory when the series has been finalised.
M107	recordsperiodStartDate	B	One	A	Obligatory for case records. Must be assigned a value when a records period starts.
M108	recordsperiodEndDate	B	One	A	Obligatory for case records. Must be assigned a value when a records period ends.

No.	Name	Type	Occ.	Trans.	Remarks
M200	referenceParent	O	One	A	Reference to records.
M202	referencePrecursor	B	One	A	Obligatory for case records.
M203	referenceSuccessor	B	One	A	Obligatory for case records.
M204	referenceClassificationsystem	B	One	A	Obligatory for case records. Reference to primary classification system.
M205	referenceFile	O	Many	A	Reference to all files in the series. Number of occurrences can therefore be high.
M206	referenceRecord	V	Many	A	See remarks below.

Remarks: Reference to record may be relevant if a series is used to control preservation and disposal decisions for particular record types (document types). The same applies if a series is used to separate paper documents and electronic documents within the same file. In principle, this contradicts the Director General of the National Archival Services' provisions, but it does open up this possibility in exceptional cases. References to record will also occur if the file level is deleted, which could be permissible for certain task systems.

Requirements for *Series*

Req. no.	Structural requirements for *Series*	Type	Remarks
5.2.13	A *Series* can have registered either no or one preferred *Classification system* and a *Classification system* can form part of no, one or several *Series(s).*	B	Obligatory for case records.
5.2.14	A *Series* can have registered no or one *Screening* and a *Screening* can form part of no, one or several *Series(s).*	O	See remarks below.
5.2.15	A *Series* can have registered no or one *Preservation and disposal* and a *Preservation and disposal* can form part of no, one or more *Series(s).*	O	See remarks below.
5.2.16	A *Series* can be linked to (contain) no, one or more *Files.*	O	

Remarks: Metadata for Screening are described in section 6.6.1. Metadata for Preservation and disposal are described in section 5.10. It is essentially an obligatory requirement that all records systems have functions for screening and preservation/disposal. However, this requirement may be omitted for simple systems without such needs.

Req. no.	Functional requirements for *Series*	Type	Remarks
5.2.17	When a service/function deletes a *Series*, this must be logged.	O	
5.2.18	There must be a service/function for updating the primary Classification system for a *Series.* (referenceClassificationsystem)	O	
5.2.19	If *Series* is registered as finalised (finalisedDate is set), it must *not* be possible to add more associated *Files* or *Records.*	O	
5.2.20	A series must contain information on the status of the records period. Authorised users must be able to alter status values. Obligatory values are: 1. Active period 2. Overlap period 3. Closed period Other values can be used when necessary.	B	Obligatory for case records and for all solutions in which periodisation is performed.
5.2.21	A series must contain the date on which the records period starts.	B	Obligatory for case records and for all solutions in which periodisation is performed.
5.2.22	A finalised series must contain the date on which the period was closed.	B	Obligatory for case records and for all solutions in which periodisation is performed. Must be assigned a value when the period is closed.
5.2.23	A series must contain information stating whether the associated documents are physical or electronic.	B	Obligatory for mixed physical and electronic records.

Remarks: Requirements for periodisation are described in section 5.11 Periodisation

.

5.3 Classification system and Class

Classification system

Modern archive theory places an emphasis on the classification system being *function-based.* All organisations perform a certain number of *functions.* These are often stable over time, but functions can be transferred from one organisation to another. An example of such a transfer is when case areas move from one ministry to another, which often happens in connection with a

change of government. An organisation will normally only have a few main functions, but some of these can be subdivided into subfunctions.

Functions are divided into *activities.* Unlike a function, an activity has a beginning and an end. An activity also has participants and leads to a result. If an activity constantly repeats itself, it belongs to a *process.*

Activities can often be divided into different stages. If these stages involve two or more parties, we often talk about a *transaction.* Transactions create archival documents (records).

This hierarchy of functions, subfunctions and activities must be reflected in a function-based classification system. This will generally correspond to what is called a "topic-based" classification. However, it is not really correct to talk about topics here. A topic indicates something about *what an object contains,* while a function indicates something about *why an object was created.*

There are many reasons why a records entity should be organised according to a function-based classification system:

- Documents that have been created as a result of the same activities are linked together. This gives the documents important contextual information.
- It simplifies the retrieval of files and documents.
- It can control access to documents. Certain classes can for example contain documents which must be screened.
- It can be a starting point for preservation and disposal. It is currently generally accepted that disposal decisions should be based on the organisation's functions and activities, and not on the content of the documents (macrodisposal).

The other main type of classification system is *object-based* classification. "The objects" will often be people, but they can also be companies, properties, etc. Unlike function-based classification systems, object-based systems are often flat, i.e. they consist of one level only.

Class

A classification consists of classes. In the case of function-based (topic-based) classification, the classes will normally form part of a hierarchy, in which three or four levels are the norm. In the conceptual model, the sublevels are called "subclasses" and appear as a self-relation in Class[5].

ISO 15489 recommends that the classes describe the organisation's functions and activities (business processes). The uppermost level will then typically describe the main functions. The second level can describe subfunctions, while the third level describes the processes (i.e. activities that are constantly repeated).

The classes must have a separate identification which is unique within the classification system. This corresponds to what is called *order value* or *file code* in Noark 4. Identifications

[5] In the state administration's archive key, the levels below the classes are called main groups, groups and subgroups. In Noark 5, the common term 'subclasses' is used for all sublevels.

from higher classes must be inherited downwards within the hierarchy, so that it is easy to see which level you are at[6].

In the case of object-based classification with just one level, the identification could for example be a national ID number or property or house number.

It must be possible to classify a case file with more than one class, i.e. with one or more *secondary classifications.* This will then enable the use of secondary file codes and multifaceted classification, e.g. the K codes which are used by many municipal authorities. In the conceptual model for File, this is illustrated by a separate class. However, all inheritance of metadata can only be routed through the *primary classification.*

The classes will often be added before a Noark 5 solution is brought into use. However, it must also be possible for authorised users to create new classes. This is particularly relevant in the case of object-based classification. It must also be possible to close classes, so that it is no longer possible to link new files to them.

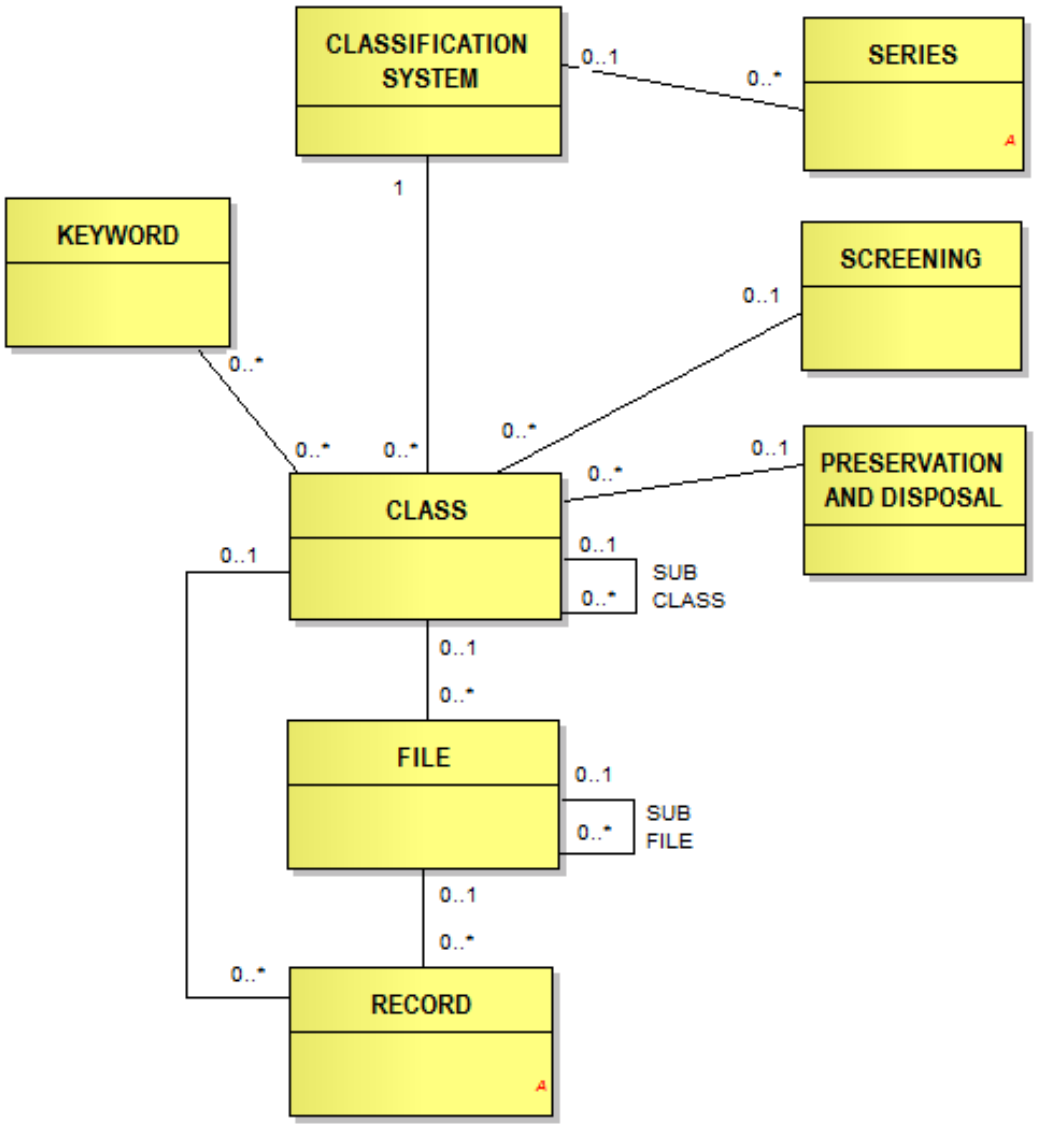
Records without classification

Classification must be obligatory for case records. However, if the inner core is integrated with certain types of task system, it should be possible to create record structures without classes or classification systems. It will then only be records and series which structure the documents at the uppermost levels.

[6] Example of identification and title of classes and subclasses in the state administration's standard key:

First level:	2	Positions and personnel
Second level:	2.3	Salaries and pensions
Third level:	2.3.6	Employer's contributions

Conceptual model for *Classification system*



<Conceptual model for the classification and class system>

Keyword

Keyword or topic word for retrieving documents. A keyword indicates something about *what an object contains.*

Preservation and disposal

Codes which indicate decisions concerning disposal. Disposal decisions determine which records material is to be removed from the archive and destroyed. (See separate section: *5.10 Retention and disposal*
)

Classification system

The classification system describes the structure of files in one or more series.

Class

Table of classes belonging to a classification system. A class will normally consist of a *classID*, which specifies permitted values in the classification system and a *class title*, which is a textual description of the topic.

Screening

Screening is used to screen registered information or individual documents. Screening takes effect when an access code is applied to the individual file, record or individual document. (See separate section: *6.6.1 Screening*
)

Metadata for *Classification system*

No.	Name	Type	Occ.	Trans.	Remarks
M001	systemID	O	One	A	
M086	classification type	V	One	A	
M020	title	O	One	A	
M021	description	V	One	A	
M600	createdDate	O	One	A	
M601	createdBy	O	One	A	
M602	finalisedDate	B	One	A	Obligatory when the classification system has been finalised.
M603	fifufinalisedBy	B	One	A	Obligatory when the classification system has been finalised.
M201	referenceChild	O	Many	A	Reference to the uppermost level with classes.

Remarks: A classification system can be omitted in certain task systems, and the obligatory metadata above will then not exist. In case records, a classification system is obligatory, making the use of classification appropriate in many task systems.

Metadata for *Class*

No.	Name	Type	Occ.	Trans.	Remarks
M001	systemID	O	One	A	

No.	Name	Type	Occ.	Trans.	Remarks
M002	classID	O	One	A	Corresponds to file code or order value in Noark 4. classIDs at subordinate level inherit classID from the superior level.
M020	title	O	One	A	
M021	description	V	One	A	
M023	keyword	V	Many	A	
M600	createdDate	O	One	A	
M601	createdBy	O	One	A	
M602	finalisedDate	B	One	A	If it is possible to close classes in the solution, a value must be assigned when the class is finalised.
M603	finalisedBy	B	One		If it is possible to close classes in the solution, a value must be assigned when the class is finalised.
M200	referenceParent	O	One		Reference to classification system or class at a higher level.
M201	referenceChild	O	Many		Reference to file or to class at a lower level. If the file level is omitted, the reference can also go to record.

Remarks: Class can be omitted in certain task systems, and the obligatory metadata above will then not exist. In case records, class is obligatory, and it will then also be appropriate to use it in many task systems.

Requirements for *Classification system* and *Class*

Req. no.	Structural requirements for *Classification system* and *Class*	Type	Remarks
5.3.1	A *Classification system* can be subdivided into no, one or more *Classes* and a *Class* can belong to just one *Classification system*.	O	

Req. no.	Structural requirements for *Classification system* and *Class*	Type	Remarks
5.3.2	A *Classification system* can form a primary system in no, one or more *Series.*	O	
5.3.3	A *Class* can be included in a hierarchy of *Classes* (outlined in the model via a self-relation).	O	
5.3.4	A *Class* can have registered no or one *Screening* and a *Screening* can be included in no, one or more *Classes.*	O	See remark 1 below.
5.3.5	A *Class* can have registered no or one *Preservation and disposal* and a *Preservation and disposal* can be included in no, one or more *Classes.*	O	See remark 1 below.
5.3.6	A *Class* can have registered no, one or more *Keywords* and it should be possible for a *Keyword* to be included in no, one or more *Classes.*	V	
5.3.7	A *Class* can be subdivided into no, one or more *Files* and a *File* can belong to just one *Class*.	O	See remark 2 below.

Remarks:

1. Metadata for screening are described in section 4.3.7.1. Metadata for preservation and disposal are described in section 4.2.10. It is essentially an obligatory requirement that all records systems have functions for screening and preservation/disposal. However, this requirement may be omitted for simple systems without such needs.

2. A file can have secondary classifications, i.e. be secondarily linked to other classes. Together, these classes can belong to the same classification system as the primary class, but they can also belong to other classification systems. Note that inheritance only takes place from the primary class.

Req. no.	Functional requirements for *Classification system*	Type	Remarks
5.3.8	It should be possible to describe a *Classification system* using different classification types. *Examples of values: "Function-based, hierarchical" "Topic-based, hierarchical archive key", "Topic-based, one level", "K codes", "Multifaceted, not hierarchy", "Object-based," "National ID number", "Property and house number".*	V	Of relevance where there is more than one classification system.
5.3.9	It must be possible to establish hierarchical classification systems. The following is standard: • Common archive key for the state administration	O	
5.3.10	It must be possible to establish faceted, hierarchical classification systems. The following is standard: • The K code key	B	Obligatory for case records in the municipal sector.

Req. no.	Functional requirements for *Classification system*	Type	Remarks
5.3.11	It must be possible to establish one-dimensional classification systems. The following is standard: • Legal person (private individual or business) • Property and house number	O	

Req. no.	Functional requirements for *Class*	Type	Remarks
5.3.12	There must be a service/function for updating a hierarchy of *Classes.*	O	
5.3.13	There must be a service/function for specifying whether a value of *Class* must/must not be used in connection with the classification of cases.	B	For case archives, it must be possible to close (end) classes so that they can no longer be used.
5.3.14	In order for a *Class* to be assigned a *File*, it must be situated at the bottom level in the class hierarchy.	O	A class cannot therefore contain both other classes and files.
5.3.15	If the value in *Class* is registered as finalised (finalisedDate), it must not be possible to assign new *Files* to the *Class.*	B	Obligatory if it is possible to finalise classes.
5.3.16	A log must be kept of when a class was created and who created it. Only authorised personnel can create classes. Other users can be given permission to create classes.	O	Often, all classes will be entered before the system is taken into use. However, permission can be given for classes to be created on an ongoing basis, something which is particularly relevant in the case of object-based classification.
5.3.17	A log must be kept of when a class was finalised and who finalised it. Only authorised personnel can finalise classes.	B	Obligatory if it is possible to finalise classes.

Remarks: The structural and functional requirements above are not relevant to task systems where classification is omitted.

5.4 File

In relation to the main structure, the file level in the model is built up using specialisation. The names of the conceptual classes at this level are therefore defined more according to their area of use.

A file groups documents which belong together in some way. The documents in a file should preferably constitute an instance (i.e. an execution) of an activity, with a defined beginning and end. An example of this is *individual cases* in case records. Such a case could for example concern an issue that is currently under consideration, and the documents in the case will then constitute the handling sequence for this issue. Such cases can typically start with an application or enquiry from an external source and end with a decision.

However, it is occasionally more logical to group documents in a file according to other criteria. In some cases, all documents that concern an object will be placed in one file, e.g. personnel files. Such files are also called *dossier files.* In other cases, it may be appropriate to place all the documents that belong to the same process (i.e. repetition of the same type of activity) in the same file. This will often concern very routine activities, where each activity might create just a single document. In case records, this is known as *file folders* or *file cases.*

The way in which the content of a file is grouped will depend on the classification system. You may not need separate personnel files if the classification system is object-based. If the files are grouped on the basis of objects or processes, the classification system will often be at an overall level. The documents that are created in a particular project can be collated together in a project file (with subfiles). However, it will probably be better to define the project in the classification system and group the files according to instances of activities.

Files must have their own identification which is unique within a particular archive. Noark 5 does not set out any requirements concerning what this code should look like. As regards case files, it is recommended that the same template as used in previous versions of the Noark standard be used, i.e. a combination of the year in which the file was created and a consecutive section number within the year, e.g. 2008/12345.

File types

Noark 5 facilitates the flexible use of files. This is because it must be possible to adapt documents that are received and created in most types of task system in the inner core. In some cases, this must be done in a simpler way than was possible in Noark 4.

A *case* in Noark 4 constitutes a particular file type in Noark 5. If a system based on Noark 5 is only to be used for case records, there is nothing to prevent the term "case" from being used in all interfaces with respect to the users, in the same way as is common in Noark 4. However, in this standard, "file" is the general term for the records unit at this level.
(*Mappe* is also an appropriate Norwegian translation of the corresponding term in NoReq2, which is called *File*).

Basic file

The starting point for all files in Noark 5 is a *basic file.* This contains the minimum fundamental metadata that must be included. However, not all metadata in a basic file are

obligatory. Metadata concerning preservation/disposal and screening belong in the basic file, but will not be obligatory if no decision concerning preservation and disposal has been made, or metadata are not to be screened. A basic file can form the starting point for a file in a task system. Many task systems will probably need extra metadata in addition to the basic file. However, in this version of Noark 5, only the basic file and case file will be specified.

Subfile

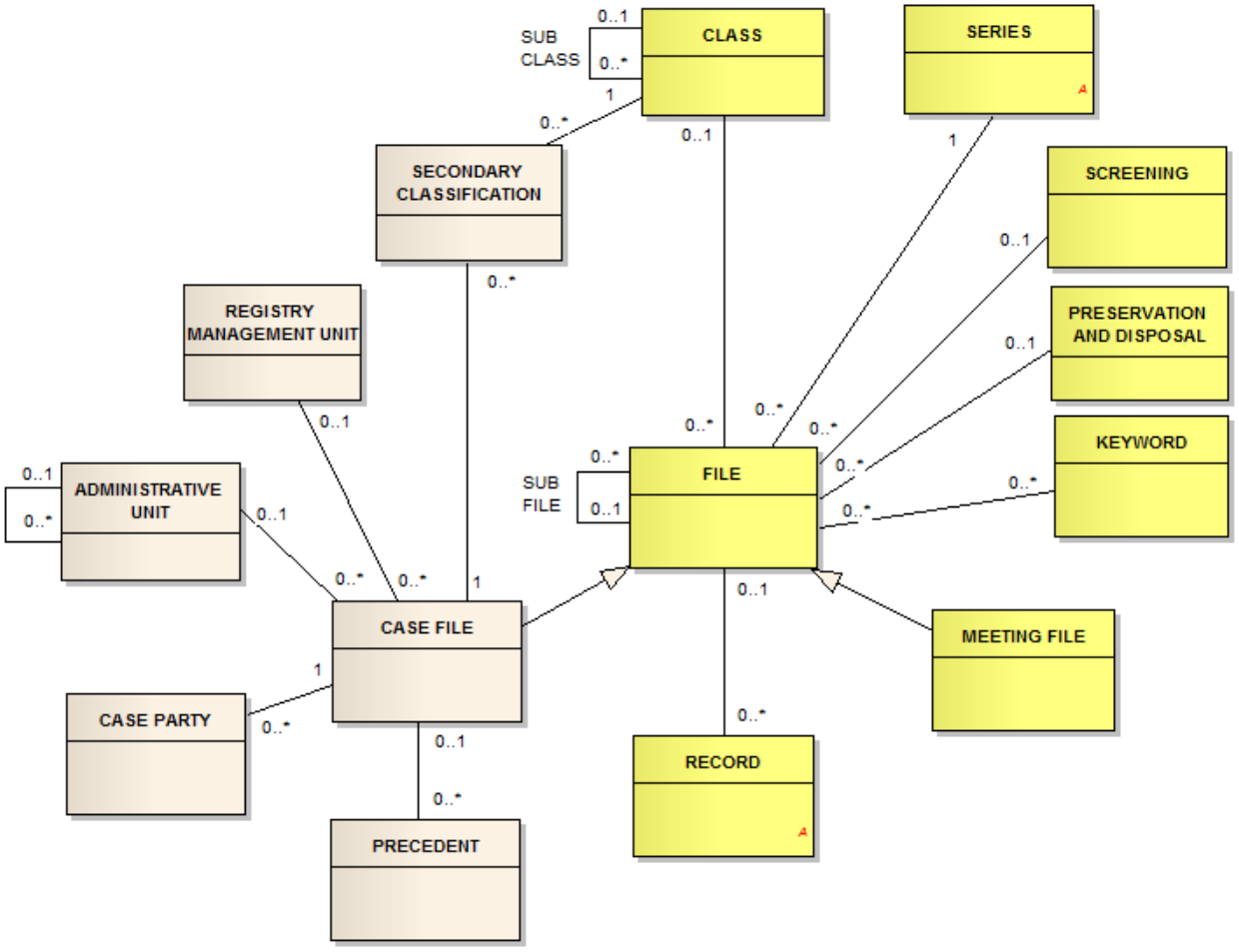
It must be possible to create a file hierarchy of subfiles (specified as a self-relation in the *Basic file*). In most cases, one level of subfiles will be sufficient, but Noark 5 also opens up the possibility of several levels of such files. This will first and foremost be relevant for task systems. The content of subfiles will normally be grouped according to content, not according to activities. Many task systems group documents according to type, e.g. invoices, orders, correspondence, etc. In a file with meeting documents, they could for example be grouped according to delegated cases, referred cases, interpellations, etc.

Inheritance from a *Class* will always go to the file at the highest level.

Records without files

For case records, the case file is obligatory In certain task systems, the file level can be omitted. A record will then be linked directly to a series and possibly to a class.

Conceptual model for File structure



<Conceptual model for the file level>

Case file

In this version of Noark 5, in addition to Basic file, a specialisation called *Case file* is defined, which corresponds to a "case" in Noark 4. The case file must contain metadata from the basic file in addition to its own metadata. A case file is backwards-compatible with a case in Noark 4, but many new metadata are optional. For case records, it is obligatory to use a case file.

It is possible to create many other specialised file types based on the case file. Many of these are also familiar from systems based on Noark 4: *appointment case, building case, meeting/board cases, division case, planning case agricultural case,* etc.
Some of these case types will typically need additional metadata and will be specified in future versions of Noark 5 as specialisations of Basic file.

Meeting file

The module for meeting handling covers many functions linked to case handling in collegial organisations such as boards, committees, etc.. Meeting handling requires a certain amount of extra functionality and metadata (specialisation of Basic file) and this is documented in a

separate section: Meeting and board handling. (See separate section: *6.4 Meeting and board* handling
).

Administrative unit

Organisational unit, e.g. agency, department, section, secretariat, sector administration or office. All Case files in the records module should be linked to an administrative unit. (See separate section: *6.7 Administrative structure*
).

Series

(See separate section: *5.2 Fonds and Series*
).

Basic file (File)

In this detailed outline of the conceptual model for the file level, we deviate from the general "file term" and use specific names/specialisations for the file types. The starting point for all files in Noark 5 is a *basic file.* A File constitutes a Case in Noark 4 and a File in MoReq2. The basic file contains the minimum fundamental metadata required in order to manage the structure.

Preservation and disposal

(See separate section: *5.10 Retention and disposal*
).

Simplified record

(See separate section: *5.5 Record*
).

Registry management unit

Registry management unit is the name of the organisational unit that is responsible for the organisation's recordkeeping. Another name that is used is 'recordkeeping unit'. As digital records become more widespread, the need to register registry management units may reduce. This will therefore no longer be obligatory in Noark 5. However, it will still be possible to set registry management unit on a file or record, and this will be included as metadata in connection with transfer.

Class

(See separate section: *0 Remarks: Requirements for.*
).

Keyword

Keyword or topic word for retrieving documents. A keyword indicates something about *what an object contains.* (See separate section: *5.7.1* **Keyword**
).

Precedence

(See separate section: *6.2.6 Precedent*
).

Case part

(See separate section: *6.2.5 Parties* to a case
).

Secondary classification

Contains one or more appropriate archive codes or order values from the classification system (the archive key) for a case document.

Screening

(See separate section: *6.6.1 Screening*
)

Metadata for *Basic file*

No.	Name	Type	Occ.	Trans.	Remarks
M001	systemID	O	One	A	
M003	fileID	O	One	A	Corresponds to case number in Noark 4. It is recommended that the format (yy/nnnnnn) should continue to be used in case records.
M080	filetype	O	One	A	
M020	title	O	One	A	
M025	officialTitle	B	One	A	Obligatory in connection with transfer if words in the title are to be screened.
M021	description	V	One	A	
M022	keyword	V	Many	A	
M300	documentmedium	B	One	A	Obligatory for mixed physical and electronic records.
M301	storagelocation	V	One		For physical records.
M600	createdDate	O	One	A	
M601	createdBy	O	One	A	
M602	finalisedDate	B	One	A	Must be assigned a value when the file is finalised.
M603	finalisedBy	B	One	A	Must be assigned a value when the file is finalised.

No.	Name	Type	Occ.	Trans.	Remarks
M200	referenceParent	O	One	A	Reference to folder or file at a superior level.
M201	referenceChild	O	Many	A	Reference to record or file at a subordinate level.
M208	referenceRecordssection	O	One	A	

Remarks: Files can be omitted in certain task systems, and the obligatory metadata above will then not exist.

Metadata for *Case file*

Case file is an expansion of Basic file, so the metadata for basic file are included in case file. The following metadata are additional:

No.	Name	Type	Occ.	Trans.	Remarks
M100	casedate	B	One	A	Obligatory for case records.
M305	administrativeUnit	B	One	A	Obligatory for case records.
M306	case-responsible	B	One	A	Obligatory for case records.
M308	registrymanagementunit	V	One	A	
M052	casestatus	B	One	A	Obligatory for case records.
M106	loanedDate	V	One		For physical records.
M309	loanedTo	V	One		For physical records.
M209	referenceSecondaryClassification	B	Many	A	See remarks below.

Remarks: The reference to the primary class can be found in the basic file: referenceParent. A case file can also have one or many secondary classifications. This facilitates multifaceted classification (as in the K codes).

Metadata for *Meeting file*

Meeting file is defined in a separate section: (See separate section: *6.4 Meeting and board* handling
).

Requirements for *File*

Remarks: When "File" is written, the requirement applies to Basic file and all specialisations of Basic file.

Req. no.	Structural requirements for *File*	Type	Remarks
5.4.1	It must be possible for a *file* to be of different types. *In the conceptual model, this is resolved through specialisation.*	O	
5.4.2	A *Basic file* must belong to a *Series* and a *Series* may contain no, one or several *Basic files.*	O	
5.4.3	A *Basic file* must be classified with a *Class* and a *Class* can classify no, one or several *Basic files.*	O	Classification is obligatory in all case records and will also occur in most task systems.
5.4.4	A *Basic file* can belong to no or one *Class* and a Class can be included in no, one or several *Basic files.* This only applies to task systems.	B	Classification can be omitted in certain types of task system.
5.4.5	It should be possible for a *Basic file* to be included in other *Basic files* in a hierarchy. These are called subfiles and are outlined in the model using a self-relation.	V	
5.4.6	It must be possible for a *Basic file* to consist of no, one or several *Records* and a *Record* can be included in (only) one *Basic file.*	O	
5.4.7	If a *Basic file* is registered as finalised (finalisedDate), it must not be possible to add more *Records* to the *File.*	O	
5.4.8	It must be possible to expand a *Basic file* to a *Case file.* -{}-For case records, it must be possible to use a specialised file type: *Case file.* A *specialised class* can be characterised as an *expansion* of the main class.	B	Obligatory for case records.
5.4.9	It must be possible to identify a *Case file* uniquely within the records. It is recommended that this identification is a combination of the case year and a consecutive sequential number for the case files within the year.	B	Other ways of identifying case files may be accepted.
5.4.10	It must be possible for a *Case file* to have registered no, one or several *Secondary classifications* and a *Secondary classification* belongs to one *Case file* only and one *Class* only.	B	Obligatory for case files.

Req. no.	Structural requirements for *File*	Type	Remarks
5.4.11	It should be possible for a *Case file* to have registered no or one *Registry management units* and a *Registry management unit* can be included in no, one or several *Case files.*	V	Registry management unit is no longer obligatory for case records.
5.4.12	It must be possible for a *Case file* to have registered no or one *Administrative units* and an *Administrative unit* can be included in no, one or several *Case files.*	B	Obligatory for case records.
5.4.13	It must be possible for a *Case file* to contain no, one or several *Case parts* and a *Case part* must always belong to a *Case file.*	B	Obligatory for case records. See also the remarks below.

Remarks: Metadata for Case part are described in section 4.3.3.2.

Req. no.	Functional requirements for *File*	Type	Remarks
5.4.14	If a primary classification system is specified for *Series*, all *Files* in the series must have values from this classification system as the primary class.	B	Obligatory if primary classification system is specified for series.
5.4.15	There must be a service/function for updating secondary classification systems against a *Case file* (referenceSecondaryClassification).	B	Obligatory for case records.
5.4.16	There should be a service/function for updating *Registry management unit* on a *Case file*.	V	
5.4.17	There must be a service/function for updating *Registry Administrative unit* on a *Case file*.	B	Obligatory for case records.
5.4.18	There must be a service/function for updating *Case part* in connection with a *Case file*.	B	Obligatory for case records.
5.4.19	There should be a service/function for setting up and updating subfiles for a *Basic file* (file hierarchy).	V	

5.5 Record

An activity can be divided into a number of stages which we call *transactions.* Strictly speaking, a transaction involves at least two people or units, but this need not always be the case. Nevertheless, we use the term transaction generally to refer to all stages into which an activity can be divided. Transactions generate *archival documents*, and the archival document is documentation that the transaction has been completed.

It is not the case that all stages in a sequence of activities necessarily need to be documented. In official correspondence-based case handling, typical transactions will be: an application is received, the executive offices assesses the application and prepares a proposed decision, the decision is approved by the manager and a letter of reply is dispatched. In such cases, at least the first and last transactions must be documented. It may be necessary to document the executive officer's deliberations leading up to the decision.

In connection with the development of task systems for standardised case handling, it is important that the various transactions are identified and that the central transactions generate documents which can be captured and archived in the inner core.

Records must have a unique identification within a particular archive. Noark 5 does not set out any requirements concerning what this code should look like. As regards registry entries, it is recommended that the same template that was used in previous versions of the Noark standard continues to be used. The identification from the file level is inherited and the records are numbered consecutively within the file, e.g. 2008/12345-1.

Record types

In the same way as Noark 5 is flexible as regards the file level, the standard is also flexible as regards the record level. Not all task systems need as much metadata at this level.

Simplified record

In physical case records, it has been commonplace to place documents which are subject to an archive obligation (not subject to archive restriction), but not a recordkeeping obligation, in the case cover without this being registered in the records. Corresponding functionality should also be possible in an electronic records system. Here, the documents must necessarily be registered, but this will take place automatically and with the least possible metadata. It must not be possible to search for and bring up this type of document according to content, and it must also not be included in the ordinary identification (numbering) of registry entries. These documents will also not be included in official records. However, it must be possible for them to be included in a transfer export if they are important archive material, and it must be possible to screen them internally. In Noark 4, this was called "logged documents". In Noark 5, this is specified as a separate record type called *simplified record.* A simplified record contains all metadata which are necessary in order to link the record to the rest of the records structure. These are metadata which must also be included in all the other record types. Metadata for simplified record are therefore obligatory, even if the solution itself does not implement any function for "archiving without recordkeeping".

Basic record

In the same way as there is a file type called basic file, there is also a separate record type called *basic record*. This contains the minimum fundamental metadata that must be included in all task systems. A basic file can form a starting point for other file types for specialised task systems.

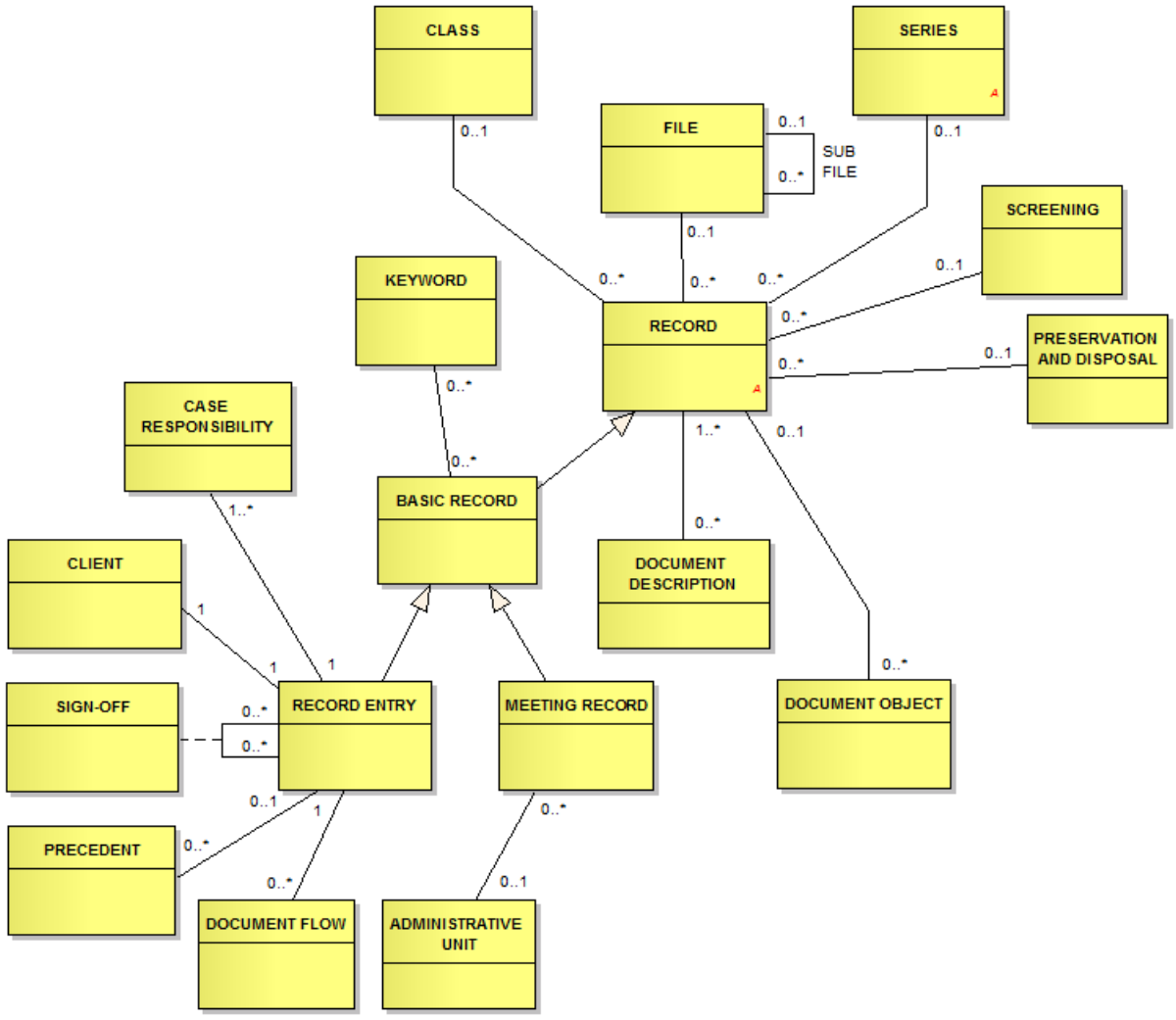
Registry entry

A *registry entry* from Noark 4 constitutes a separate record type in Noark 5. A *registry entry* represents an "entry in the records". The records are a chronological list of incoming and outgoing documents and, where applicable, internal documents that form part of case handling.

By way of comparison, a *basic record* represents a general "entry" in all types of records systems, including those that do not contain correspondence-based documents.

The record type registry entry is obligatory for case records. All documents that are subject to a *recordkeeping obligation* in the public administration must be registered as registry entries and be included in case records.
If a system based on Noark 5 is to be used for case records only, there is nothing to prevent the term "registry entry" from continuing to be used in all interfaces with users, in the same way as with Noark 4. In this standard, record is used as a general designation for record units which document transactions. (*Registrering*, or "Record", is also an appropriate Norwegian translation of the corresponding term in MoReq2, which is called *Record*).

Conceptual model for *Record*



<Conceptual model for the Record level>

Metadata for *Simplified record*

These are metadata which are common to all record types.

No.	Name	Type	Occ.	Trans.	Remarks
M001	systemID	O	One	A	
M081	recordtype	O	One	A	
M600	createdDate	O	One	A	
M601	createdBy	O	One	A	
M604	archivedDate	B	One	A	Must be assigned a value when the document is archived.
M605	archivedBy	B	One	A	Must be assigned a value when the document is archived.
M200	referenceParent	O	One	A	Reference to file, where appropriate to class.
M208	referenceRecordssection	V	One	A	See remark 1 below.
M207	referenceDocumentdescription	B	Many	A	Obligatory for electronic records (electronic documents)
M216	referenceDocumentobject	V	Many	A	See remark 2 below.

Remarks:

1. *Reference to series may be relevant if a series is used to control preservation and disposal decisions for particular record types (document types). This also applies if a series is used to separate paper documents and electronic documents within the same folder. In principle, this contradicts the Director General of the National Archival Services' provisions, but it does open up this possibility in exceptional cases. References to series will also occur if the folder level is deleted, which could be permissible for certain task systems.*
2. *Direct reference to document object could be used for certain task systems with automatic document capture. The preconditions then are that each registry entry only contains an individual document and that this document is not linked to other registry entries.*

Metadata for *Basic record*

In addition to the metadata from *Simplified record*, a basic record must contain the following:

No.	Name	Type	Occ.	Trans.	Remarks
M004	recordID	O	One	A	Corresponds to the combination of case number and document number in Noark 4 in connection with case records. It is recommended that the format (yy/nnnnnn-nnnn) continue to be used in case records.
M020	title	O	One	A	
M025	officialTitle	B	One	A	Obligatory for transfer if words in the title are to be screened.
M021	description	V	One	A	
M022	keyword	V	Many	A	
M024	author	O	Many	A	Obligatory in basic record, but can be replaced by executive officer in registry entry.
M300	documentmedium	B	One	A	Obligatory for mixed physical and electronic records.
M301	storagelocation	V	One		For physical records.

Metadata for *Registry entry*

In addition to the metadata from *simplified record* and *basic record*, a registry entry must contain the following:

No.	Name	Type	Occ.	Trans.	Remarks
M009	serialnumber	B	One	A	Obligatory for case records. It is recommended that the format in Noark 4 (nnnnnnn/yy) continue to be used.
M082	registryentrytype	B	One	A	Obligatory for case records and task systems with correspondence documents.

No.	Name	Type	Occ.	Trans.	Remarks
M053	recordsstatus	B	One	A	Obligatory for case records.
M101	registrydate	B	One	A	Obligatory for case records.
M103	documentDate	V	One	A	
M104	receivedDate	B	One	A	Obligatory for case records and task systems with correspondence documents if the communication is electronic.
M105	sentDate	B	One	A	Obligatory for case records and task systems with correspondence documents if the communication is electronic.
M109	duedate	V	One		
M110	confidentialityassessedDate	V	One		
M305	numberofAppendices	V	One	A	For physical records.
M106	loanedDate	V	One		For physical records.
M309	loanedTo	V	One		For physical records.

Metadata for *Clients*

Metadata for clients must be grouped into metadata for registry entry. Client is obligatory and may occur one or more times in a registry entry.

No.	Name	Type	Occ.	Trans.	Remarks
M087	clienttype	B	One	A	Obligatory for case records and task systems with correspondence documents.
M400	clientName	B	One	A	Obligatory for case records and task systems with correspondence documents.
M406	postaladdress	V	One	A	
M407	postcode	V	One	A	

No.	Name	Type	Occ.	Trans.	Remarks
M408	postaltown	V	One	A	
M409	foreignaddress	V	One	A	
M410	emailaddress	V	One	A	
M411	telephonenumber	V	One	A	
M412	contactperson	V	One	A	

Metadata for *Case responsibility*

Metadata for case responsibility must be grouped into metadata for registry entry. In the case of internal documents which must be followed up, there is a need to group information concerning case responsibility because it may occur on several occasions (on both the sender and the receiver side). Case responsibility is obligatory and may occur one or more times in a registry entry.

No.	Name	Type	Occ.	Trans.	Remarks
M305	administrativeUnit	B	One	A	Obligatory for case records.
M307	executiveofficer	B	One	A	Obligatory for case records.
M308	registrymanagementunit	V	One	A	

Metadata for *Meeting file*

Meeting file is defined in a separate section: See Meeting and board handling.

Requirements for *Record*

Req. no.	Structural requirements for *Record*	Type	Remarks
5.5.1	It must be possible for a *Simplified record* to be divided into different types. *Remarks: In the conceptual model, this is resolved through specialisation, i.e. expansions for each type.*	O	
5.5.2	If the File level is used, a *Simplified record* must belong to (only) one *Basic file* and a *Basic file* can contain no, one or several *Simplified records.*	O	

Req. no.	Structural requirements for *Record*	Type	Remarks
5.5.3	If the File level is not used, a *Simplified record* must belong to (only) one *Series* and a *Series* can contain no, one or several *Simplified records.* *Remarks: This is outlined in the model via an EITHER/OR constraint.*	B	Only relevant for certain task systems.
5.5.4	If the File level is not used, a *Simplified record* must belong to only one *Class* and a *Class* can be included in no, one or several *Simplified records.* *Remarks: This is outlined in the model via an EITHER/OR constraint.*	B	Only relevant for certain task systems.
5.5.5	It must be possible for a *Simplified record* to contain no, one or several *Document descriptions* and a *Document description* must be included in one or more *Simplified records.*	O	See remarks.
5.5.6	It must be possible to expand a *Simplified record* to a *Basic record.*	O	As a minimum requirement, all task systems must contain metadata for Simplified records + Basic records.
5.5.7	It must be possible to expand a *Basic record* to a *Registry entry.*	B	Obligatory for case records.
5.5.8	It must be possible to define a *registry entry* as being of different types ("Noark document type").	B	Obligatory for case records.
5.5.9			
5.5.10	A *Registry entry* must have registered a *Case responsibility (i.e. administrative unit, Executive officer* and where appropriate a *registry management unit)* and it must be possible for a *Case responsibility* to be included in no, one or several Registry entries.	B	Obligatory for case records.
5.5.11	A *Registry entry* must have registered a *Client* and a *Client* must be included in (only) one *Registry entry.*	B	Obligatory for case records.

Remarks: There may also be some task systems where the document description level can be omitted. This will typically concern task systems with automatic document capture, in which only one document is linked to the record and in which the document is not included in other fonds.

Req. no.	Functional requirements for *Record*	Type	Remarks
5.5.12	There must be a service/function for updating a *Registry management unit* on a *Record* (Registry entry).	V	
5.5.13	There must be a service/function for updating an *Administrative unit* and *Executive officer* on a *Record* (Registry entry).	O	
5.5.14	There must be a service/function for updating a *Client* on a *Registry entry*.	O	

5.6 Document description and Document object

Document description

A document is an object that can be handled as a unit, regardless of what it contains. In order to underline this, we can use the term *individual document.* A record that documents a transaction will normally consist of just one individual document. The document description contains metadata for individual documents.

However, in some cases, the record may consist of several documents. The most common situation is a main document with appendices, where the main document and each of the appendices each constitutes an individual document.

In the user interface, it should be possible to hide the document description level. Task systems that will never contain records with more than one individual document do not need this level at all. In the model, this is resolved by adding a direct reference between Record and Document object.

Disposal

It must also be possible to carry out preservation and disposal at this level, e.g. based on document types. It must also be possible to screen individual documents, e.g. the main document may be unclassified, while the appendix is screened.

Noark 4

In Noark 4, it was not permitted for a document to be linked to several registry entries as a main document (although there could be a main document in one registry entry and an appendix in another one). This restriction has been lifted in Noark 5.

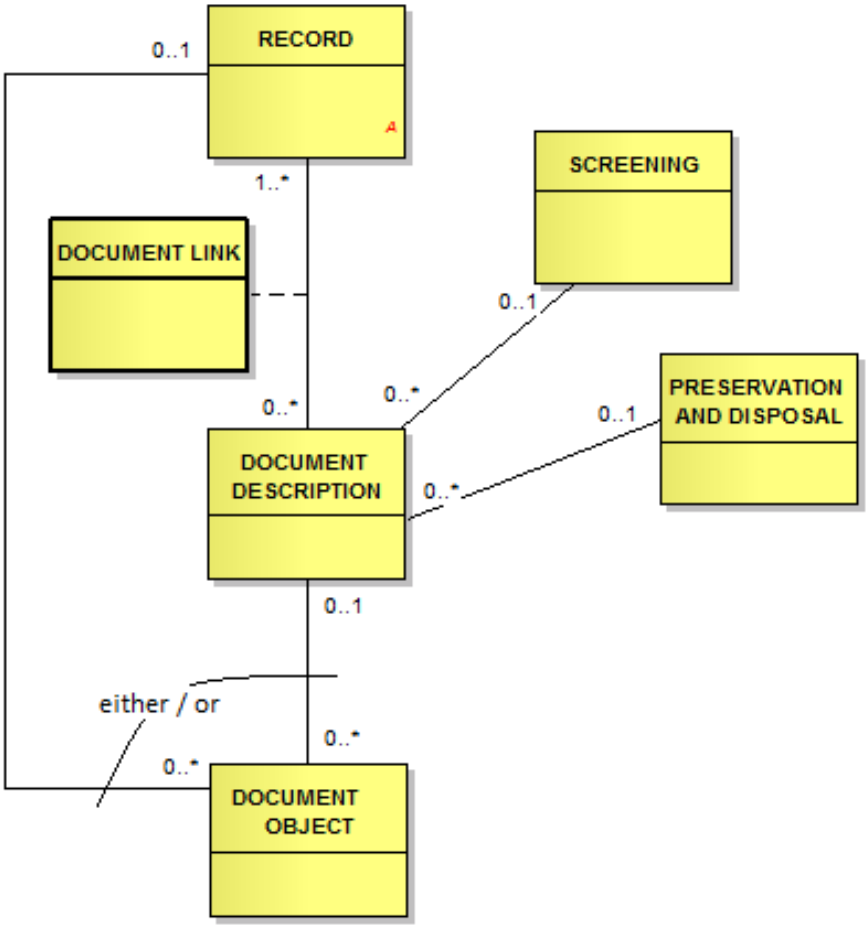
Document object

Document object is the lowest metadata level in the fonds structure. A document object must refer to one and only one file. This file contains a *byte sequence*, which represents an electronic document. If the document is archived in several *versions*, we must have a document object for each version. Each version of the document can also be archived in several different *formats*, and separate document objects must then also be created for each format. In some cases, it may also be appropriate to create *variants* of individual documents. The most common variant will be a publicly available version of the document from which confidential information has been

removed, so that the variant can be made publicly available. The document object will contain more technical metadata than the other record units.

What appears to be a document (a defined unit) to users can be stored as several files in the system. A common example is an HTML document with associated graphics, in which each graphic element is saved as a separate file. Saving documents in this way in an active solution based on Noark 5 is entirely permissible. However, in the case of export for transfer, the individual document (i.e. versions and variants of documents) must be represented as an individual file. Requirements are imposed concerning the transfer format that can be used.

Conceptual model for *Document description* and *Document object*



<Conceptual model for Document description and Document object>

Metadata for *Document description*

A document description can be linked to more than one record, and in the case of transfer, metadata will be duplicated for each link.

No.	Name	Type	Occ.	Trans.	Remarks
M001	systemID	O	One	A	
M083	documenttype	B	One	A	
M054	documentstatus	B	One	A	Obligatory for case records.
M020	title	B	One	A	Obligatory for case records.
M021	description	V	One	A	
M024	author	V	One	A	
M600	createdDate	O	One	A	
M601	createdBy	O	One	A	
M300	documentmedium	B	One	A	Obligatory for mixed physical and electronic fonds.
M301	storagelocation	V	One		
M216	referenceDocumentobject	O	Many		

Remarks: In certain task systems with automatic document capture, document description can be omitted and none of the metadata above will then be obligatory. The reference will then go directly from record to document object. The preconditions for this are that the record is only linked to one document and that this document is not linked to other records.

Metadata for *Document link*

Metadata for linking Record and Document object. Because it must be possible to link a document to more than one record, the following extra metadata are required. In the case of transfer exports, these metadata must be merged with metadata for the document description. In the transfer export, metadata for document description will be duplicated for each occasion that the document description occurs in the export.

No.	Name	Type	Occ.	Trans.	Remarks
M206	referenceRecord	O	One		
M217	linkedRecordAs	O	One		Specifies the “role” of the document in relation to the record (main document, appendix, etc.).
M007	documentnumber	O	One		Numbering of the documents within a record.

No.	Name	Type	Occ.	Trans.	Remarks
M620	linkedDate	O	One		
M621	linkedBy	O	One		

Remarks: Documentlink has no reference to the document description. In connection with transfer, metadata for document link will be included in metadata for document description. (However, in a database model, a table for document link must of course have a reference to both record and document description).

Metadata for *Document object*

No.	Name	Type	Occ.	Trans.	Remarks
M001	systemID	O	One	A	
M005	versionnumber	O	One	A	Identification of versions within the same document. See also remark 1 below.
M700	variantformat	O	One	A	Specification of whether it concerns production format, archival format, screened document, etc. See also remark 2 below.
M701	format	O	One	A	
M702	formatDetails	V	One	A	
M600	createdDate	O	One	A	
M601	createdBy	O	One	A	
M207	referenceDocumentdescription	O	One	A	
M206	referenceRecord	B	One	A	Only applies to task systems in which the document description level is omitted.
M218	referenceDocumentfile	O	One	A	The reference to the document file's "path", i.e. file directory structure + file name.
M705	checksum	O	One	A	Generated when the transfer export is produced.

No.	Name	Type	Occ.	Trans.	Remarks
M706	checksumAlgorithm	O	One	A	Generated when the transfer export is produced.
M707	filesize	O	One	A	Generated when the transfer export is produced.

Remarks

1. *This concerns archived versions of the same document. All the archived variants must be included upon transfer.*
2. *In connection with transfer, only documents in transfer format must be included. If documents occur in archival format and do not need to be converted, it is important that the value is set to "Archival format" as soon as the document is created. If sections of the document are to be removed, both the original document and the screened document must follow.*

Requirements for *Document description* and *Document object*

Req. no.	Structural requirements for *Document description* and *Document object*	Type	Remarks
5.6.1	It must be possible for a *Simplified record* to consist of no, one or several *Document descriptions* and a *Document description* must be included in one or more *Simplified records.* These records can be linked to *files* which belong to different *series* and *fonds*.	O	
5.6.2	It must be possible to divide *Document description* into different types.	O	
5.6.3	A *Document description* must have one or more *Document objects* and a *Document object* can be included in no or one *Document description.*	O	
5.6.4	If *Document description* is not used, *Document object* must belong to (only) one *Simplified record* and a *Simplified record* can contain no, one or several *Document objects.* *Remarks: This is outlined in the model via an EITHER/OR constraint.*	B	Only applies to certain task systems.
5.6.5	It must be possible for a *document description* for a physical document (e.g. paper) to have a reference to a storage location for the document.	V	For physical fonds.

Req. no.	Structural requirements for ***Document description*** and ***Document object***	Type	Remarks
5.6.6	It must be possible for a *Document object* that is linked to the same *document description* to refer to different *versions* of the document.	O	
5.6.7	It must be possible for a *Document object* that is linked to the same *document description* to refer to different *variants* of a document.	O	
5.6.8	It must be possible for a *Document object* that is linked to the same *document description* to refer to the same document stored in different *formats.*	O	

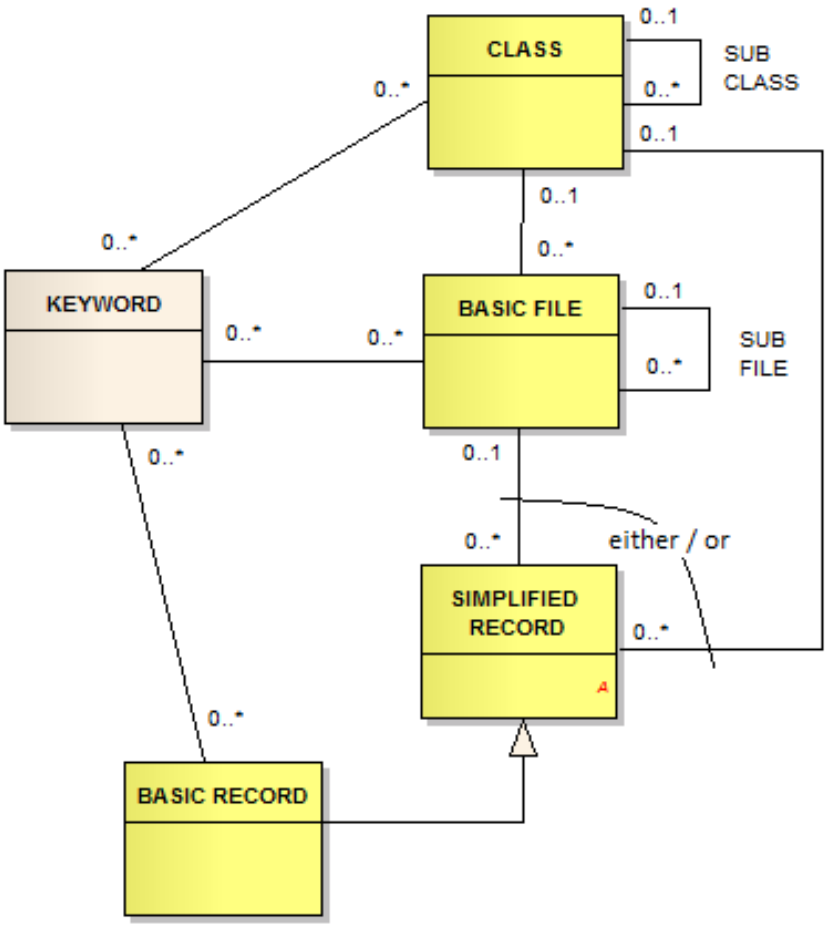
Req. no.	Functional requirements for ***Document description*** and ***Document object***	Type	Remarks
5.6.9	There must be functions which, on creation of a new document, link the new document to a *Document description.*	O	
5.6.10	It must be possible to create a *Document description* without an electronic document.	O	
5.6.11	There must be a function/service for archiving one or more versions/variants/formats of a document.	O	
5.6.12	It must not be possible to delete an archived document. However, it must be possible to delete older versions of the document.	O	

5.7 Common functionality for the fonds structure

5.7.1 Keyword

It should be possible to add one or more keywords to a class, a basic file or a basic record. Keyword must not be confused with faceted classification based on topic words. While the *classification* should give information on the document's *context* (the function that created the document), the *keywords* should indicate something about the document's *content.* The purpose of keywords is to improve the search opportunities for a class, file or record. Keywords can be linked to a controlled glossary (thesaurus). It is not obligatory to implement keywords.

Conceptual model for *Keyword*



<Conseptual model for Keyword>

Metadata for *Keyword*

No.	Name	Type	Occ.	Trans.	Remarks
M022	keyword	V	Many	A	

Requirements for *Keyword*

Req. no.	Structural requirements for *Keyword*	Type	Remarks
5.7.1	It must be possible for a *Class* to have registered no, one or several *Keywords* and it must be possible for a *Keyword* to form part of no, one or several *Classes.*	V	
5.7.2	It must be possible for a *Basic file* to have registered no, one or several *Keywords* and it must be possible for a *Keyword* to form part of no, one or several *Basic files.*	V	

Req. no.	Structural requirements for *Keyword*	Type	Remarks
5.7.3	It must be possible for a *Basic record* to have registered no, one or several *Keywords* and it must be possible for a *Keyword* to form part of no, one or several *Basic records.*	V	

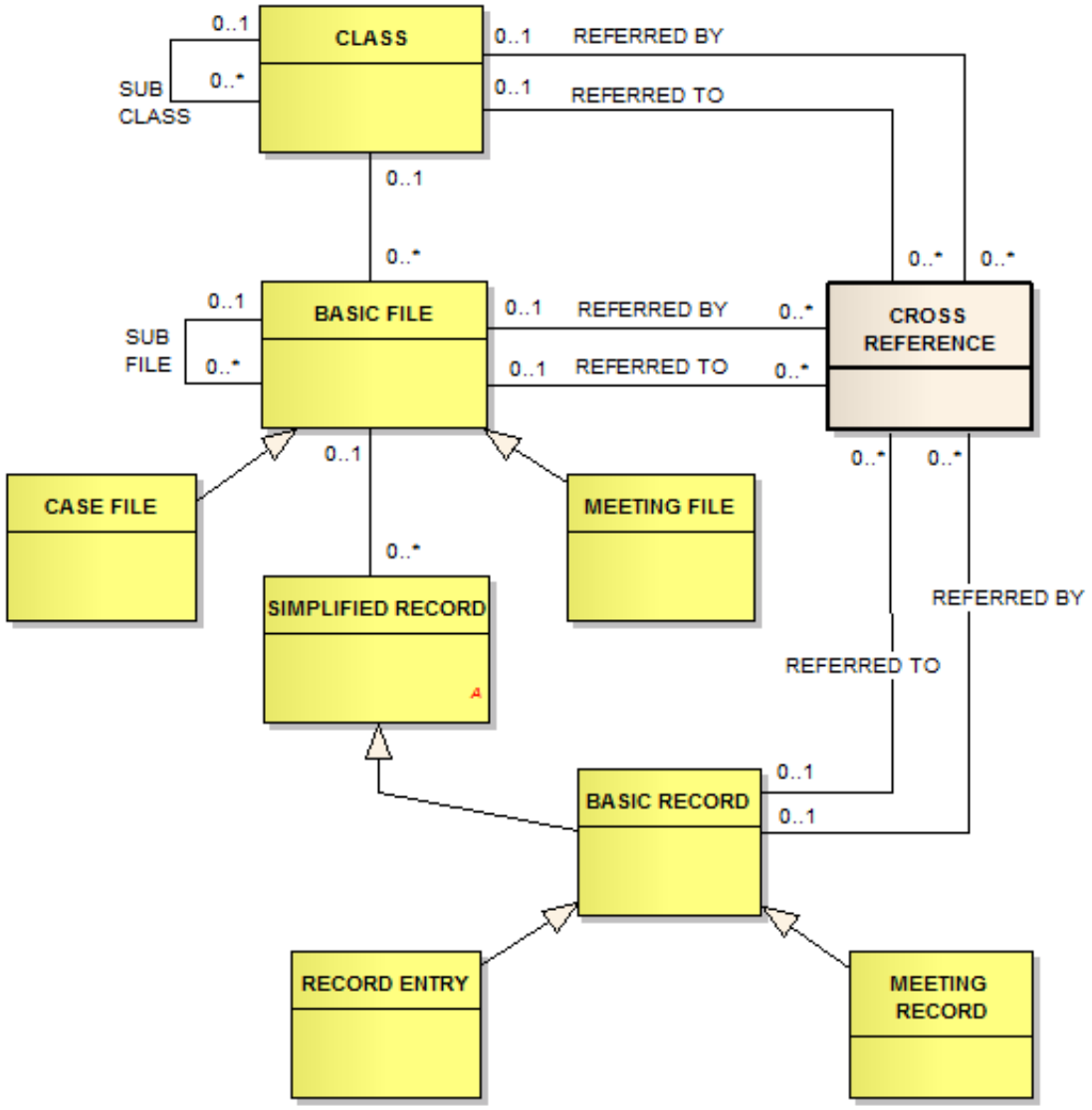
Req. no.	Functional requirements for *Keyword*	Type	Remarks
5.7.4	There must be a service/function for linking one or more keywords to classes, files and records (except simplified records).	V	

5.7.2 Cross-reference

This is a reference across the hierarchy in the fonds structure. The reference can go from one file to another file, from one record to another record, from a file to a record or from a record to a file. Reference can also be made from one class to another class.

The cross-reference will also cover expanded classes (specialisations). As Cross-references are linked to Basic file and Basic record, this means that References are also linked to all the expansions (specialisations) under these (Case file, Meeting file and Registry entry, Meeting record).

Conceptual model for *Cross-reference*



< References in the Record structure>

Metadata for *Cross-reference*

Metadata for cross-reference must be grouped into metadata for class, basic file or basic record. Cross-reference is optional and may occur on one or more occasions.
The reference can go from one class to another class, from one file to another file, from one record to another record, from a file to a record and from a record to a file. The cross-reference will also cover specialisations. A cross-reference can therefore go from a meeting file to a case file. References between classes are optional.

No.	Name	Type	Occ.	Trans.	Remarks
M219	referenceToClass	V	One	A	Grouped into class.
M220	referenceFromClass	V	One	A	Grouped into class.

No.	Name	Type	Occ.	Trans.	Remarks
M210	referenceToFolder	V	One	A	Grouped into file or record.
M211	referenceFromFile	V	One	A	Grouped into file or record.
M212	referenceToRecord	V	One	A	Grouped into file or record.
M213	referenceFromRecord	V	One	A	Grouped into file or record.

Requirements for *Cross-reference*

Req. no.	Structural requirements for *Cross-reference*	Type	Remarks
5.7.5	From one *Class*, it should be possible to refer to one or several other *Classes.*	V	
5.7.6	It should be possible to refer to a *Class* from one or several other *Classes.*	V	
5.7.7	From one *Basic file*, it should be possible to refer to one or several other *Basic files.*	B	Obligatory for case records, relevant to many task systems.
5.7.8	It should be possible to refer to a *Basic file* from one or several other *Basic files.*	B	Obligatory for case records, relevant to many task systems.
5.7.9	From one *Basic file*, it should be possible to refer to one or more *Basic records.*	B	Obligatory for case records, relevant to many task systems.
5.7.10	It should be possible to refer to a *Basic file* from one or several other *Basic records.*	B	Obligatory for case records, relevant to many task systems.
5.7.11	From one *Basic record*, it should be possible to refer to one or several other *Basic records.*	B	Obligatory for case records, relevant to many task systems.
5.7.12	It should be possible to refer to a *Basic record* from one or several other *Basic records.*	B	Obligatory for case records, relevant to many task systems.

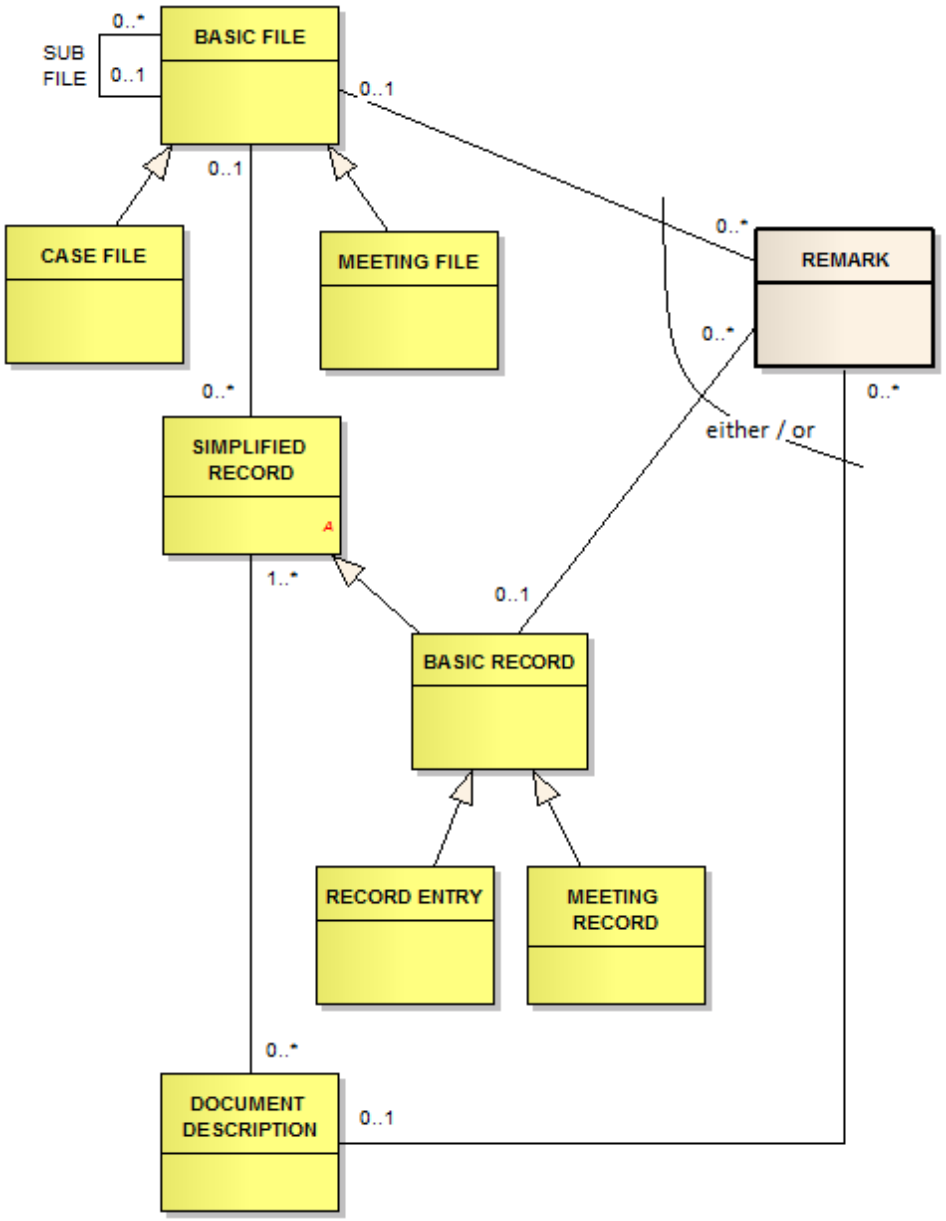
Req. no.	Functional requirements for *Cross-reference*	Type	Remarks
5.7.13	There must be a service/function that can *store, retrieve, alter and delete* a Cross-reference between: • Basic files • Basic records or to references between them.	O	
5.7.14	There should be a service/function that can *store, retrieve, alter and delete* a Cross-reference between: • Classes	V	

5.7.3 Remarks

It must be possible to link one or several remarks to a basic file, basic record or document description. Remarks must be used to document special circumstances concerning the case handling and archiving of documents and this information must be included in transfer exports.

As regards the approval of documents in flow, there is a separate metadata element for remarks – see section 6.6 Document flow.

Conceptual model for Remarks



<Remarks in the record structure>

Metadata for *Remarks*

Metadata for remarks must be grouped into metadata for basic file, basic record and document description. Remarks are optional and may occur on one or more occasions.

No.	Name	Type	Occ.	Trans.	Remarks
M310	remarktext	V	One	A	
M084	remarktype	V	One	A	
M611	remarkdate	V	One	A	

No.	Name	Type	Occ.	Trans.	Remarks
M612	remarkRegisteredBy	V	One	A	

Requirements for *Remarks*

Req. no.	Structural requirements for *Remarks*	Type	Remarks
5.7.15	A *Remark* must be included in (belong to) either a *Basic file, Basic record* or *Document description.* *Remarks: This is modelled using an "either/or" constraint in the conceptual model.*	B	Obligatory for case records, relevant to many task systems.
5.7.16	It must be possible for a *Basic file* to be linked to no, one or more *Remarks.*	B	Obligatory for case records, relevant to many task systems.
5.7.17	It must be possible for a *Basic record* to be linked to no, one or more *Remarks.*	B	Obligatory for case records, relevant to many task systems.

Req. no.	Functional requirements for *Remarks*	Type	Remarks
5.7.18	There must be a service/function that can register a *Remark* to a *Basic file* or *Basic record.*	B	Obligatory for case records, relevant to many task systems.
5.7.19	If more than one remark is linked to a *Basic file* or a *Basic record*, the metadata must be grouped together upon export and exchange.	B	Obligatory for case records, relevant to many task systems.
5.7.20	It should be possible to freely define types of remarks.	V	

5.8 Document capture

Electronic documents that are created or received as part of the case handling may have their origins in both internal and external sources. The electronic documents will have many different formats and be produced by different authors, and may be either simple files or complex documents.

Some documents are produced internally within an organisation as part of case handling. Others are received through various communication channels, e.g. e-mail, fax, post, SMS and self-service solutions on the internet.

A function for flexible document capture is essential for handling this. It must also be possible to capture documents completely independently of the document's format. It will for example be appropriate to establish functions for document capture from office support equipment

(word processors, spreadsheets, etc.), e-mail, video, websites, scanned documents and audio recordings.

In some contexts, it will also be appropriate to capture other types of document, such as blogs, compressed files, electronic calendars, data from geographic information systems, multimedia documents, documents that contain links to other documents, instant messaging services, text messages to mobile telephones (SMS), pictures to mobile telephones (MMS) and wikis.

Structure and content specification (XML form) for general document capture will follow in a later version of Noark 5.

Req. no.	Functional requirements for document capture	Type	Remarks
5.8.1	There must be functionality for capturing electronic documents independently of file format, methods for technical coding, sources or other technical characteristics.	O	
5.8.2	Data capture must take place in such a way that the document's appearance (layout integrity) is maintained.	O	
5.8.3	Data capture must take place in such a way that the document's content integrity is maintained.	V	
5.8.4	There should be functionality for fully automatic document capture.	V	
5.8.5	In connection with fully automatic document capture, it must be possible to link all obligatory metadata to the document.	B	
5.8.6	In connection with fully automatic document capture, it must be possible to link documents to a classification system.	B	
5.8.7	In connection with fully automatic document capture, it should be possible to link documents to one or several files or classes in the record structure.	V	
5.8.8	There must be no restrictions on the number of documents that can be linked to a class or file.	O	
5.8.9	There must be no restrictions on the number of documents that can be archived in the solution.	O	
5.8.10	There must be functions for ensuring that all components in a composite document are captured.	O	
5.8.11	There must be functions for ensuring that a composite electronic document is handled as an entity, in which the relationship between the components and the document's internal structure is maintained.	O	

Requirements for batch import, electronic forms for completion via the internet, electronic document exchange and migration between Noark solutions are described in section *6.3 Electronic communication*

.

5.9 Retrieval

"Retrieval" is defined as the inner core's scope to deliver the metadata and documents that the outer core and Noark 5 complete request, e.g. when a search is initiated from a task or pre-system.

In order for the outer core and complete solutions to be able to produce statutory and optional reports and statistics, it is essential that the core is provided with services or functions for retrieval and logical combinations of metadata. Public registries are an example of such a statutory report.

Searching in metadata is carried out through searching individual metadata elements or a combination of metadata elements, or with the aid of a free text search, e.g. searching according to a given text string in a set of metadata elements.

Document retrieval is typically carried out through a search of the documents' metadata, e.g. in document description metadata. If the format permits, free text searches can be performed in documents.

Search results must take into consideration access to documents in the core and to the screening of information.

Req. no.	Functional requirements for retrieval	Type	Remarks
5.9.1	There must be services/functions for retrieving/searching for metadata.	O	
5.9.2	When searching, it must be possible to create logical combinations of metadata.	O	
5.9.3	When searching in metadata, it must be possible to use left- and right-truncation, as well as the marking of one or more characters in the search criteria.	O	
5.9.4	In metadata elements which represent dates, it must be possible to search for date intervals.	O	
5.9.5	In metadata elements that represent dates, it must be possible to search for periods that fall before or after a given date.	O	
5.9.6	It must be possible to perform free text searches in metadata.	O	

Req. no.	Functional requirements for retrieval	Type	Remarks
5.9.7	When performing free text searches in metadata, it must be possible to search for several search terms combined using Boolean operators.	O	
5.9.8	There must be services/functions for retrieving/searching for documents.	O	
5.9.9	It must be possible to retrieve documents on the basis of document metadata.	O	
5.9.10	It must be possible to perform free text searches in a document if the format permits.	O	
5.9.11	Search results must reflect current access.	O	
5.9.12	Search results must be necessarily screened.	O	
5.9.13	It must be possible for upper- and lower-case letters to be handled as equivalents when searching.	O	
5.9.14	There should be a service/function to cancel a search that has been initiated.	V	
5.9.15	The search functions should be organised so that when searching for a term in Norwegian bokmål form, the user also gets hits for the corresponding Nynorsk forms and vice versa.	V	

5.10 Retention and disposal

Disposal means that electronic documents are removed from the fonds structure. If the document is not linked to other records, a disposal will also result in the document being deleted entirely from the Noark 5 solution. Disposal of physical documents means that they are picked from the place where they are stored and shredded or destroyed appropriately.

The number of files and associated archive documents in an archive will increase gradually. As time passes, older files will become more and more irrelevant to the fonds creator. In purely general terms, it is assumed that the public bodies will have no administrative need to retain archive material that is more than 30 years old. However, there will be material that must be preserved for longer, and there will also be material that can be disposed of after a shorter period of time. In many cases, the preservation time will be set out in laws and regulations. In accordance with accounting legislation, accounting documents can be disposed of after just 10 years. Patient fonds on the other hand must be retained for much longer, for up to 10 years after a patient has died. Some types of health information will therefore have an administrative lifetime of over 100 years.

The Director General of the National Archival Services has authority to take preservation and disposal decisions concerning official archives. This means that official fonds creators cannot freely dispose of their documents as they wish. A preservation decision means that the archive

material concerned must be preserved without any time restriction and that it must be *transferred* to an archive repository. Transfer is described in section 4.2.12.

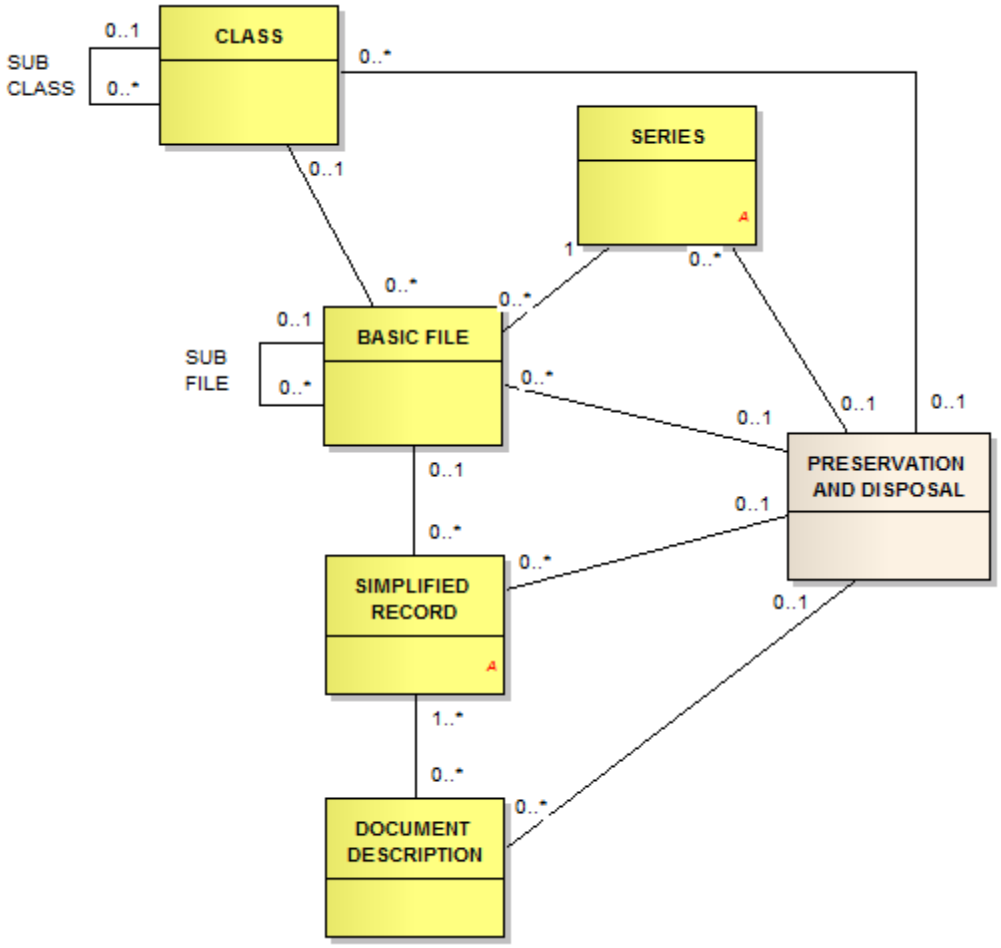
Disposal of electronic documents

Disposal is just as relevant to electronic fonds as it is to physical fonds. Long-term preservation and administration (e.g. conversion to new formats) of large numbers of electronic documents is as expensive as the long-term storage of physical documents. However, finance is not the only reason why all documents that have no preservation value – for either the fonds creator or the archive authorities – should be disposed of on an ongoing basis. The flow of information is overwhelming in today's society, and the more unnecessary information that is retained, the more difficult it can be to search for and find the information you really need.

Disposal does not mean that you have to go in and assess the preservation value of every single document. In order for the disposal of electronic documents to be practicable, preservation and disposal criteria must be established at an overall level, i.e. at a macro-level. International archive theory argues for *function-based macro-disposal.* This means that the archive documents' preservation value depends on the function or activity that created the document – and not on the actual content of the document. There is also agreement in Norway that function-based disposal at macro level can be an important method, although some people claim that consideration must also be given to the documents' content.[7]

[7] Methods for preservation and disposal are described in the report from the Preservation Committee (*Bevaringsutvalget*) (2002).

Conceptual model for *Preservation and disposal*



< Disposal in the record structure>

Metadata for *Preservation and disposal*

Metadata for preservation and disposal must be grouped into metadata for series, class, file, record and document description. Metadata for preservation and disposal are optional and can occur once.

In Noark 4, these attributes have different names depending on the level in the fonds structure to which they are linked. References to attributes at case level are shown below.

Metadata for *disposal*

No.	Name	Type	Occ.	Trans.	Remarks
M450	disposaldecision	B	One	A	
M453	disposalauthority	V	One	A	
M451	preservationtime	B	One	A	

No.	Name	Type	Occ.	Trans.	Remarks
M452	disposaldate	B	One	A	

A *preservation and disposal decision* indicates what is to happen to the documents when the *preservation time* has elapsed. Obligatory values are "To be preserved", "To be disposed of" and "To be assessed later". The preservation time can typically be 5, 10 or 30 years. The *disposal date* is calculated automatically based on the preservation time. The preservation time begins to elapse the moment a case file is finalised. However, it must also be possible to establish other rules for calculating the disposal date.

Function-based disposal assumes that the classification system describes the organisation's functions and activities. In Noark 5, it must be possible to set preservation and disposal decisions in the individual classes in a classification system. This can then be automatically passed on to all files that are assigned to the class.

It must also be possible to set preservation and disposal decisions for a series. This will then mean that all files in the series will inherit the same decision. If inheritance takes place from the series, it will not simultaneously be possible to inherit from the classes. Preservation and disposal decisions for many series are first and foremost of relevance in connection with certain task systems that produce so-called "single-type series".

It must be possible for inheritance to take place further down to record and document description level. Although disposal often involves entire files, it must be possible to preserve one or more of the records in the file and dispose of the rest.[8]

It is expected that all requirements linked to preservation and disposal will be met in a standard case records system. If it is established through a decision approved by the Director General of the National Archival Services that disposal is not to take place from the solution, the requirements other than 5.10.1 need not be fulfilled.

Req. no.	Structural requirements for ***Preservation and disposal***	Type	Remarks
5.10.1	It must be possible for a *Series* to have registered no or one *Disposal decision* and a *Disposal decision* can be included in no, one or several *Series.*	O	
5.10.2	It must be possible for a *Class* to have registered no or one *Disposal decision* and a *Disposal decision* can be included in no, one or several *Classes.*	B	Obligatory for disposal beyond series.
5.10.3	It must be possible for a *Basic file* to have registered no or one *Disposal decision* and a *Disposal decision* can be included in no, one or several *Basic files.*	B	Obligatory for disposal beyond class.

[8] An example of this could be an appointment case, where you wish to dispose of all applications from the unsuccessful applicants.

Req. no.	Structural requirements for ***Preservation and disposal***	Type	Remarks
5.10.4	It must be possible for a *Simplified record* to have registered no or one *Disposal decision* and a *Disposal decision* can be included in no, one or several *Simplified records.*	B	Obligatory for disposal beyond basic file.
5.10.5	It must be possible for a *Document description* to have registered no or one *Disposal decision* and a *Disposal decision* can be included in no, one or several *Document descriptions.*	B	Obligatory for disposal decisions beyond simplified record.

Req. no.	Functional requirements for ***Preservation and disposal***	Type	Remarks
5.10.6	There must be a service/function for updating disposal decisions, disposal authority and preservation time for a *Class.*	B	Obligatory if requirements 5.10.2 – 5.10.5 are met.
5.10.7	It must be possible for metadata concerning preservation and disposal for a *Class* to be passed on to *File, Document description* and *Document object.*	B	Obligatory if requirements 5.10.2 – 5.10.5 are met.
5.10.8	There must be a service/function for updating disposal decisions, disposal authority and preservation time for a *Series.*	B	Obligatory if requirements 5.10.2 – 5.10.5 are met.
5.10.9	It must be possible for metadata concerning preservation and disposal for a *Series* to be passed on to *File, Document description* and *Document object.*	B	Obligatory if requirements 5.10.2 – 5.10.5 are met.
5.10.10	If the inheritance of metadata concerning preservation and disposal is to take place from series, this must override the inheritance of metadata from the classes.	B	Obligatory for function for inheritance of disposal code.
5.10.11	There must be a service/function for registering a disposal decision for a *File, Record* or *Document description.* The disposal decision must consist of the following obligatory values: 1. To be preserved 2. To be disposed of 3. To be assessed later Other values can be added.	B	Obligatory for application of disposal decisions beyond series and class.

Req. no.	Functional requirements for ***Preservation and disposal***	Type	Remarks
5.10.12	It must be possible to manually register disposal decisions, disposal authority and preservation time for a *File*, *Record* or *Document description.*	B	Obligatory if 5.10.11 is fulfilled.
5.10.13	It must be possible for the preservation date for a *File*, *Record* or *Document description* to be calculated automatically on the basis of preservation time and the date on which the file was finalised.	B	Obligatory if 5.10.11 is fulfilled.
5.10.14	Other rules for calculating preservation date should be possible.	V	
5.10.15	It must also be possible to register the preservation date for a *File*, *Record* or *Document description* manually. Preservation time will then not be obligatory.	B	Obligatory if 5.10.11 is fulfilled.
5.10.16	It must be possible to deactivate the function for inheritance from classes and series, so that metadata concerning preservation and disposal is not passed on to underlying files.	B	Obligatory for function for inheritance of disposal code.
5.10.17	It must be possible to specify that the inheritance of metadata concerning preservation and disposal must also extend down to record and document description.	B	Obligatory for function for inheritance of disposal code.
5.10.18	It must be possible for metadata concerning preservation and disposal that are inherited from an archive object to all underlying archive objects to be overwritten.	B	Obligatory for function for inheritance of disposal code.
5.10.19	If an archive object is set to disposal and then changed back to preservation, all overlying archive objects in the hierarchy (in an immediately ascending line) must be altered accordingly.	B	Obligatory for function for inheritance of disposal code.

Disposal of document types

Preservation and disposal are therefore essentially linked to metadata that are inherited from the class, or possibly the series, to all underlying files. In addition, it must also be possible to perform a general disposal of certain types of document. It should therefore also be possible to link preservation and disposal to record types, document types or other self-defined types.[9]

Disposal of document types can be implemented through certain record types or document types automatically being linked to a series that contains the preservation and disposal decision for that particular type. This decision must then be passed on to the record or document decision. However, there may also be other ways of implementing this functionality without using series.

[9] An example of this could be advertising enclosures that are enclosed with bids.

Req. no.	Functional requirements for *Preservation and disposal*	Type	Remarks
5.10.20	There should be a service/function that automatically links a particular type of record or document descriptions to a preservation and disposal decision.	V	
5.10.21	Metadata concerning preservation and disposal will then be passed on to all created records or document descriptions of the same type.	B	Obligatory if 5.10.20 is fulfilled.

Overview of documents that are to be disposed of or reassessed

Before disposal is carried out, it must be possible to bring up an overview of documents that are to be disposed of. Such an overview must include the most important metadata, including all metadata for preservation and disposal. From this overview, it must also be possible to open the document itself, so that you can have the document content checked. If the overview contains documents that are not to be disposed of on this occasion, it must be possible to alter metadata directly from the overview. It must be possible to limit the overview so that it covers selected documents, e.g. documents linked to a particular class.

In the same way, it must be possible to bring up an overview of documents that are to be considered for preservation and disposal at a later date. This is primarily of relevance for archive material that documents the rights of individuals or organisations, or where there is uncertainty as to whether or not the documentation need is permanent. For other types of material, it is not desirable that the option of assessment in the future is used. From this overview, it must also be possible to alter metadata directly.

Such functionality will only be necessary in cases where series contain both information which is to be disposed of and information which is to be preserved. It is obligatory for ordinary case records systems to have such functionality. There may be solutions where such advanced functionality will not be necessary, where a function to open documents from the presentation of disposable documents will not be necessary or where an option to create a special overview of disposable documents will not be necessary.

All general case records solutions must fulfil the requirements below.

Req. no.	Functional requirements for *Preservation and disposal*	Type	Remarks
5.10.22	It must be possible to bring up an overview of documents that are to be disposed of after a specific time. It must be possible to limit such an overview to a small selection of documents.	O	
5.10.23	It must be possible to bring up an overview of documents that are to be reassessed for preservation or disposal after a specific time. It must be possible to limit such an overview to a small selection of documents.	O	

Req. no.	Functional requirements for *Preservation and disposal*	Type	Remarks
5.10.24	The overview must contain the most important metadata for the documents, including metadata for preservation and disposal.	O	
5.10.25	It should be possible to open a document for the presentation of content directly from this overview.	V	
5.10.26	Authorised users should be able to alter metadata for preservation and disposal for the individual documents directly from the overview.	V	

Deletion of documents and metadata

The criterion for a document being disposable is that the metadata for the disposal decision has the value "To be disposed of" and that today's date has passed the preservation date. The solution should check that precedence cases are never permitted.

The disposal of electronic documents involves deletion of the reference between the metadata and the documents, so that the documents can no longer be retrieved using metadata. This takes place through all metadata concerning the document object being removed. All versions, variants or formats of the document must be covered by the disposal. If the same document (document description) is linked to several records, the document must not be deleted from the file system. If there is no such link, the document must also be deleted.

The disposal of documents is therefore a critical function that many people shy away from performing. It should therefore be possible to undo a disposal and restore the link to the documents that have been disposed of; cf. the option in operating systems to retrieve documents that have been "thrown into the Recycle bin".

It must be possible to limit the actual function for performing disposal to cover selected documents, e.g. all documents that belong to a particular class. It must be possible to perform the disposal as an automatic process, but it must also be possible to ask to be asked whether disposal is relevant to every single document.

The disposal of documents does not mean that metadata must be deleted. As regards case records within the public administration, the Archives Regulation contains a preservation order for "record databases". This means that metadata concerning discarded documents must generally be preserved and transferred to a repository. It must nevertheless be possible to specify that disposal also involves the deletion of associated metadata. This will be particularly relevant for certain types of task system or "single type series". In such cases, neither the metadata nor the documents will be preserved.

Metadata for completed disposal

Metadata for completed disposal must be grouped into metadata for document description.

No.	Name	Type	Occ.	Trans.	Remarks
M630	disposedofDate	B	One	A	Obligatory when disposal has been carried out.
M631	disposedofBy	B	One	A	Obligatory when disposal has been carried out.

Req. no.	Functional requirements for ***Preservation and disposal***	Type	Remarks
5.10.27	There must be a function for disposing of all documents that have the value "To be disposed of" as the disposal decision and where the preservation date is older than today's date. It must be possible to limit such a function to a small selection of documents.	B	Obligatory in solutions where disposal is to take place and when necessary to distinguish between disposable and non-disposable documents.
5.10.28	It must not be possible to set the disposal decision "To be disposed of" for a file that has been registered as a precedence decision.	O	
5.10.29	It must be possible for the disposal to be carried out automatically for all selected documents, but it must also be possible to ask to be asked whether disposal is to be carried out for every single document.	B	Obligatory when 5.10.27 is met.
5.10.30	Only authorised users can start a function for the disposal of documents.	O	
5.10.31	All versions, variants and formats of the document must be covered by the disposal.	B	
5.10.32	Disposal must involve all metadata concerning the document object being deleted. The document itself must be deleted from the file system if the document (the document description) is not linked to other records.	O	
5.10.33	The function for disposal should be executed in two stages, so that during the first stage it is possible to restore the documents that have been disposed of. It must be possible for the final deletion of document objects and documents to take place at a later time.	V	
5.10.34	Metadata concerning the document down to document description should as a general rule not be deleted even if the document is disposed of.	O	

Req. no.	Functional requirements for ***Preservation and disposal***	Type	Remarks
5.10.35	For every document that is disposed of, the date of disposal and the name of the person who performed the disposal must be logged at document description level.	O	
5.10.36	It must be possible to specify that both the documents and the associated metadata up to file level are to be deleted when the disposal is effected.	O	

5.11 Periodisation

In the case of physical archiving, it has often been desirable to separate out the oldest and most obsolete material from material that is in active use. This material was often placed somewhere where the storage costs were lower than where the active archive was stored. The traditional term for this is *remote storage.* Fonds that have been put into remote storage will still be kept by the fonds creator. Such fonds are in an intermediate stage. The organisation still has a need to retrieve documents from the remote storage archive – but this need will not arise very often.

It is recommended that remote storage be linked to fixed, time-delimited periods called *fonds periods.* A fonds period can typically be five years, but both shorter and longer periods are entirely possible. In the case of physical archiving, *periodisation* means both that documents are moved from one storage place to another and that this movement is indicated by the fonds structure and the metadata that are linked to the documents.

In many cases, periodisation will also be appropriate in electronic fonds. Here, it is not the consideration of the physical storage location that is decisive, but rather the need for an overview and rapid retrieval during searches. As the number of files increases, it will become increasingly impractical to have older finalised files stored together with those which are still open or which have just been finalised. In connection with electronic fonds, it can therefore also be of benefit to organise the fonds into an *active* period and one or more *closed* periods. This subdivision will then also cover both the electronic documents and the associated metadata.

The principles for periodisation that were introduced in Noark 4 will be continued in Noark 5. Here, a distinction is made between two main types of periodisation: sharp period division and division through overlap period.

Sharp period division means that all open files (ongoing cases) in a closed period must be closed and then recreated in a new period (the successor) in connection with the next record. This means therefore that documents that belong together will be placed in two different files, and these will each belong to their own period. These files must therefore be linked together by a reference. Sharp period division is not recommended for electronic fonds.

Periodisation with *overlap periods* (also known as "soft" period division) means that if a file is not finalised at the end of the period, the entire file – with all previous records – must be moved to a new, active period in connection with the next record. This transfer must take place

automatically for as long as the overlap period lasts. At the end of the overlap period, most active cases will be transferred to a new period.

The routines for periodisation of different types of file will be discussed in more detail in the guidelines. In this standard, only the requirements for metadata and for essential functionality for implementing different forms of periodisation will be described.

Fonds period and series

Series play a pivotal role in connection with periodisation. The series represent different periods and it is the affinity of the files to series that determines the period they are placed in. The series' *record status* provides information on whether the period concerned is an active, overlap or closed period. The series must also have a reference between them, so that the predecessor and successor can be linked together. The successor must be linked to the same classification system as the predecessor.

Documents that must be periodised according to different principles, e.g. function-based case files that are periodised through an overlap period and personnel files that are periodised on an ongoing basis as they become obsolete, must each belong to their own series. Several series can therefore be active at once and the non-current periods may constitute several "generations" with fonds periods.

Req. no.	Structural requirements for periodisation	Type	Remarks
5.11.1	It must be possible for a series to contain a text-based description of the principles to be used in the periodisation.	O	
5.11.2	A series must contain references to any predecessors and successors.	O	

Functionality in connection with periodisation

A series that contains an *active period* is open for all record. It must be possible for new files to be linked to the series as they are created.

A series that contains a *closed period* is closed to new files, and the files that already exist must be finalised. A finalised series is therefore "frozen" as regards all new additions of files and documents and essentially also for the alteration of metadata.

A series that contains an *overlap period* is in an intermediate position. New files cannot be linked, but existing files may still be open. A new record may be added to a file during the overlap period. However, the solution must then *automatically* transfer the entire file to the series that is the successor. This means therefore that the entire file and all records and associated documents change affinity from one series to another automatically. Before the status of the overlap period is set to closed, a check must be made to ensure that there are no more open files left. If there are, the files must either be finalised or transferred manually to the successor. It must be possible to transfer all open files in a single automated process.

Although it is not permitted to link new files to a finalised series, it must be possible to move finalised files to such a series. If an overlap period is not used (e.g. in connection with the periodisation of personal files), it may be appropriate to create an empty series with the status of a closed period. The personal files can then be moved there on an ongoing basis as they become non-current.

Files can be moved to a finalised series manually, i.e. the link to the series is altered for each file. However, there should also be a function for moving a group of files to a finalised series as a single entity. This could for example be carried out for all files that have been found through a search based on certain criteria.

The use of periodisation, particularly with overlap periods, is not relevant for all types of solution. For ordinary case records systems, it is however obligatory to have such functionality. For some, only sharp period divides will be relevant. In such cases, all requirements concerning overlap periods will cease to apply.

Req. no.	Functional requirements for periodisation	Type	Remarks
5.11.3	It must be possible to link newly created files to a series that contains an active fonds period.	O	
5.11.4	A series that contains an overlap period must be blocked for the addition of newly created files. However, existing files in an overlap period must be open to new records.	O	
5.11.5	If a new record is added to a file that belongs to a series in an overlap period, the file must automatically be transferred to the series's successor.	O	
5.11.6	A series that contains a closed fonds period must be blocked for the addition of new files. All files must be finalised, so that no records or documents can be added either.	O	
5.11.7	It should be possible to finalise a series in an overlap period if it still contains open files.	V	
5.11.8	It must be possible to obtain an overview of files that are still open in an overlap period.	O	
5.11.9	It must be possible to transfer open files from a series in an overlap period to the series's successor.	O	
5.11.10	It should be possible to transfer in a single, automated process.	V	
5.11.11	It must be possible to move finalised files to a series that contains a closed period.	B	Obligatory for function for periodisation

Req. no.	Functional requirements for periodisation	Type	Remarks
5.11.12	It must be possible to move a group of finalised files to a series that contains a closed period in an automated process.	B	Obligatory for general case records.
5.11.13	If the documents in a series are not electronic (physical), it must also be possible to record the storage location.	O	

5.12 Transfer to repository

Transfer means the transfer of archival material from a fonds creator to an archive repository. Public bodies must transfer archival material for which a preservation decision has been taken. The main rule is that the material must be transferred 25 years after it was created, because it is then considered to no longer be in normal administrative use. Transfer involves the right of disposal over the material being transferred from the fonds creator to the archive repository. The archive repository will be responsible for maintaining the material in future and for making it available to users.

The transfer of physical fonds involves moving them from one storage location to another. The transfer of electronic archive material means that a *transfer export* is produced which consists of metadata and documents and that a copy of this export is sent to the archive repository. In most cases, electronic archive material will first be transferred as a *deposit.* Its status will later change automatically to transfer when it is 25 years old. Upon deposition, the right of disposal concerning the material will remain with the fonds creator. In the case of transfer, the archive repository will take over the right of disposal. The distinction between transfer and deposition is entirely based on this right of disposal, and therefore also on the responsibility for all use of the solution. The technical and documentation requirements that are imposed on transfer exports are however identical for both deposition and transfer.

The arrangement with deposition before transfer has been established to ensure that transfer exports are prepared while the solutions are still in operational use. The reason why such early transfers of material are not also formalised as transfers is that the fonds creator must remain responsible for serving both himself and his own users. The archive repository cannot normally take over responsibility for the management of active solutions. The fonds creator can therefore not delete deposited material until it has been given the status “transferred”.

The change in status from deposition to transfer will in normal cases take place when the youngest part of the material is 25 years old. If the transfer export consists of year-based files, this change can take place gradually as each individual year reaches 25 years of age, where practicable.

Upon transition from deposition to transfer, it may be necessary to produce and transfer a new transfer export. This will be relevant if the information in the export has been corrected in the production system concerned during the deposition period, e.g. through disposals being carried out or through changes being made in the screening of metadata or documents. It is however assumed that the preparation of a data export for archiving will be organised so that it only covers closed parts or periods from the solution concerned.

It is the responsibility of the fonds creator concerned to respond to enquiries concerning the material while it is being stored by the archive repository with the status "Deposited".

No distinction is made between deposition and transfer in this section. References to transfer here also cover deposition.

Metadata for transfer

In connection with the production of a transfer export, metadata must be generated concerning the transfer. These metadata must be transferred in a separate file.

The requirements below are obligatory for all Noark solutions which contain documents that must be preserved for more than 10 years.

No.	Name	Type	Occ.	Trans.	Remarks
M606	responsibleExport	B	One	A	
M607	exportedDate	B	One	A	
M608	numberofFilesExported	B	One	A	
M609	numberofRecordsExported	B	One	A	
M610	numberofDocumentsExported	B	One	A	
M708	checksumMetadata	B	One	A	
M709	checksumTransfer	B	One	A	
M706	checksumAlgorithm	B	One	A	

General requirements for transfer exports

General requirements concerning the metadata that transfer exports must consist of and how metadata and documents must be organised in such exports are defined in ISO 14571 OAIS (Open Archival System). These requirements will also form the basis for transfer exports from Noark 5. This means that transfer exports must constitute a *Submission Information Package* in accordance with OAIS. The Norwegian expression for this is *informasjonspakke for avlevering.*

The metadata elements that must be included in an export will be specified in the conceptual model for Noark 5 and the metadata directory. The structure of the transfer is defined in the National Archival Services of Norway's XML form for transfer from Noark 5 cores, whilst valid formats for the documents (archival formats) are defined in the *Regulation pursuant to the Archives Act of 1 December 1999 No. 1566 concerning supplementary technical and archival provisions regarding the handling of public fonds, Chapter VIII.* This Regulation also contains other requirements concerning transfer exports, e.g. concerning the organisation of files in the export.

The requirements below are obligatory for all Noark solutions which contain documents that must be preserved for more than 10 years.

Req. no.	General requirements for transfer exports	Type	Remarks
5.12.1	It must be possible to produce transfer exports consisting of metadata and documents.	B	Obligatory where transfer to an archive repository may be relevant.
5.12.2	The transfer export must constitute a Submission Information Package, as defined in ISO 14571 OAIS.	B	Obligatory where transfer to an archive repository may be relevant.
5.12.3	The format of the metadata component of the transfer export must be XML (XML 1.0).	B	Obligatory where transfer to an archive repository may be relevant.
5.12.4	The character set for the metadata element of the transfer export must be UTF-8.	B	Obligatory where transfer to an archive repository may be relevant.
5.12.5	Metadata elements that do not have a value must be omitted from the transfer export. In other words, the export must not contain empty elements with only start and end tags.	B	Obligatory where transfer to an archive repository may be relevant.
5.12.6	The structure and content of the metadata components of the transfer export must follow the National Archival Services of Norway's XML form for transfer from Noark 5 cores (separate appendix).	B	Obligatory where transfer to an archive repository may be relevant.
5.12.7	Alphanumeric values in the transfer export must be represented using an XML Form – data type string.	B	Obligatory where transfer to an archive repository may be relevant.
5.12.8	Dates without a time in the transfer export must be represented using an XML Form – data type date.	B	Obligatory where transfer to an archive repository may be relevant.
5.12.9	Dates with a time in the transfer export must be represented using an XML Form – data type dateTime.	B	Obligatory where transfer to an archive repository may be relevant.

Req. no.	General requirements for transfer exports	Type	Remarks
5.12.10	The format of documents in the transfer export must be one of the archival formats defined in the *Regulation pursuant to the Archives Act of 1 December 1999 No. 1566 concerning supplementary technical and archival provisions regarding the handling of public fonds, Chapter VIII.*	B	Obligatory where transfer to an archive repository may be relevant.
5.12.11	The organisation of the files in the transfer export must follow the *Regulation pursuant to the Archives Act of 1 December 1999 No.* 1566 concerning supplementary technical and archival provisions regarding the handling of public fonds, Chapter VIII.	B	Obligatory where transfer to an archive repository may be relevant.

The scope of a transfer export

The scope of a transfer export from case records must be determined by the content of a finalised series. All documents and metadata that are linked to the series must be included in the export. If the documents are physical, the export will only consist of metadata. All metadata marked with "To be transferred" in the metadata tables must be included in the export if they have a value, i.e. they are not empty. Record units that do not have documents linked to them must also be included in the export. This applies for example to classes that do not contain files (unused archive codes) and also to files that are removed due to incorrect record or the transfer of records to other files.

The export must only contain documents in archival format. If the document has been archived in several versions, all the document versions must be included. The same applies if the document has been archived in several variants.

Documents that have been disposed of before the export is produced must not be included. However, the metadata concerning these documents down to the document description level must be included.

As an alternative to an export of entire series, it should also be possible to produce exports based on a start date and end date, e.g. createdDate for a file. Exports with a scope based on all records during a given period are most relevant to certain task systems. Such exports will then be dependent on the affinity to series.

The requirements below are obligatory for all Noark solutions which contain documents that must be preserved for more than 10 years.

Req. no.	Requirements for the scope of a transfer export	Type	Remarks
5.12.12	A transfer export from electronic case records must consist of all metadata marked "To be transferred" and all documents in archival format in a finalised series.	B	Obligatory where transfer to an archive repository may be relevant.

Req. no.	Requirements for the scope of a transfer export	Type	Remarks
5.12.13	A transfer export from physical case records must consist of all metadata marked "To be transferred" in a finalised series.	B	Obligatory where transfer to an archive repository may be relevant.
5.12.14	All archived document versions in the finalised series must be included in the export.	B	Obligatory where transfer to an archive repository may be relevant.
5.12.15	All archived document variants in the finalised series must be included in the export.	B	Obligatory where transfer to an archive repository may be relevant.
5.12.16	Documents that have been disposed of when the export is produced must not be included. However, metadata concerning discarded documents down to document description level must be included.	B	Obligatory where transfer to an archive repository may be relevant.
5.12.17	It should be possible to produce a transfer export based on a start date and end date.	V	

Requirements concerning the contents of an information package for transfer

OAIS groups the contents of an information package into four main parts:

- *Content Information*: The content – or message – of the documents themselves. It is the documents that are subject to preservation and they must be preserved with their integrity and authenticity maintained. Content information will usually consist of text, but it could also consist of drawings, pictures, sound or video.

- *Preservation Description Information*: The most important group with metadata. Subdivided into the following subgroups:
  - *Reference Information*: Unique identification of the documents and metadata. All fonds units must be identified with a systemID.
  - *Provenance Information*: Documentation concerning the origin of the archive documents, e.g. the fonds creator who created them. Metadata linked to the fonds units "fonds" and "series" contain such information.
  - *Context Information*: Documentation of the archive documents' link to their surroundings. Examples of such information are the link to the activity (the process) that created the document, when the document was created and who created it. Relations between different fonds units, e.g. the archive documents that belong under a single common file, also constitute context information. Metadata concerning context can be found in most fonds units, but especially in class, file and record.
  - *Fixity Information:* Metadata which guarantee that the document's authenticity and integrity has been maintained, i.e. that the document is genuine and has not been altered

since it was archived. All documents must be given a checksum and a checksum must also be generated for the metadata.

- *Packaging Information*. This is general information that links together all digital objects in the package. The most important aspect here is the reference between the metadata and the documents.

- *Descriptive Information*: These are metadata that are included in search and retrieval tools used by the fonds creator (e.g. in Asta systems), which the archive repository itself adds after transfer. It will often be possible to extract these metadata from the preservation description information, e.g. name of classification value or file description ("case title"). Two reports also form part of a transfer: ongoing report and public registry. The archive repository can publish these as retrieval aids.

In order for it to be possible to interpret digital objects (both documents and metadata), *representation information* is also needed. This is also called *technical metadata.* Technical information can be linked to the document object, e.g. information on the document's format. Many technical metadata are not included in Noark 5, as it is considered that much of the data will be widely known and documented elsewhere (Knowledge Base). This concerns the detailed documentation of the various document formats for example. As regards the metadata, the structure of these is documented as an XML form which follows as a separate appendix.

The requirements below are obligatory for all Noark solutions which contain documents that must be preserved for more than 10 years.

Req. no.	Requirements concerning the content of an information package	Type	Remarks
5.12.18	Each document in archival format must be exported as a file in the transfer export. Different document versions and document variants are exported as separate files.	B	Obligatory where transfer to an archive repository may be relevant.
5.12.19	For each document, there must be a document object that contains a unique reference to the document file.	B	Obligatory where transfer to an archive repository may be relevant.
5.12.20	The document object must contain a checksum that is generated on the basis of the content of the associated document. The algorithm that was used to generate the checksum must also be documented.	B	Obligatory where transfer to an archive repository may be relevant.
5.12.21	A checksum must also be generated for all metadata in the transfer export.	B	Obligatory where transfer to an archive repository may be relevant.

Req. no.	Requirements concerning the content of an information package	Type	Remarks
5.12.22	Metadata for the entire fonds structure must be exported as a file. If this file becomes very large, the XML form for export will open as several files.	B	Obligatory where transfer to an archive repository may be relevant.
5.12.23	The change log must be exported as a separate file.	B	Obligatory where transfer to an archive repository may be relevant.
5.12.24	Public registries (section 4.3.6.2) and ongoing registries (ap. 4.3.6.3) must be included in the transfer. These reports must be selected within the same time period as fondsperiodStartDate and fondsperiodEndDate in the finalised series.	B	Obligatory where transfer to an archive repository may be relevant.

Comparison with the transfer format in Noark 4

In Noark 4, structured data were to be transferred as a *table export* in XML format. Each table – as specified in the technical part of the specification of requirements – was to be exported to its own file. The table exports were to contain most attributes in Noark 4. No distinction was made between metadata and system data. The number of table exports would vary from solution to solution and the way in which the solution was implemented. The specification of requirements in Noark 4 consisted of 95 tables, of which 39 contained obligatory attributes. A separate file called NOARKIH.XML would document the tables and attributes that were included in the exports. The *documents* were to be exported as individual files, and the references between the table exports and the documents were to be included as an attribute in the DOCVERSION table.

The general idea behind this transfer format was that data could be imported into a distribution solution that was built around a similar data model to that of the original production solution. However, in practice, this proved to be difficult to implement, because the table exports often contained inconsistent data which rendered importing impossible. Table exports are therefore not used in Noark 5.

The transfer also contained another type of export, known as a *report export.* Report extracts were to cover the same cases and registry entries as table exports, but they were to be structured as hierarchical (nested) XML files. Data was to be sorted and collated in the same way as can be done in a report (extract), hence the name "report export". In Noark 4, two such files were to be included in any transfer to a repository: *Chronological (ongoing) registry* and *Case and document summary.* The same information was therefore to be transferred to a repository in two main formats: table export and report export. The new transfer format in Noark 5 is based partly on the structure in Case and document summary.

5.13 Administration of the core

This section contains Noark 5 core's requirements for the system administration of the Noark 5 core. The requirements are intended to enable registry administrators to administer and maintain control over the fonds, the fonds structure and the metadata that belong to the record

units in the structure, i.e. to enter master data such as types of files and records and the metadata over and above the obligatory metadata that can be added to these data.

It will also provide opportunities for troubleshooting over and above that which would otherwise be permitted under the rules for alteration and freezing of metadata and documents in the solution.

The solution must also enable administrators to maintain control over the archival documents and the formats in which these documents are stored, i.e. it must enable them to implement established rules for when conversion is to take place.

Req. no.	Requirements for administration of the core	Type	Remarks
5.13.1	There must be a service/function for administration of the core.	O	
5.13.2	At least one user must be defined as a registry administrator, who can explicitly log on to the Noark 5 core in order to alter the configuration and global parameters.	O	
5.13.3	There must be a service/function for creating, editing and deleting fonds units (fonds, series, classification system, class, file, record, document description and document object) and associated metadata. Such records must be logged.	O	
5.13.4	Fonds and the fonds' metadata must only be created through the Administrator function for Noark 5 core.	O	
5.13.5	A *Subrecord* must only be defined and altered through the Administrator function for Noark 5 core.	O	
5.13.6	A *series* and the series's metadata must only be created through the Administrator function for Noark 5 core.	O	
5.13.7	A *Classification system* and the classification system's metadata must only be created and altered through the Administrator function for Noark 5 core.	O	
5.13.8	There must be a service/function which enables the registry administrator to go beyond the role-based access restrictions that are defined in the solution.	O	
5.13.9	It should be possible to use parameters to specify that the status "Document has been finalised" is to be automatically set to *Document description* in connection with other statuses of *File* or *Record.*	V	
5.13.10	It must be possible to specify parameters to ensure that only authorised units, roles or people have the right to archive a new version of a document on a *Record* with the status "Dispatched", "Registered" or "Finalised".	O	

Req. no.	Requirements for administration of the core	Type	Remarks
5.13.11	It must be possible to specify parameters to ensure that only authorised roles, units and people can delete inactive versions, variants and formats of a document.	O	

5.13.1 Conversion to archival format

Metadata for conversion to archival format

Metadata for conversion to archival format are grouped into metadata for document object.

No.	Name	Type	Occ.	Trans.	Remarks
M615	convertedDate	B	One	A	Obligatory when conversion has been performed.
M616	convertedBy	B	One	A	Obligatory when conversion has been performed.
M703	previousFormat	B	One	A	Obligatory when conversion has been performed.
M704	previousFormatDetails	V	One	A	

Requirements for conversion to archival format

Req. no.	Requirements for conversion to archival format	Type	Remarks
5.13.12	There must be a service/function which enables registry administrators to specify which document formats are defined as archival formats.	O	
5.13.13	There must be a service/function which enables registry administrators to set up rules for when (which statuses) archival documents must be converted to archival format.	O	
5.13.14	It must be possible to specify parameters to determine whether documents should be converted to archival format when the status of document description is set to “Document has been finalised”.	O	
5.13.15	It must be possible to specify parameters to determine whether all or specifically marked versions should be converted to archival format.	O	

Req. no.	Requirements for conversion to archival format	Type	Remarks
5.13.16	There must be a service/function and reporting for file format testing of the documents that are stored in the core. The report should give an overview of the files, records and/or document descriptions that do not contain documents stored in an approved archival format.	O	

Metadata for change log

Metadata for change log must be transferred as a separate file. These metadata must therefore not be grouped together with the other metadata. The change log must therefore have a reference to the record unit to which it belongs and the metadata that have been altered.

No.	Name	Type	Occ.	Trans.	Remarks
M680	referenceRecordunit	B	One	A	
M681	referenceMetadata	B	One	A	
M682	changedDate	B	One	A	
M683	changedBy	B	One	A	
M684	previousValue	B	One	A	
M685	newValue	B	One	A	

5.13.2 Deleting versions, variants and formats

An important requirement in Noark 5 is that it must not be possible to delete archived electronic documents. Controlled deletion must only be performed by authorised users in connection with disposal; see section 4.2.10 Preservation and disposal.

Documents can also be deleted by authorised users if they have been formally transferred to an archive repository; see section 4.2.12 Transfer. It is stressed that this latter rule only applies to transferred documents, not to documents that have only been deposited in the archive repository.

If a document is archived in more than one version, it must be possible to delete the older versions. Normally only the most recent, finalised version will be archived. However, it may also be appropriate to archive previous versions if they have documentation value. This could for example be the case if a manager has made significant changes to a draft prepared by an executive officer. The executive officer's draft can then be archived as a previous version of the finalised document. This will provide additional documentation concerning the case handling sequence. If previous versions have been archived unnecessarily, it must be possible to tidy up the archive effectively. Such tidying up must always be carried out before a transfer export is produced.

Metadata for deletion of documents

Metadata for deletion of documents must be grouped into metadata for document description.

No.	Name	Type	Occ.	Trans.	Remarks
M089	deletiontype	B	One	A	Obligatory when deletion has been carried out.
M613	deletedDate	B	One	A	Obligatory when deletion has been carried out.
M614	deletedBy	B	One	A	Obligatory when deletion has been carried out.

Req. no.	Requirements for the deletion of documents	Type	Remarks
5.13.17	Authorised users must be able to delete an archived inactive document version. It must not be possible to delete the most recent, final version.	O	
5.13.18	It must be possible to search for and retrieve documents that have been archived in several versions.	O	
5.13.19	It should be possible to carry out the deletion of many inactive document versions simultaneously, e.g. all inactive document versions that have been found following a search.	V	
5.13.20	Deletion of archived inactive document versions must be logged.	O	

If the original document has content which must be screened, a variant can be created from which information which is to be screened has been removed. In this way, the document can still be made publicly available.
Such variants can be deleted if they are no longer needed. It may be appropriate to transfer document variants, so deletion must be assessed in each individual case. Variants that have not been deleted when the transfer export is produced must be transferred.

Req. no.	Requirements for deletion of documents	Type	Remarks
5.13.21	Authorised users must be able to delete an archived document variant. It must not be possible to delete the original document.	O	
5.13.22	It must be possible to search for and retrieve archived document variants.	O	

Req. no.	Requirements for deletion of documents	Type	Remarks
5.13.23	It should be possible to delete many document variants simultaneously, e.g. all document variants that have been found following a search.	V	
5.13.24	Deletion of archived document variants must be logged.	O	

All documents that are to be transferred must be converted to archival format. The original production format can then be routinely deleted. Some users will probably wish to retain the production format for the time being, e.g. because they need to re-use text in an office support tool. How long this will be appropriate for will be up to each individual user to decide. There is no requirement for the production formats to be deleted before the transfer export is generated, because this will only include documents in archival format. However, many users will still have a need to go through and delete older production formats efficiently.

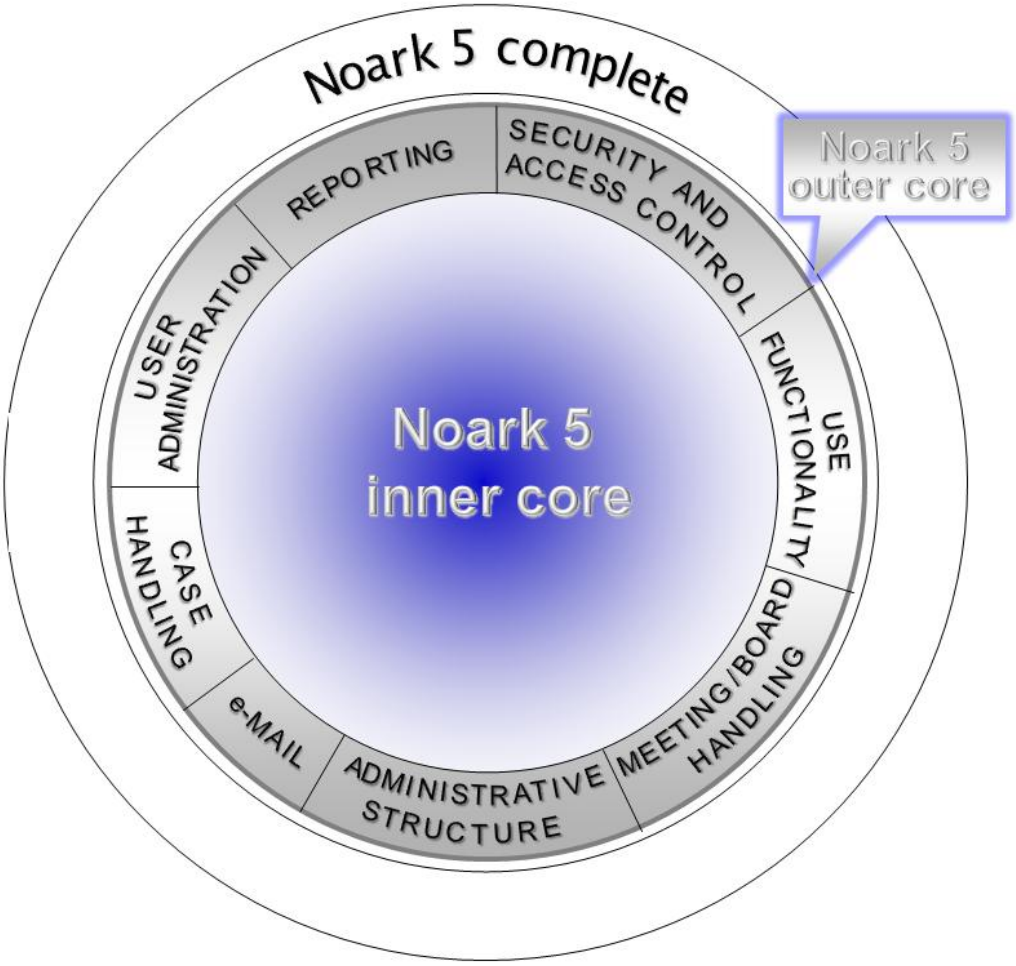
Req. no.	Requirements for deletion of documents	Type	Remarks
5.13.25	It must be possible to delete an archived document in production format if the document has been converted to archival format. It must not be possible to delete the document in archival format.	O	
5.13.26	It must be possible to search for and retrieve documents archived in production format.	O	
5.13.27	It should be possible to delete many production formats simultaneously, e.g. all production formats variants that have been found following a search.	V	
5.13.28	Deletion of archived production formats must be logged.	O	

6 Noark 5 outer core

Noark 5 core requirements for external (optional) solutions

Noark 5's core is dependent on interacting with various pre-systems implemented according to the needs of the individual organisation or supplier. In order for Noark 5 to function in an integrated archive system environment, it must be possible to integrate Noark 5 with a number of pre-systems/task systems which must be implemented in order to supplement a recordkeeping and archive solution. This section therefore sets out guidelines and requirements for the various task systems or pre-systems which can be freestanding solutions in relation to Noark 5. These requirements must be considered as part of the Noark 5 core requirements and must be fulfilled in order for a system solution to be approved as a Noark 5 solution.

It is important to note that a subdivision into Noark 5 inner core, outer core and complete will not necessarily mean that solutions have these as technically defined layers. This is a logical subdivision, not a technical one. The inner core is archived, regardless of where metadata are stored. The outer core consists of the requirements that the archive, the recordkeeping, imposes on any system that is to interact with the archive (to the degree that is appropriate). The functionality need not be contained within a technical layer between a technically defined core and an outer environment.



Noark 5 core does not have its own defined user interface. All case handling, including all tasks linked to recordkeeping that are performed by users of the solution, must therefore be

carried out from a pre-system. In order for recordkeeping to take place appropriately, the core must therefore impose certain requirements concerning how this should take place from the pre-systems.

In Chapter 5 on the inner core, requirements were set out which enable recordkeeping to take place. These are general requirements which enable files, records, document descriptions, etc. to be created and assigned metadata. This section clarifies and delimits the general requirements, so that controlled recordkeeping can take place from any pre-system.

The requirements for case handling with respect to Noark 5 core are therefore minimum requirements. Suppliers and users are free to define and develop functions which extend beyond the obligatory requirements.

6.1 Integrity requirements for the freezing of metadata and documents

Basic requirements for archival documents are that they must be preserved with their authenticity, reliability, integrity and usability maintained. Metadata which provide information on each archival document, which link it to the action that created it (as required in accordance with Chapter 5), are a basic requirement to ensure this. A further basic requirement is that metadata and documents are protected from changes where necessary.

The requirements in this section set out the minimum requirements as regards which metadata must be frozen in connection with which statuses of *file, record* and *document description*, and the preconditions for users being permitted to finalise these. Freezing of the document itself is an important part of this. This section therefore focuses on what must be frozen and when.

Nevertheless, these requirements alone cannot be governing for what all users should be permitted to do in a Noark solution. They must be seen in connection with the requirements for authorisations and the structure of roles and role profiles in Chapter 12.

Req. no.	Requirements for the freezing of metadata for *File*	Type	Remarks
6.1.1	There must be a service/function for finalising a *Basic file* i.e. setting *finalisedDate*).	O	
6.1.2	For a *Basic file* that has been finalised, it must not be possible to alter the following metadata: • title • documentmedium • referenceParent • referenceChild • referenceFondssection	O	
6.1.3	There must be a service/function for setting the Status of a *Case file.*	B	Obligatory for case records.

Req. no.	Requirements for the freezing of metadata for *File*	Type	Remarks
6.1.4	The following status values are obligatory for *Case file*: • Being processed • Finalised • Dismissed	B	Obligatory for case records.
6.1.5	The following status values are recommended for *Case file*: • Created by executive officer • Finalised by executive officer • Exempt from process management	V	
6.1.6	When the status of *Case file* is set to Finalised, finalisedDate must be set automatically.	B	Obligatory for case records.
6.1.7	It must not be possible to finalise a *Case file* unless a primary classification (*Class*) has been specified.	B	Obligatory for case records.
6.1.8	It must not be possible to finalise a *Case file* that contains *Records* that have not been finalised.	B	Obligatory for case records.
6.1.9	It must not be possible to finalise a *Case file* that contains *Records* that have not been depreciated.	B	Obligatory for case records.
6.1.10	It must not be possible to finalise a *Case file* in a series for electronic documents if it contains *Records* that are not linked to electronic documents.	B	Obligatory for case records.
6.1.11	It must not be possible to finalise a *Case file* unless all main documents for the records in the file are stored in archival format.	B	Obligatory for case records.
6.1.12	It must not be possible to finalise a *Case file* unless all back log in *Records* have been depreciated.	B	Obligatory for case records.
6.1.13	When the status of a *Case file* is set to finalised, it must not be possible to alter the following metadata at file level: • casedate • administrativeUnit • case-responsible	B	Obligatory for case records.
6.1.14	When the status of a *Case file* is set to finalised, it must still be possible to alter the other metadata for *Case file*. Changes must be logged.	B	Obligatory for case records.
6.1.15	It must be possible for authorised roles and persons to open a finalised *Case file*. It must be possible to specify parameters to determine who is authorised to open a file. The opening of files must be logged.	B	Obligatory for case records.

Req. no.	Requirements for the freezing of metadata for ***File***	Type	Remarks
6.1.16	When the status of a *Case file* is set to finalised, the status of all *Document descriptions* in the file must be set to the status "Document has been finalised".	B	Obligatory for case records.
6.1.17	It must not be possible to delete a *Basic file* that has been finalised.	B	Obligatory for case records.
6.1.18	It must not be possible to delete a *Case file* which currently contains or which has contained *Registry entries* with the status "Dispatched", "Registered" or "Archived".	B	Obligatory for case records.

Req. no.	Requirements for the freezing of metadata for ***Record***	Type	Remarks
6.1.19	There must be a service/function for archiving a *Record* (i.e. setting *archivedDate*).	O	
6.1.20	For a *Simplified record* that has been archived, it must not be possible to alter the following metadata: • referenceParent • referenceFondssection • referenceDocumentdescription • referenceDocumentobject	O	
6.1.21	For a *Basic record* that has been archived, it must not be possible to alter the following metadata: • title • documentmedium	O	
6.1.22	When a *Basic record* has been archived, it must still be possible to alter the other metadata under *Basic record.* Changes must be logged.	O	
6.1.23	There must be a service/function for setting the Status of a *Record* (Registry entry).	B	Obligatory for case records.

Req. no.	Requirements for the freezing of metadata for *Record*	Type	Remarks
6.1.24	The following status values are obligatory for *Registry entry*: • Dispatched • Registered (Document has been registered and the record has been quality-assured) • Archived (processing has been finalised, a paper document has been placed in the case file/electronic document finalised) • Dismissed (the document has been incorrectly registered and is being dismissed) • Finalised by executive officer • Approved by manager	B	Obligatory for case records.
6.1.25	The following status values for *Registry entry* are recommended: • Temporary record of incoming document • Executive officer has registered incoming document • Reserved document, i.e. an inhouse-produced document is being worked on.	V	
6.1.26	When the status of *Registry entry* is set to Archived, archivedDate must be set automatically.	B	Obligatory for case records.
6.1.27	It must not be possible to delete a *Record* with the status "Archived", "Registered" or "Dispatched".	B	Obligatory for case records.
6.1.28	It should not be possible to delete a *Record* with the status "Finalised by executive officer" or "Approved by manager".	V	
6.1.29	It must be possible to specify *Registry entry* with different values of registry entry type.	B	Obligatory for case records.
6.1.30	Obligatory registry entry types must be: • incoming document • -{}-outgoing document • -{}--{}--{}-internal memo for follow-up • internal memo without follow-up • case draft	B	Obligatory for case records.
6.1.31	For *Registry entry* of incoming documents with the status "Registered", alteration of the following metadata must not be permitted: • serialnumber • receiveddate	B	Obligatory for case records.

Req. no.	Requirements for the freezing of metadata for *Record*	Type	Remarks
6.1.32	For *Registry entry* of incoming documents with the status archived, alteration of the following metadata for *Registry entry* must not be permitted: • registryentrytype • registrydate • documentDate • client It must be possible for authorised personnel to alter all other metadata. It must be possible to specify parameters to set roles, units, groups or people who are to be authorised. Changes must be logged.	B	Obligatory for case records.
6.1.33	For *Registry entry* of inhouse-produced documents (outgoing documents, internal documents for follow-up, internal documents without follow-up) with the status "Dispatched", "Registered" or "Archived", it must not be possible to alter the following metadata for *Registry entry*: • serialnumber • registryentrytype • documentDate • sentDate • executiveofficer • administrativeUnit • title • client It must be possible for authorised personnel to alter all other metadata. It must be possible to specify parameters to set roles, units, groups or people who are to be authorised. Changes must be logged.	B	Obligatory for case records.
6.1.34	It must be possible to alter (reverse) the status of a *Registry entry* after the status has been set to "Dispatched", "Registered" or "Archived". However, when the status is reversed, alteration of the following metadata only is permitted: • title Changes must be logged.	B	Obligatory for case records.
6.1.35	For the *Record* of incoming documents with the status "Temporarily registered" or "Registered by executive officer", it must be possible to change all metadata for record.	V	

Req. no.	Requirements for the freezing of metadata for *Record*	Type	Remarks
6.1.36	For the *Record* of inhouse-produced documents (registry entry type "outgoing document", "internal document for follow-up", "internal document without follow-up") with the status "Registered by executive officer" and "Finalised by executive officer", it should be possible for authorised personnel to alter all metadata. It should be possible to specify parameters to set roles, units, groups or people who are to be authorised. Changes must be logged.	V	
6.1.37	If a *Record* is marked as finalised, it must not be possible to add more *Document descriptions.*	O	
6.1.38	It must be possible to archive a new version of a document on a *Record* with the status "Dispatched", "Registered" or "Archived" without having to reverse the status.	B	Obligatory for case records.
6.1.39	When archiving a new version of a document on a *Record* with the status "Dispatched", "Registered" or "Archived", a *Remark* must be linked to the record with a statement of the reason.	B	Obligatory for case records.

Req. no.	Requirements for the freezing of documents and metadata for *Document description*	Type	Remarks
6.1.40	It must be possible to enter metadata for *Document description* automatically based on metadata from *Record* in connection with creation.	O	
6.1.41	It must be possible to register that a document is in paper form and where it is located.	O	
6.1.42	The following statuses for document description and document object are obligatory: • "Document is being edited" • "Document has been finalised"	O	
6.1.43	The status "Document has been finalised" under document description must be set automatically when *File* is finalised or *Record* is set to the status "Dispatched", "Registered" or "Archived".	O	
6.1.44	It must not be possible to make changes in a document for *Document description* with the status "Document has been finalised".	O	
6.1.45	It must not be possible to alter (reverse) the status "Document has been finalised".	O	

Req. no.	Requirements for the freezing of documents and metadata for *Document description*	Type	Remarks
6.1.46	For *Document description* with the status "Document has been finalised", it must be permitted to alter the title of the main document and appendices.	O	
6.1.47	In connection with the linking of a document to a *Record*, it must be possible to specify whether it is a main document or an appendix.	O	

6.2 Handling of case files

This section sets out requirements for a number of specialised functions that can be grouped under the collective term "case handling". These are functions linked to the handling or updating of defined metadata or groups of metadata in the core. They are therefore requirements for case handling functions which affect metadata in the core and must be transferred where they exist. This concerns requirements for case distribution, the splitting and merging of files, depreciation, handling of case parties and requirements for the record and use of precedents.

6.2.1 General requirements for handling of case files

Req. no.	General requirements for case handling	Type	Remarks
6.2.1	There must be a service/function for updating the *lending* of a *Case file*.	B	Obligatory for physical fonds.
6.2.2	It must be possible to link a handling log to a *Case file.*	B	Obligatory for case records.

6.2.2 Case distribution

Req. no.	Requirements concerning case distribution	Type	Remarks
6.2.3	There must be functions for obtaining information on undistributed *Records* (i.e. there is no *executive officer* for the registry entry).	B	Obligatory for case records.
6.2.4	There must be a service/function for distributing undistributed *Records.*	B	Obligatory for case records.

Metadata for case distribution

Metadata for case distribution are grouped into case file or registry entry.

No.	Name	Type	Occ.	Trans.	Remarks
M666	distributedTo	B	One	A	Obligatory when cases/registry entries are distributed.
M667	distributedBy	B	One	A	Obligatory when cases/registry entries are distributed.
M668	distributedDate	B	One	A	Obligatory when cases/registry entries are distributed.

6.2.3 Splitting and merging of files and moving of records

Noark 5 provides for the splitting or merging of files. In practice, this will involve moving one or several records in one file to another file. The need to do this may arise as a result of erroneous records or a case handling process that develops in several directions, or as a result of a different picture of the case handling process emerging over time than was originally anticipated. This is functionality which requires resources, accuracy and control. Strict requirements are therefore imposed on who is to have permission to carry out these actions.

Req. no.	Requirements concerning the splitting and merging of files and moving of records	Type	Remarks
6.2.5	There must be a service/function for moving a *Record* from one *File* to another *File.* Moving involves alteration of the metadata element *referenceParent* for the *Record.* The change must be logged.	O	
6.2.6	If *recordID* under *Basic record* in case records uses the recommended format yy/nnnnnn-nnnn (i.e. the combination of case number (*fileID*) and document number in the case), *recordID* should be altered automatically. The *record* should be automatically assigned the first available document number in the *File* to which it is being moved.	V	
6.2.7	*Records* that are not being moved in a *File* from which *Records* are being moved should not have their *recordID* altered.		
6.2.8	It should be possible to move several *Records* that are linked to the same *File* in a single operation.	V	
6.2.9	It must not be possible to move a *Record* if this *Record* depreciates or is depreciated by other *Records* that are not being moved. If an attempt is made to do this, the user must receive a message about the links that block movement.	B	Obligatory for case records.

Req. no.	Requirements concerning the splitting and merging of files and moving of records	Type	Remarks
6.2.10	Movement of archived *Records* must only be carried out by the role of Administrator.	O	
6.2.11	It should be possible to use parameters to enable others, particularly authorised users, to also have permission to move *Records.*	V	
6.2.12	It should be possible to use parameters to enable all users to move *Records* for which they themselves are the executive officer if the status is "Temporarily registered" or "Registered by executive officer".	V	
6.2.13	In connection with moving and renumbering, the user must be given reminders to alter the necessary references under physical documents in the archive.	B	Obligatory for physical fonds.

6.2.4 The sign off of records

A Registry entry of the type "incoming document" or "internal document for follow-up" will be in a back log list until it is marked as finalised or depreciated. This section sets out the requirements for sign off of records.

Metadata for the sign off of records

Metadata for the sign off of records must be grouped into metadata for registry entries. The sign off of records is obligatory for incoming documents and internal documents that are to be followed up and may occur on one or several occasions in a registry entry.

No.	Name	Type	Occ.	Trans.	Remarks
M617	signoffdate	B	One	A	Obligatory when the sign off is carried out.
M618	signedoffBy	B	One	A	Obligatory when sign off is carried out.
M619	signoffMethod	B	One	A	Obligatory when sign off is carried out.
M214	referenceSignoffsRegistryentry	B	Many	A	Obligatory when a document signs off another document.
M215	referenceSignoffedByRegistryentry	B	Many	A	Obligatory when a document signs off another document.

Req. no.	Requirements for the Sign off of records	Type	Remarks
6.2.14	There must be functions for obtaining information concerning back log.	B	Obligatory for case records.
6.2.15	There must be a service/function for signing off a *Record* (Registry entry).	B	Obligatory for case records.
6.2.16	It must be possible to sign off a registry entry with one or several (other) registry entries.	B	Obligatory for case records.
6.2.17	It must be possible for a registry entry to be signed off by several (other) registry entries.	B	Obligatory for case records.
6.2.18	When the status of a file is set to finalised, all records not signed off Registry entries of the type "incoming document" or "internal document for follow-up" that are linked to the file, are signed off with case finalised.	B	Obligatory for case records.
6.2.19	There must be functionality to enable the signing off of internal documents that are to be followed up to be performed separately for each individual recipient. This means that an internal document that has been received can be signed off for some recipients but not for others.	B	Obligatory for case records.
6.2.20	There must be a reference between an incoming document that is signed off by an outgoing document.	B	Obligatory for case records.
6.2.21	There must be a reference between a memo that is signed off by another memo.	B	Obligatory for case records.
6.2.22	Sign off must not be registered under CC addressees.	B	Obligatory for case records.

6.2.5 Parties to a case

One or more organisations or people can be linked to a case file as parties to a case (*case parties*). A party is the party at which a decision is aimed or which the case otherwise directly concerns. Case party in Noark 5 consists of information (name, address, etc.) which describes the parties in a case.

Information concerning Case parties is not obligatory in Noark 5 core. The requirements for Case parties are obligatory for solutions that involve parties. Information on Case parties is obligatory for transfer.

Metadata for *Case party (parties to a case)*

One or more organisations or people can be linked to a case file as *case parties.*
Metadata for case party must be grouped into metadata for case file. Case party is optional and may occur one or more times in connection with a case file. If there is more than one case party, the metadata must be grouped together on export and exchange.

Metadata for case party are included in the metadata structure for case file.

No.	Name	Type	Occ.	Trans.	Remarks
M010	casepartyID	V	One	A	
M302	casepartyName	B	One	A	Obligatory if case party is used.
M303	casepartyRole	B	One	A	Obligatory if case party is used.
M406	postaladdress	V	One	A	
M407	postcode	V	One	A	
M408	postaltown	V	One	A	
M409	foreignaddress	V	One	A	
M410	emailaddress	V	One	A	
M411	telephonenumber	V	One	A	
M412	contactperson	V	One	A	

Functional requirements for Case party

Req. no.	Requirements for Case party	Type	Remarks
6.2.23	It must be possible for a Case party to contain an arbitrary number of *Case parties.*	B	Obligatory for solutions which include parties.
6.2.24	There must be a service/function for updating *Case party* for a *Case file*.	B	Obligatory for solutions which include parties.
6.2.25	It must be possible to screen *Case party* entirely or partially.	B	Obligatory for solutions which include parties.

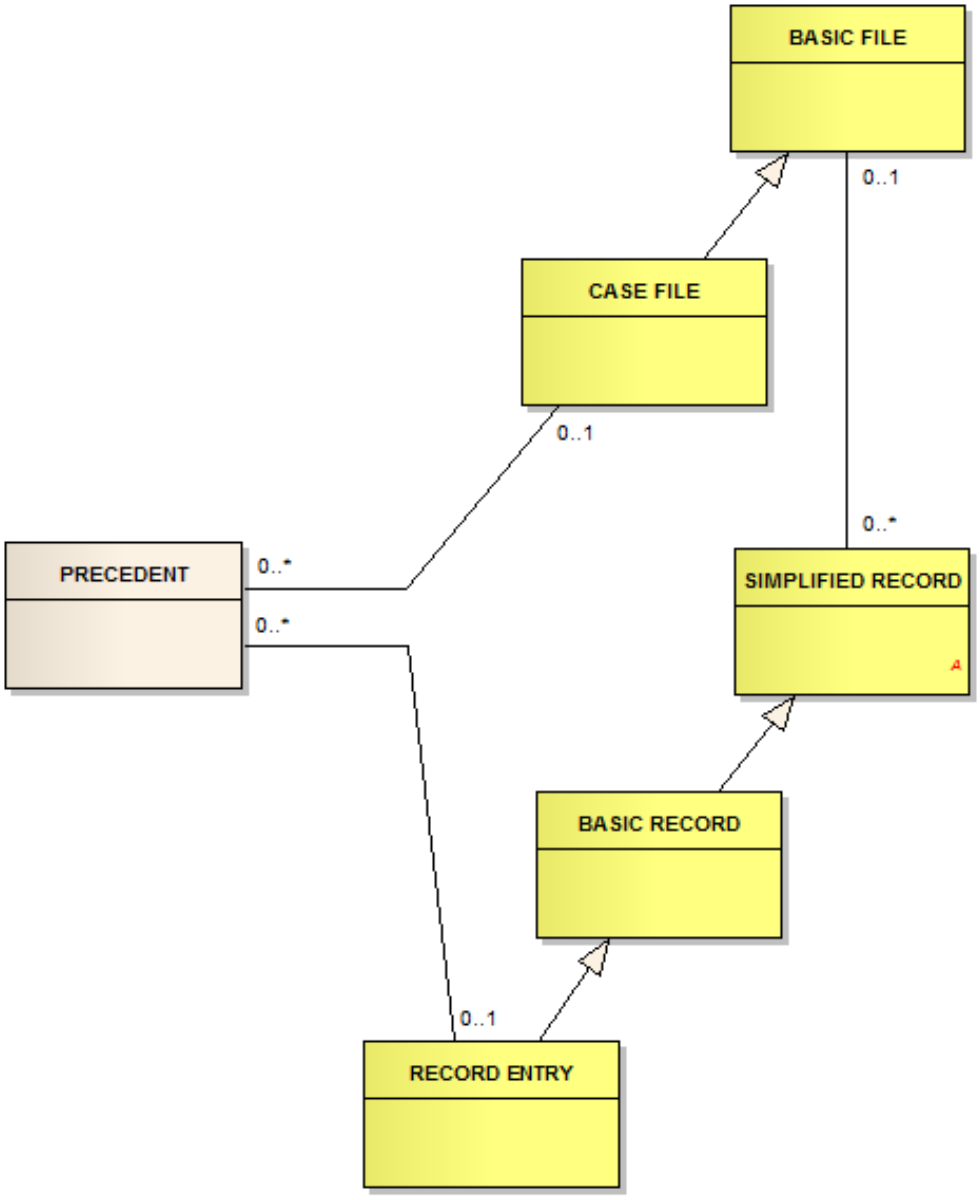
6.2.6 Precedent

"Precedent" means a (legal) decision which can subsequently act as a guide in similar situations or cases. A precedent can also be a case that is governing for the processing of other similar cases. This usually involves administrative resolutions, i.e. individual resolutions passed in accordance with the administrative area of the body concerned which contain a legal opinion that is subsequently used as a basis in other similar cases. It must therefore be possible for fundamental decisions linked to different case areas to be established in an appropriate manner and made available to executive officers.

We normally talk about precedent *cases*, but there are usually one or more documents in the case that form a precedent. In addition to registering the entire case, it must therefore be

possible to identify the document or documents that contain precedent decisions. If information concerning precedent has been registered, precedence is obligatory for transfer.

Conceptual model for Precedent



< Precedent>

Metadata for Precedent

Metadata for precedent must be grouped into metadata for case file or registry entry. Precedent is optional and may occur on one or more occasions.

No.	Name	Type	Occ.	Trans.	Remarks
M111	precedentDate	B	One	A	Obligatory when precedent is included.
M600	createdDate	B	One	A	Obligatory when precedent is included.
M601	createdBy	B	One	A	Obligatory when precedent is included.
M020	title	B	One	A	Obligatory when precedent is included.
M021	description	V	One	A	
M311	precedentAuthority	V	One	A	
M312	legalsourcefactor	B	One	A	Obligatory when precedent is included.
M628	precedentApprovedDate	V	One	A	
M629	precedentApprovedBy	V	One	A	
M602	finalisedDate	V	One	A	
M603	finalisedBy	V	One	A	
M056	precedentStatus	V	One	A	

Requirements for Precedent

Noark 5 facilitates the creation of a precedent register with references to Case files and Registry entries that form a precedent. The register is built up through the precedent metadata being linked to the fonds units (cases or registry entries) that create a precedent.

Req. no.	Requirements for Precedence	Type	Remarks
6.2.26	It should be possible to create a precedent linked to a case or a registry entry.	V	
6.2.27	It should be possible to create a register of the values from which precedentAuthority can be selected.	V	
6.2.28	It must be possible to register previous precedent, i.e. decisions that were taken before ICT-based solutions for recordkeeping and archiving were introduced.	B	Obligatory for solutions which include precedents.
6.2.29	It must be possible to identify the registry entry or entries in a case file that contain the precedent decision.	B	Obligatory for solutions which include precedents.
6.2.30	Record, alteration and access to precedents must be controlled by access rights.	B	Obligatory for solutions which include precedents.

Req. no.	Requirements for Precedence	Type	Remarks
6.2.31	The following statuses for *Precedent* are obligatory: • "Current" • "Obsolete"	B	Obligatory for solutions which include precedents.
6.2.32	It must not be possible to delete obsolete precedents.	B	Obligatory for solutions which include precedents.
6.2.33	It must not be possible to delete a precedent.	B	Obligatory for solutions which include precedents.
6.2.34	It must be possible to establish a collective precedent overview in connection with the fonds structure.	B	Obligatory for solutions which include precedents.
6.2.35	There must be a service/function which makes it possible to obtain a complete overview of all precedents.	B	Obligatory for solutions which include precedents.
6.2.36	It must be possible to present the precedent decision in an official document or official variant.	B	Obligatory for solutions which include precedents.

6.3 Electronic communication

6.3.1 E-mail

There is an increasing need for organisations to be able to send and receive e-mail, files and documents that are automatically registered by the recipient, as this is both time- and labour-saving. In order to achieve this, an exchange format must be defined with requirements concerning the metadata that must be received from the sender in order for the recipient to automatically import it.

Electronic message exchange/exchange format

Exchange format is a set of metadata that is used to send e-mail and documents for automatic record by the recipient. The general requirements for e-mail and exchange format will be set out in this subsection.

General security requirements have been set up, but the requirements in Chapter *12 Security and* functions
also apply to exchange format. The rules in sections *4.2 The* record structure
and *0 An* of archive. If the inner core is integrated with a task system, this will in many cases not be necessary systems is specialised case handling, where a *few activities* are repeated according to fixed routines. The number of documents that are received andgenerated high. In such cases, there may be a need for a simpler also apply to exchange format.

A precondition for the secure use of an exchange format is that the organisations that are to communicate with each other have entered into an agreement concerning this communication. Recipients and senders must be predefined before dispatch. Where necessary, the communication must be sent via secure lines. It must not be possible for unauthorised persons to have e-mail or documents registered automatically.
The organisations concerned must have special instructions with routines for how they decide to use the functions based on the exchange format.

The exchange format for this service/functionality is not yet in place. This will be set up in future versions of Noark 5, and requirements established for electronic message exchange via e-mail and fixed exchange format will be included in Noark 5.

6.3.2 Encryption and electronic signature

In the case of electronic communication, it is necessary to specify requirements for security. This involves requirements for encryption and electronic signatures, in addition to documentation of the security of documents that have been sent or received in electronic form. It must also be possible to specify requirements for security at different levels in the fonds structure.

Metadata for the verification of electronic signatures

Metadata for the verification of electronic signatures must be grouped into metadata for registry entry.

No.	Name	Type	Occ.	Trans.	Remarks
M507	electronicSignature Securitylevel	B	One	A	Obligatory when the verification of electronic signatures is performed.
M508	electronicSignature Verified	B	One	A	Obligatory when the verification of electronic signatures is performed.
M622	verifiedDate	B	One	A	Obligatory when the verification of electronic signatures is performed.
M623	verifiedBy	B	One	A	Obligatory when the verification of electronic signatures is performed.

Req. no.	Requirements for metadata for documents received or sent with an electronic signature	Type	Remarks
6.3.1	Electronic documents that are received in encrypted form must be decrypted upon receipt. The following metadata must be stored upon record: • Security level. Specified using text or codes, covering at least the following variants[10]: 1. Symmetrically encrypted, use of common password or key which is shared between the sender and receiver. 2. Sent with PKI/organisation certificate, third party which approves the organisation that is the sender. 3. Sent with PKI/"person standard" certificate, third party which accepts the person that is the sender. 4. Sent with PKI/"person high" certificate, strong authentication of sender. • Electronic signature, verification of irrefutability/non-deniability (that the content has not been altered/manipulated). Specified using text or codes which cover these variants: 1. Signature not added, nothing to verify 2. Signature has been added, but verification not performed 3. Signature has been added and verified	O	
6.3.2	When an electronic document is dispatched by an organisation in encrypted form, the following metadata must be stored with the record: • Security level. Specified using text or codes, covering at least the following variants: 1. Symmetrically encrypted 2. Sent with PKI/organisation certificate 3. Sent with PKI/"person standard" certificate 4. Sent with PKI/"person high" certificate • Indication as to whether an electronic signature has been added to an outgoing dispatch in order to be able to claim irrefutability/non-deniability.	O	

[10] Variants 2, 3 and 4 in this and subsequent references to "security level" are based on the specification of requirements for PKI in the public sector.

Req. no.	Requirements for metadata for documents received or sent with an electronic signature	Type	Remarks
6.3.3	At the following levels in the fonds structure, the fonds administrator should be able to specify the security level that is to be required and whether an electronic signature is to be required for incoming documents: • Fonds • Series • Classification system • File	V	
6.3.4	At the following levels in the fonds structure, the fonds administrator should be able to specify the security level that is to be used and whether an electronic signature is to be used in connection with the electronic sending of documents: • Fonds • Series • Classification system • File	V	
6.3.5	It must be possible to configure the Noark 5 solution so that all documents that are sent or received encrypted are stored in non-encrypted form in the fonds. (This is the main principle which most administrative bodies should be able to choose).	O	
6.3.6	It should be possible to configure the Noark 5 solution so that all documents that are sent or received encrypted are also stored in encrypted form in the fonds.	V	
6.3.7	If the solution allows documents to be stored in encrypted form, sufficient metadata must be stored to enable an authorised user to decrypt the document when required.	B	

6.3.3 Batch import

Case handling, document handling and document exchange are making use of an ever-increasing number of new channels. The fonds systems should not be a barrier to efficiency improvements in these areas, and it is also particularly important that the authenticity and integrity of documents is ensured. *Batch import* will enable several documents to be imported into the Noark 5 solution in a single sequence.

Documents can come in batches to the core in many ways, e.g.:

- a batch import from another Noark solution.
- a batch import from a document store.
- a batch import from a scanning system for example.
- a batch import from the files of an operating system.
- a batch import from a website.

Noark 5 must have the option of accepting these and must include solutions for handling the capture and maintenance of the content and structure of the imported documents.

In a batch import, the core must capture the same information as in a normal import, i.e. the document and its metadata.

Batch import must handle exceptions and errors. This could be relevant in connection with electronic consultation procedures, e.g. via web servers on the internet, document production in cooperation rooms, "case handling" with the e-mail system as an exchange channel or in other cases where relatively comprehensive document handling has taken place without the concurrent creation of an archive. For example, the Noark 5 solution could offer functionality where the user can select/highlight files that are located on one or more file servers, ftp servers or similar, in order to import them. The user must be able to link the files to a folder or a record in a particular folder. Alternatively, batch imports can for example be handled through a search engine, where the documents are linked to metadata and imported to a defined fonds unit in an automated process.

The following requirements for batch import are general and independent of tools and technology.

Batch import triggered from a pre-system

In the case of batch import triggered from a pre-system, it is the responsibility of the pre-system to organise the data and documents that are to be imported and to develop functionality that reads the underlying data and sends them as integration messages to Noark 5.

Requirement no.	Requirements for batch import triggered from a pre-system	Type	Remarks
6.3.8	Batch imports triggered from a pre-system must deliver integration messages to Noark 5 based on the structure and content specification for document capture in Noark 5 once this is in place in a future version.	V	

Batch import triggered from Noark 5 core

Requirement no.	Requirements for batch import triggered from Noark 5 core	Type	Remarks
6.3.9	The Noark 5 solution should contain batch import functionality that retrieves documents from a specified location and links them to classes, files, records or document descriptions.	V	

Requirement no.	Requirements for batch import triggered from Noark 5 core	Type	Remarks
6.3.10	In connection with batch imports, it should be possible to decide whether all imported documents should be linked to a single record unit at the same level in the fonds structure or whether each individual document should be linked to a different record unit in the fonds structure.	V	
6.3.11	In connection with batch imports, it should be possible to link imported documents to a pre-existing class, file, record or document description.	V	
6.3.12	In connection with batch imports, it should be possible to define and complete the metadata set for the documents that are to be imported, once only.	V	
6.3.13	The Noark 5 core should have automatic provision for capturing documents that have been generated and transferred from other systems.	V	
6.3.14	The Noark 5 core should have provision for handling input queues in connection with batch import. *Remarks: For the handling of input queues, it could for example be desirable to view the queues, pause one or more queues, restart one or all the queues or delete a queue.*	V	
6.3.15	The Noark 5 core should be able to automatically capture metadata linked to all the documents that are being transferred. It should be possible to override this in the event of missing or erroneous metadata.	V	
6.3.16	In the case of automated batch imports, there must be functionality for validating metadata and associated documents automatically, in order to ensure that data integrity is maintained.	B	Obligatory for function for automated batch import.
6.3.17	In connection with batch imports, it must be possible to import log information concerning the imported documents, and the log information must be included in the import as a separate document or documents.	B	Obligatory for function for automated batch import.
6.3.18	The Noark 5 solution must not import the log information in such a way that it becomes part of the Noark 5 solution's own log information. Imported log information must be archived separately, independently of the Noark 5 solution's own logs.	O	

Requirement no.	Requirements for batch import triggered from Noark 5 core	Type	Remarks
6.3.19	An administrator role must be defined in the Noark 5 solution which will be able to specify that imported records, series, classes, files and records are to be automatically set as finalised after importing. *Remarks: In the event of the merger of two or more organisations, it may be appropriate to finalise all or parts of the organisations' fonds.*	O	

6.3.4 Electronic form for completion via the internet

The public sector is in the process of establishing electronic self-service functions, where businesses and members of the public can perform and receive electronic services 24 hours a day, in what we call "24-hour electronic administration". A key tool in a self-service function is electronic forms for completion via the internet.

The *response data* from an electronic form should be considered as a document as understood in the Archives Act and must therefore be handled in the same way as other types of document that are received by the organisation, i.e. they should normally be registered and archived. Both parties and the public have the right to request access to information or documents concerning a case that has been received by the administrative body via electronic forms. In principle, people should therefore be able to see both the response data and the environment that the user saw when he or she completed the form. In order to protect legal rights and ensure traceability for the person who completed the electronic form, it must be possible to retrospectively retrieve an authentic representation of the data that were entered in the version of the form that was used during completion of the form.

An electronic form for completion via the internet can be *static*, so that all users completing the form are shown header texts, guideline information and response fields in the same way, in a fixed layout. In order to present a completed form of this type retrospectively, a PDF file for example could give a complete picture of the user interface in the data entry situation. However, electronic forms will increasingly be created as a *dynamic* screen dialogue. Electronic forms with a dynamic screen dialogue are characterised by having self-help texts which can be retrieved for each question, path options and greyed-out questions, where the person completing the form is guided past pages or questions that are irrelevant given his or her previous answers. These are recommendations in the ELMER2 guidelines for public sector web forms. Presenting a completed form of this type retrospectively requires the file and response data to be imported back into the original user environment.

Relevant archive data in connection with electronic form functions can be of one of three types in a Noark context:

- **The actual response data**
  The user's entries in free text fields and selections from single- or multiple-choice lists. Of importance in a Noark 5 context for example are fields for identifying the sender, applicant and parties.

- **Transaction information**
  Information on the actual transfer of data from the user's PC to the recipient system. Of importance in a Noark 5 context is the time of transfer to the task importer, which corresponds to the date of receipt of the form.
- **Fixed information for the individual form**
  This is information which has not been completed as response data and which is not naturally logged for transactions. In a Noark 5 context, this could typically be a description of the case circumstances (the case file) or the document (the registry entry), class, executive officer, case-handling unit, confidentiality and information concerning preservation/disposal.

In principle, the form solution can facilitate the complete document capture of response data from electronic forms and complete, automatic record, archiving and even distribution to the case-handling unit or person. However, it is therefore the form solution that determines the questions that are asked and thus which response data can be used automatically and which transaction data and fixed information are sent to the public body.

Requirement no.	Requirements for electronic form for completion via the internet	Type	Remarks
6.3.20	There should be functionality for retrieving both relevant response data and transaction information from electronic forms and entering them as a file, record, document description and document in an automated process.	V	
6.3.21	It must be possible to enter fixed information for an individual form type in addition to response data and transaction information.	B	Obligatory when 6.3.20 is fulfillled.
6.3.22	The total result data set from an electronic form must be stored together with relevant transaction information and fixed information for the form type in an approved archival format.	B	Obligatory when 6.3.20 is fulfillled.
6.3.23	It must be possible to choose which individual response data fields, transaction information and fixed information for an electronic form should be integrated in a Noark 5 core.	B	Obligatory when 6.3.20 is fulfillled.
6.3.24	Received form data must be archived in the form of a complete copy of the response data and completion environment in an approved archival format.	B	Obligatory when 6.3.20 is fulfillled.
6.3.25	For dynamic forms, information concerning the current version of the form and presentation software should be stored together with or as part of the result data set, incorporated in the version of the form that was used during completion of the form.	V	

6.3.5 Electronic document exchange

In this context, "electronic document exchange" means the exchange of individual documents between (Noark) solutions as part of the ordinary case handling.

Secure electronic document exchange between different Noark solutions and between different cooperating administrative bodies is important in order to realise the goal of e-Administration, improve the transfer of documents between public bodies and ensure that the relevant archival requirements are met.

The purpose of this set of requirements is to ensure that public sector organisations can exchange all types of information regardless of which Noark solution they use. Such document exchange must be both simple to use and facilitate the exchange of sensitive information.

A structure and content specification (XML form) for document exchange will follow in a later version of Noark 5.

Requirement no.:	Requirements for electronic document exchange	Type	Remarks
6.3.26	There should be functions for secure, automated document exchange between Noark solutions, based on an XML form for document exchange.	V	
6.3.27	There must be functions for automatically registering received case documents.	B	Obligatory if 6.3.26 is fulfilled.
6.3.28	Metadata for outgoing and incoming documents sent through electronic message exchange must at least contain obligatory metadata.	B	Obligatory if 6.3.26 is fulfilled.
6.3.29	In the case of electronic document exchange involving sensitive information, encryption must be carried out when the message is dispatched from the organisation's secure network. Only the predefined recipient should be able to decrypt.	B	Obligatory if 6.3.26 is fulfilled.
6.3.30	In connection with electronic document exchange, the transmission must be protected against unauthorised alteration.	B	Obligatory if 6.3.26 is fulfilled.
6.3.31	In connection with electronic document exchange, it must be possible for relevant logs to be stored in the Noark solution.	B	Obligatory if 6.3.26 is fulfilled.

6.3.6 Migration between Noark solutions

In this context, *migration* means the movement of complete data sets from one technical platform to another (new version or new solution), where the data must remain as unmodified as possible once they have been moved.

It must be possible to export or extract the information that is stored in a Noark 5 solution to a system-independent format. The export must include the fonds structure, metadata and any associated electronic documents. A distinction is made between two variants of export – migration export and transfer export. Transfer exports are considered in section 4.2.12.

It must be possible to use migration exports for the migration of data in connection with upgrades to a new version of the same solution or on transition to another Noark solution. It should also be possible to transfer active series from one system to another, e.g. in connection with organisational changes. This means that a Noark solution must also be able to import data from a migration export.

The migration of data means that a Noark solution must be able to handle exports and imports. Such migration may be relevant in connection with an upgrade to a new version. Users who are switching to a new Noark solution from another supplier must be able to transfer their old data to the new solution without any problems. It should also be possible to import certain data from one solution into another solution that is already in use. This may be appropriate in connection with reorganisations where for example part of a public body's area of responsibility is transferred to another body.

If one or more series are moved from one solution to another, an agreement will be needed which regulates the actual content of the migration export. This is to take account of any differences between the solutions.

A structure and content specification (XML form) for the migration export will follow in a later version of Noark 5.

Requirement no.:	Requirements for migration between Noark solutions	Type	Remarks
6.3.32	It must be possible to export all metadata that are defined in this standard and associated documents based on the transfer format.	O	
6.3.33	It must be possible to export all metadata that are defined in this standard and associated documents based on the transfer format.	O	
6.3.34	It should be possible to export parts of the fonds structure, e.g. a series or class.	V	
6.3.35	It should be possible to export parts of the fonds structure, e.g. a series or class.	V	
6.3.36	A log must be generated of all metadata and documents that cannot be imported and of any other errors that occur during import.	O	

Requirement no.:	Requirements for migration between Noark solutions	Type	Remarks
6.3.37	When an import is performed, a log file must be generated with information on the success or otherwise of the import, e.g. the number of metadata elements and documents. The log file must also contain a list of all metadata elements and documents that could not be imported.	O	

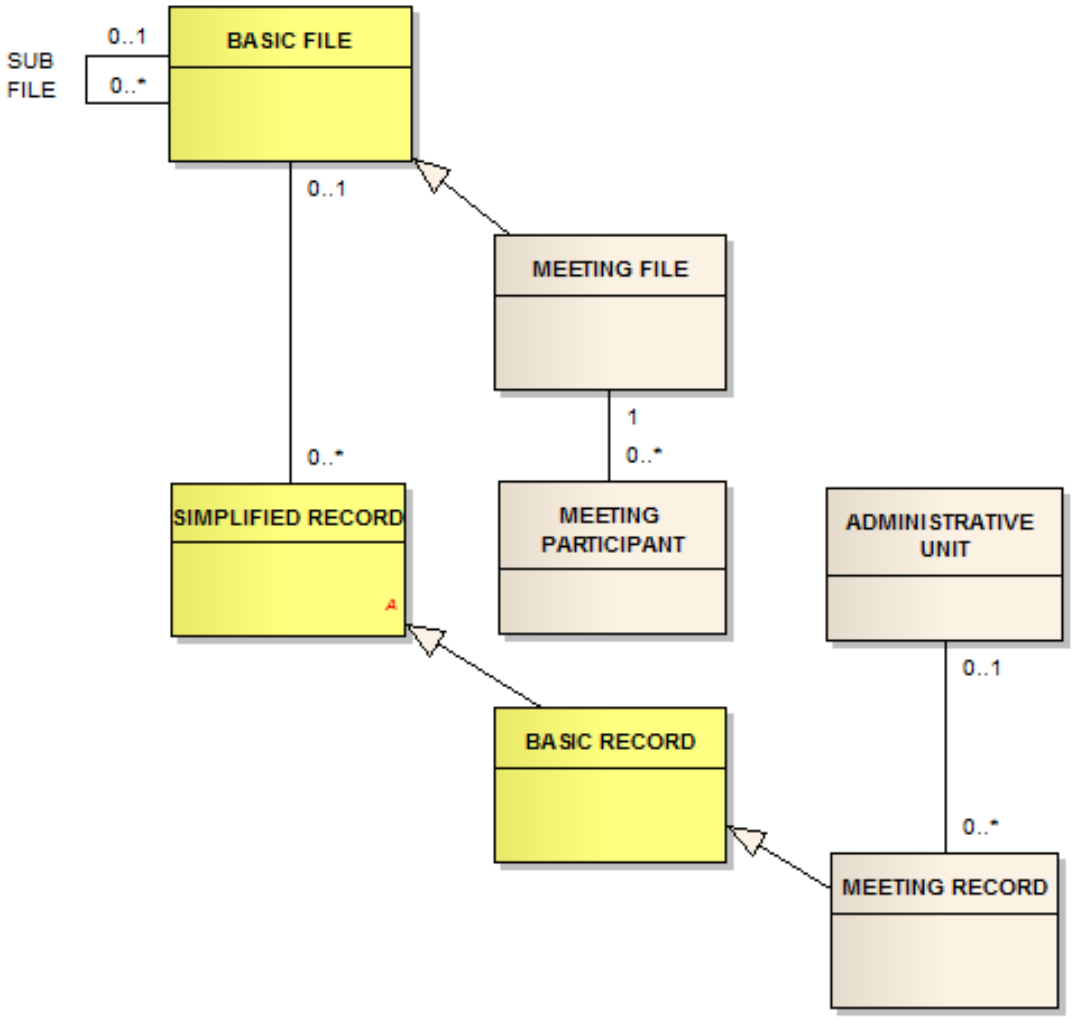
6.4 Meeting and board handling

A module for meeting handling must cover a series of functions linked to case handling in collegiate bodies such as boards, committees, etc. If a separate solution for meeting handling is used in a Noark 5 solution, the solution must offer services / have functions for recordkeeping, archiving, periodising and transferring the valuable archival information that is generated in the solution.

Documents that are produced in connection with a meeting must be collated in a *Meeting file*, which is an expansion of a basic file.

The individual documents that are produced in connection with the meeting must be assigned metadata in the form of a *Meeting record*, which is an expansion of a Basic record.

Conceptual model for Meeting and board handling



<Conceptual model for Meeting and Board Handling>

Metadata for meeting and board handling

Metadata for *Meeting file* (based on basic file)

Metadata for basic file forms part of meeting file. The following metadata are additional.

No.	Name	Type	Occ.	Trans.	Remarks
M008	meetingnumber	B	One	A	Obligatory for fonds with meeting and board handling.

No.	Name	Type	Occ.	Trans.	Remarks
M370	Board	B	One	A	Obligatory for fonds with meeting and board handling.
M102	meetingdate	B	One	A	Obligatory for fonds with meeting and board handling.
M371	meetingplace	V	One		
M221	referencePreviousMeeting	V	One	A	
M222	referenceNextMeeting	V	One	A	

Metadata for *Meeting participant*

Metadata for meeting participant must be grouped into metadata for meeting file. Meeting participant is obligatory and may occur one or more times in a meeting file.

No.	Name	Type	Occ.	Trans.	Remarks
M372	meetingparticipantName	B	One	A	Obligatory for fonds with meeting and board handling.
M373	meetingparticipantFunction	B	One	A	Obligatory for fonds with meeting and board handling.

Metadata for *Meeting record* (based on basic record)

Metadata for basic record forms part of meeting record. The following metadata are additional.

No.	Name	Type	Occ.	Trans.	Remarks
M085	Meetingrecordtype	B	One	A	Obligatory for fonds with meeting and board handling.
M088	meetingcasetype	B	One	A	Obligatory for fonds with meeting and board handling.
M055	meetingrecordstatus	V	One		
M305	administrativeUnit	B	One	A	Obligatory for fonds with meeting and board handling.
M307	executiveofficer	B	One	A	Obligatory for fonds with meeting and board handling.
M223	referenceToMeetingrecord	V	Many	A	
M224	referenceFromMeetingrecord	V	Many	A	

Requirements for Meeting and board handling

Requirement no.	Structural requirements for Meeting handling	Type	Remarks
6.4.1	It must be possible to specialise a *Basic file* in a meeting file.	B	Obligatory for fonds with meeting and board handling.
6.4.2	A *Meeting file* must expand a *Basic file*, and a *Basic file* can be expanded by a Meeting file.	B	Obligatory for fonds with meeting and board handling.

Requirement no.	Structural requirements for Meeting handling	Type	Remarks
6.4.3	It must be possible to define relevant additional metadata for *Meeting file* in addition to the metadata that have been defined.	B	Obligatory for fonds with meeting and board handling.
6.4.4	It must be possible to specialise a *Basic record* in a *Meeting record*.	B	Obligatory for fonds with meeting and board handling.
6.4.5	A *Meeting record* must belong to (only) one Basic record and a Basic record can contain (only) one *Meeting record*.	B	Obligatory for fonds with meeting and board handling.
6.4.6	It must be possible to define relevant additional metadata for *Meeting record* in addition to the metadata that have been defined.	B	Obligatory for fonds with meeting and board handling.

Requirement no.	Functional requirements for meeting handling	Type	Remarks
6.4.7	There must be services/functions for registering, archiving, periodising and transferring information and documents that are generated in connection with meeting handling.	B	Obligatory for fonds with meeting and board handling.

Requirement no.	Functional requirements for meeting handling	Type	Remarks
6.4.8	Meeting record types that must be capable of being registered will include: • Meeting summons • Enclosure to meeting case • Decision in meeting case • Memo to political committee • Case list • Meeting folder • Meeting report • Meeting minutes • Case report • Overview of participants, representatives and members of committees, councils, boards, etc. • Case draft It is not necessary to register all the information elements above individually. If summaries of information elements are produced, it is sufficient for the summaries to be registered.	B	Obligatory for fonds with meeting and board handling.
6.4.9	There must be a service/function for creating a separate *Meeting file* based on *Basic file.*	B	Obligatory for fonds with meeting and board handling.
6.4.10	There must be a service/function for creating a separate *Meeting record* based on basic record.	B	Obligatory for fonds with meeting and board handling.
6.4.11	It must be possible to specify meeting case types. The following types will be relevant in connection with meeting handling in the municipal sector: • Political case • Delegated meeting case • Referred case • Interpellation • Unregistered case	B	Obligatory for fonds with meeting and board handling.
6.4.12	There must be a service/function for defining separate meeting record types.	B	Obligatory for fonds with meeting and board handling.

Requirement no.	Functional requirements for meeting handling	Type	Remarks
6.4.13	Process and handling events for Meeting file and Meeting record must be logged.	B	Obligatory for fonds with meeting and board handling.

Remarks: Although the meeting handling must have strong links to the administration and fonds structure in Noark 5, it will also be necessary to store a certain amount of logistical information for the meeting handling. These information elements have no natural link to the fonds structure or other functions in Noark 5, and it is therefore natural that the functionality for meeting handling is created as a separate module (case handling module), in which the information elements that belong to the meeting handling for example can be saved as information elements in a series.

6.5 Reporting and statistics

This section applies to case records. The obligatory reports that are covered by this section are reports which are necessary in order to fulfil the requirements in the legislation and regulations or which are normally required for other reasons.

Remarks:
The nine obligatory reports are largely a continuation of the reports from Noark-4. It has not finally been decided which metadata elements should be included in them, although the reports will have the same basic content as they had in Noark-4.

The requirement tables for each report set out requirements for selection, sorting and report content. *Selection* indicates which metadata elements the report should be selected from. *Sorting* indicates how the report is to be sorted, i.e. according to which metadata elements it should be organised. *Report content* defines what information is actually to be included in the report. The reason for this distinction is that the report will not necessarily be sorted according to all
the selection criteria or selected on the basis of all the sorting criteria. In most cases, the report will contain more information than the criteria according to which it was selected and sorted.

Noark 5 gives no instructions concerning the typographical layout of the reports.

6.5.1 Fonds summary

The purpose of the report *Fonds summary* is to provide an overview of the series into which the fonds
have been subdivided, with a statement of the fonds period that it or they are included in, classification system, status and physical location. This is important for the overview in the fonds.

Requirement no.	Requirements for the report *Fonds summary*	Type	Remarks
6.5.1	The report *Fonds summary* is obligatory.	B	Obligatory for case records.
6.5.2	*Selection:* It must be possible to select the report freely according to the following metadata elements: • *referenceParent* in *Series*, or • *fondsperiodStartDate and fondsperiodEnddate in Series*	B	Obligatory for case records.
6.5.3	*Sorting:* It must be possible to sort the report freely according to the following metadata elements: • *referenceParent* in *Series*, or • *fondsperiodStartDate and fondsperiodEnddate* in *Series*	B	Obligatory for case records.

Requirement no.	Requirements for the report *Fonds summary*	Type	Remarks
6.5.4	*Report content:* The following metadata must be included in the report, where they exist in the solution: From *Fonds*: *systemID* *title* *fondscreatorname* *fondsstatus* *createdDate* *finalisedDate* *From Classification system* *classificationtype* *title* From *Series*: *systemID* *title* *referenceParent* *referenceClassificationsystem* *fondssectionstatus* *referenceSuccessor* *referencePrecursor* *physicalDocuments* *referenceDocumentdescription* *createdDate* *finalisedDate* *fondsperiodStartDate* *fondsperiodEndDate* *storagelocation* *description* *exportedDate* *responsibleExport*	B	Obligatory for case records.

6.5.2 Public registry

The purpose of the report *Public registry* is to provide the public with information on the public body's registered
documents. The registry is largely formulated in the same way as the report *Registry*, but it will screen information that is exempt from public access.

The requirements for the report are formulated in accordance with the provisions of the Freedom of Information Act and
Section 2-7 of the Archives Regulation.

The requirements below are obligatory for case record solutions and other solutions covered by the provisions of the Freedom of Information Act concerning public registries.

Requirement no.	Requirements for the report *Public registry*	Type	Remarks
6.5.5	The report *Public registry* is obligatory.	B	Obligatory for fonds covered by the Freedom of Information Act.
6.5.6	The report must contain all registry entry types. Simplified records are not included.	B	Obligatory for fonds covered by the Freedom of Information Act.
6.5.7	The metadata element *screeningMetadata* contains information on the elements that are to be screened. The metadata field *officialTitle* is a copy of title, but all the words that are to be screened have been removed here (e.g. replaced by *****).	B	Obligatory for fonds covered by the Freedom of Information Act.
6.5.8	*Selection:* It must be possible to select the report on the following metadata elements (from *Registry entry* unless stated otherwise): • *registrydate* (it must be possible to specify an interval) • *registrymanagementunit* • *administrativeUnit* for executive officer	B	Obligatory for fonds covered by the Freedom of Information Act.
6.5.9	For organisations that have begun using functionality for temporary blocking, it must be possible, as an alternative to selecting according to registry date, to select according to the following metadata element: • *confidentialityassessed* (cf. *Registry entry*). It must be possible to specify an interval.	B	Obligatory for fonds covered by the Freedom of Information Act.
6.5.10	*Sorting:* It must be possible to sort the report freely according to: • *serialnumber*, or • *registryentry*, *registrydate* and *serialnumber*, or • *adminstrativeUnit* for executive officer, *registrydate* and *serialnumber*.	B	Obligatory for fonds covered by the Freedom of Information Act.

Requirement no.	Requirements for the report *Public registry*	Type	Remarks
6.5.11	*Report content:* The following metadata must be included in the report, where they exist in the solution: ***Case file information*** From *Case file*: *fileID* *officialTitle* From *Class* (additional classification is not to be included): *classID* (not to be printed if marked as screened in the solution). ***Registry entry information*** From *Registry entry*: *serialnumber* *recordID* *registrydate* *documentDate* (text "Undated" if there is no date) *officialTitle* *clienttype* *clientName* (not to be printed in a public registry if the name is exempt from public access) *depreciationmethod* *depreciationdate* *referenceDepreciatedByRegistryentry* *referenceDepreciatesRegistryentry* Each registry entry must also show: 1) serial number of the previous registry entry in the case file concerned (e.g. with the header "Previous serial no. in the case"), 2) serial number which is answered (where applicable) by the registry entry concerned (e.g. with the header "Response to serial no."). *It must be possible for "Response to serial no." to contain several serial nos.*	B	Obligatory for fonds covered by the Freedom of Information Act.

Requirement no.	Requirements for the report ***Public registry***	Type	Remarks
6.5.12	It should also be possible for the report to freely contain one or more of the following items of information (where they exist in the solution): ***Case file information*** From *Case file*: *administrativeUnit* *case-responsible* *accessrestriction* *screeningauthority* ***Registry entry information*** From *Registry entry* (sorted according to *recordID* unless specified otherwise): *accessrestriction* *screeningAuthority* *administrativeUnit* *executiveofficer*	V	

6.5.3 Ongoing registry

The purpose of the report *Registry* is to provide an overview of all archived documents for each day. The report must contain information from case file and registry entry, including the information that is screened in the solution.

The provisions concerning registries are set out in Sections 2-6 – 2-10 of the Archives Regulation.

Requirement no.	Requirements for the report ***Ongoing registry***	Type	Remarks
6.5.13	The report *Ongoing registry* is obligatory.	B	Obligatory for case records.

Requirement no.	Requirements for the report *Ongoing registry*	Type	Remarks
6.5.14	*Selection:* It must be possible to freely select the report according to the following metadata elements (from *registry entry* unless stated otherwise): • *registrydate* (it must be possible to specify an interval), or • *serialnumber* (it must be possible to specify an interval) • registryentry*type* (it must be possible to select one or more) • *registryentry* for the person responsible for the processing • *administrative unit* for the person responsible for processing (here, it must be specified whether or not underlying units are to be included).	B	Obligatory for case records.
6.5.15	For internal documents, it must be possible to delimit the report to only cover received documents, so that the same document is not listed twice.	B	Obligatory for case records.
6.5.16	*Sorting:* It must be possible to sort the report freely according to: • *serialnumber*, or • *registrymanagementunit* of the person responsible for processing, thereafter by *registrydate* and *serialnumber* within each registry date, or • *administrative unit* of the person responsible for processing, thereafter by *registrydate* and *serialnumber* within each registry date.	B	Obligatory for case records.

Requirement no.	Requirements for the report *Ongoing registry*	Type	Remarks
6.5.17	*Report content:* The following metadata must be included in the report, where they exist in the solution: ***Case file information*** From *Case file*: *fileID* *title* *adminstrativeUnit* *case-responsible* *referenceFondssection* From *Class* *classID and title* ***Registry entry information*** From *Registry entry*: *serialnumber* *recordID* *registrydate* *documentDate* (text "Undated" if there is no date) *title* *accessrestriction* *screeningauthority* *numberofAppendices* *confidentialityassessedDate* *clienttype* *clientname* *administrativeUnit* *executiveofficer* *registrymanagementunit* Each registry entry must also show: 1) serial number of the previous registry entry in the case file concerned (e.g. with the header "Previous serial no. in the case"). 2) serial number which is answered (where applicable) by the registry entry concerned (e.g. with the header "Response to serial no."). It must be possible for "Response to serial no." to contain several serial nos.	B	Obligatory for case records.

Requirement no.	Requirements for the report *Ongoing registry*	Type	Remarks
6.5.18	It must be possible to retrieve an overview of the most recent version of all the documents (main document and appendices) that are linked to each registry entry. The following metadata elements should then be printed out: From *Documentlink*: *linkedRecordAs* From *Documentdescription:* *title* *documenttype* *storagelocation* *accessrestriction* *screeningauthority* ***Version information*** From *Version* (sorted according to *Versionno., Variant*): *versionnumber* *variantformat*	B	Obligatory for case records.

6.5.4 Back log list

At specific times, public sector bodies are required to extract overviews of documents that have not been fully processed. In government bodies, this is normally done four times a year. This overview is called an *back log list.* The aim of the back log check is to ensure that all enquiries received by the organisation are answered within a reasonable period of time. This is pursuant to Section 11a of the Public Administration Act (i.e. the provision concerning case handling time and provisional replies). The back log list also provides an overview of the organisation's workload. This is pursuant to Section 3-7, second paragraph of the Archives Regulation.

The back log list is intended to give managers information on the current back log situation within
his or her unit and which case files have back log associated with them. For case-responsibles, the back log list can be used as a reminder that there are unfinalised cases for which they are responsible. Similarly, executive officers will receive a reminder that they still have documents that require processing.

Requirement no.	Requirements for the report *Back log list*	Type	Remarks
6.5.19	The report *Back log list* is obligatory.	B	Obligatory for case records.

Requirement no.	Requirements for the report *Back log list*	Type	Remarks
6.5.20	*Selection:* It must be possible to select the report on the following metadata elements: • *registrydate* from *Registry entry* (it must be possible to specify an interval) and • registryentry*type* from *Registryentry* • *registrymanagementunit* • *administrativeUnit* (here, it must be possible to specify whether underlying units are to be included). • *depreciationmethod* (here, it must be possible to choose between *non-depreciated documents* and *non-depreciated* and *provisionally depreciated documents* (value ***). • *CC addressee*. It must be possible to specify whether or not CC addressees are to be included.	B	Obligatory for case records.
6.5.21	*Sorting:* Sorting must be performed on the basis of the recipients who meet the selection criterion. If several recipients linked to the same registry entry meet the selection criterion, the registry entry must be included in the extract once for each of these recipients. It must be possible to sort the report freely according to: • *registrymanagementunit* and then by *executiveofficer* and *fileID* from *Case file* and *recordID* from *Registry entry* or • *administrativeUnit* and then by *executive officer* and *fileID* from *Case file* and *recordID* from *Registry entry*, or • *registrymanagementunit* and then by *case-responsible* and *fileID* from *Case file* and *recordID* from *Registry entry*, or • *administrativeUnit* and then on *case-responsible* and *fileID* from *Case file* and *recordID* from *Registry entry*.	B	Obligatory for case records.

Requirement no.	Requirements for the report ***Back log list***	Type	Remarks
6.5.22	*Report content:* The following metadata must be included in the report, where they exist in the solution: ***Case file information*** From *Case file*: *fileID* *title* *administrativeUnit* *case-responsible* *registrymanagementunit* From *Class* *classID and title* ***Registry entry information*** From *Registry entry*: *recordID* *registrydate* *documentDate* (text "Undated" if there is no date) *title* *duedate* *clienttype* *clientName* *administrativeUnit* *executiveofficer*	B	Obligatory for case records.
6.5.23	The page numbering must be per administrative unit, i.e. it must start on p.1 upon switching to a new administrative unit. Space must be allocated for remarks from the executive officer after each registry entry.	B	Obligatory for case records.
6.5.24	It should be possible to define the report so that certain case areas are not included in the back log list. This could for example concern case files/registry entries which have particular order values or which are being processed by particular administrative units.	V	

6.5.5 Maturity list

The purpose of the report *Maturity list* is to be able to show documents with a deadline for case handling, in order to notify the executive officer. If the archive is responsible for the maturity check, the registry must notify the executive officer of the maturity date. Alternatively,
an executive officer with record access can perform the record him-/herself and follow up maturity dates for
his or her documents.

The maturity list is intended as a tool for fulfilling the requirements in Section 3-7 first paragraph of
the Archives Regulation.

Requirement no.	Requirements for the report Maturity list	Type	Remarks
6.5.25	*Selection:* It must be possible to select the report on the following metadata elements: • *registrydate* from *Registry entry* (it must be possible to specify an interval) and • *registryentrytype* from Registry entry • *registrymanagementunit* • *administrativeUnit* (here, it must be possible to specify whether or not underlying units are to be included). • *CC addressee*: It must be possible to specify whether or not CC addressees are to be included. • *maturitydate* in *Registry entry* (it must be possible to specify an interval)	B	Obligatory for case records.
6.5.26	*Sorting:* Sorting must be performed on the basis of the recipients who meet the selection criterion. If several recipients linked to the same registry entry meet the selection criterion, the registry entry must be included in the extract once for each of these recipients. It must be possible to sort the report freely according to: • *registrymanagementunit* and then by *executive officer* and *fileID* from *Case file* and *recordID* from *Registry entry*, or • *administrativeUnit* and then by *executive officer* and *fileID* from *Case file* and *recordID* from *Registry entry*, or • *registrymanagementunit* and then by *case-responsible* and *fileID* from *Case file* and *recordID* from *Registry entry*, or • *administrativeUnit* and then by *case-responsible* and *fileID* from *Case file* and *recordID* from *Registry entry*.	B	Obligatory for case records.

Requirement no.	Requirements for the report Maturity list	Type	Remarks
6.5.27	*Report content:* The report must contain the following information, where it exists in the solution: ***Case file information*** From *Case file*: *fileID* *title* *administrativeUnit* *case-responsible* *registrymanagementunit* From *Class* *classID and title* ***Registry entry information*** From *Registry entry*: *recordID* *registrydate* *documentDate* (text "Undated" if there is no date) *title* *duedate* *clienttype* *clientName* *administrativeUnit* *executiveofficer*	B	Obligatory for case records.

6.5.6 Downgrading list

The purpose of the report *Downgrading list* is to provide an overview of documents that must be reviewed in order to assess downgrading.
The principles are based on the provisions in current legislation and regulations. Documents graded according to the Protection Decree are downgraded automatically after 30 years. It is however possible to set shorter deadlines for downgrading, normally two or five years, and it is also possible to exempt documents from automatic downgrading. The secrecy obligation in accordance with the Public Administration Act is generally revoked after 60 years.

Requirement no.	Requirements for the report Downgrading list	Type	Remarks
6.5.28	*Selection:* It must be possible to select the report on the following metadata elements from: *Registry entry*: • *downgradingdate* (it must be possible to specify an interval) • *gradingauthority* (it must be possible to select one or more) • *fondsperiodStartDate and fondsperiodEnddate from Series* • *referenceFondssection* from Case file	B	Obligatory for solutions where downgrading is relevant.
6.5.29	*Sorting:* It must be possible to sort the report freely according to: • *administrativeUnit* from *Case file*, then by *case-responsible* and thereunder *fileID*, or: • administrative*Unit*, then *executiveofficer* and thereunder *fileID*, or: • *downgradingdate* from *Registry entry* and thereunder *fileID*.	B	Obligatory for solutions where downgrading is relevant.

Requirement no.	Requirements for the report Downgrading list	Type	Remarks
6.5.30	*Report content:* The report must include the following information, where it exists in the solution: ***Case file information*** From *Case file*: *fileID* *title* *administrativeUnit* *case-responsible* From *Class* *classID and title* ***Registry entry information*** From *Registry entry*: *recordID* *registrydate* *documentDate* (text "Undated" if there is no date) *title* *accessrestriction* *screeningAuthority* *registryentrytype* *downgradingdate* *gradingauthority* *clienttype* *clientName* *administrativeUnit* *executiveofficer* *registrymanagementunit*	B	Obligatory for solutions where downgrading is relevant.

6.5.7 Disposal list

The purpose of the report *Disposal list* is two-fold. It is intended firstly as an aid in the actual disposal work and secondly as an overview of the cases that have been disposed of.
Section 3-14 of the Archives Regulation requires public sector bodies to prepare summary lists of
fonds that are disposed of.

Requirement no.	Requirements for the report *Disposal list*	Type	Remarks
6.5.31	*Selection:* It must be possible to select the report on the following metadata elements in *Case file*: • *disposaldate* (it must be possible to specify an interval) • *disposaldecision* • *administrativeUnit* (here, it must be possible to specify whether underlying units are to be included). • *registrymanagementunit* • *referenceFondssection* • fondsperiodStartDate and fondsperiodEnddate from Series	B	Obligatory for solutions that must facilitate disposal.
6.5.32	It must be possible to sort the report according to the metadata elements: • *fondsperiodStartDate* and *fondsperiodEnddate* from *Series* • *referenceFondssection Case file* • *classID* from *Class* • *fileID* from Case file	B	Obligatory for solutions that must facilitate disposal.
6.5.33	The report must contain the following information, where it exists in the solution: ***Case file information*** From *Case file*: *fileID* *title* *createdDate* *referenceChild* *disposaldecision* *disposaldate* *administrativeUnit* *referenceFondssection* From *Class* *classID and title* From *Series*: *referenceParent* *fondsperiodStartDate* *fondsperiodEndDate*	B	Obligatory for solutions that must facilitate disposal.

6.5.8 List for remote storage, transfer and handover

The purpose of this report is to obtain an overview of the sections of the archive material that must
be transferred to a remote storage archive, an archive repository or another public sector

body. The report can be used as a remote storage list for the public body itself in connection with periodisation, as a
handover list in connection with the transfer of archive material between public sector bodies or as a
transfer list in connection with transfers to an archive repository.

The requirement for a remote storage list is set out in Section 3-14 of the Archives Regulation. The remote storage list is a
complete fonds list covering what is to be preserved, corresponding to the transfer list.
Section 5-4 of the Archives Regulation contains a provision which requires public sector bodies that transfer
older and finalised material to an archive repository to prepare a complete transfer list
of the material that is to be transferred. The transfer list must be enclosed with the transfer to the archive repository.

Section 3-22 of the Archives Regulation requires public sector bodies that hand over archive material to another
public sector body to prepare a handover list for the material that is to be handed over.
The handover list must be prepared in the same way as a transfer list for transfers to an archive repository.
The organisation must retain a copy of both handover and transfer lists. These should
be included in the organisation's fonds plan.

Requirement no.	Requirements for the report List for remote storage, transfer and handover	Type	Remarks
6.5.34	*Selection:* It must be possible to select the report freely on the following metadata elements: • *fondsperiodStartDate and fondsperiodEndDate* from *Series* (one or more), or • reference*Fondssection* from *Case file* (one or more). • *registrymanagementunit* from *Case file* (one or more). • *administrativeUnit* from *Case file* (here, it must be possible to specify whether or not underlying units are to be included). • *casestatus* in *Case file* • *depreciationdate* from *Registry entry* (here, it must also be possible to specify the value "empty field"). • disposaldecision	B	Obligatory for solutions that must facilitate remote storage, transfer and handover.
6.5.35	*Sorting:* It must be possible to sort the report on the following metadata elements: • *referenceFondssection* from Case file • *classID* from *Class* • *fileID* from *Case file* and then *recordID* from *Registry entry*	B	Obligatory for solutions that must facilitate remote storage, transfer and handover.

Requirement no.	Requirements for the report List for remote storage, transfer and handover	Type	Remarks
6.5.36	*Report content:* The report must contain the following information, where it exists in: the solution: ***Case file information*** From *Case file*: *fileID* *createddate* *title* *casestatus* *referenceChild* *disposaldecision* *disposaldate* *referenceFondssection* From *Class* *classID and title* From *Series*: *referenceFonds* *fondsperiodStartDate* *fondsperiodEndDate*	B	Obligatory for solutions that must facilitate remote storage, transfer and handover.
6.5.37	For each new ClassID, the classification system's text (the derived metadata element *title*) must be included on a separate line as a heading.	B	Obligatory for solutions that must facilitate remote storage, transfer and handover.
6.5.38	Both the right- and left-hand margins in the report must be at least 4cm in order to provide sufficient space for remarks.	B	Obligatory for solutions that must facilitate remote storage, transfer and handover.
6.5.39	If the report contains documents that are graded, the number of graded documents must be marked in connection with the case.	B	Obligatory for solutions that must facilitate remote storage, transfer and handover.

6.6 Security and access control

The basic model for access control and security with regard to change in Noark 5 is based on the core specifying the conditions for obtaining access to objects, while the modules outside the core accept that the conditions are met.

An external module must be known to the core. The core must therefore not disclose information or perform actions at the request of an unidentified module. For many Noark 5 fonds, it will be sufficient for the external module to be known. The core will then "trust" the external module and accept its authorisation for the information to be used.

However, different fonds may have differing requirements as regards how precisely rights to objects must be specified, as well as differing requirements as regards how certain the core must be that it is actually communicating with a module that there is reason to trust.

In certain special cases, there may also be a need for the core to have an overview of the actual personal users who are to have access to which objects. It should also be possible to configure the core in such a way that it does *not* "trust" the external modules. To facilitate simple integration and an integrated security policy across an organisation's IT systems, security functions that provide for user directories outside the Noark 5 core are however recommended.

The security requirements in Noark 5 outer core are therefore subdivided into the following main topics:

- Security configuration
- Rights specifications

Security configuration is the choices that are made concerning the strictness of the requirements that are imposed for access within each series. The aim is flexibility. The requirements for security will vary from organisation to organisation. Rights specifications are the concrete link between objects in the fonds and the services, or alternatively personal users, that have access rights to them.

Requirement no.	Requirements for security in the core	Type	Remarks
6.6.1	All modules or systems outside the core that are to communicate with or have access to objects in Noark 5 core must be identified and recognised by the core.	O	
6.6.2	An external module that is no longer to have access to services must still be identified in the core, but with a status that indicates that it is "passive".	O	
6.6.3	There must be an overview of the period or periods during which each external module has been active.	O	
6.6.4	At least one user must be defined as a registry administrator, who can explicitly log onto the Noark 5 core in order to alter the configuration and global parameters.	O	
6.6.5	It must be possible to set the log-on identifier for a registry administrator who is no longer to have access to the core to the status "Passive", which will prevent the administrator from logging on.	O	

Requirement no.	Requirements for security in the core	Type	Remarks
6.6.6	There must be an overview of the period or periods during which the log-on identifier has been active.	O	
6.6.7	The minimum requirement for authentication strength for logging on as a registry administrator is a password. Here, requirements can be imposed concerning the strength of the password (complexity, length, duration, etc.).	O	
6.6.8	It should be possible to use other and stronger authentication methods as an alternative to passwords.	V	

The security configuration is unique to each series. Each of the options represents a statement of the degree of trust that the core is to have in the external modules. The fact that the core has a high degree of trust in external modules will not necessarily weaken information security if the organisation's security measures are generally well integrated.

Requirement no.	Requirements for security configuration	Type	Remarks
6.6.9	For a series, it must be possible to specify which authentication method(s) should be required for the external modules that are to be given access to use services in the core.	O	
6.6.10	For a series, it should be possible to specify whether only the individual external module is to be identified, or whether each individual personal user must also be identified in the core.	V	
6.6.11	For a series, it must be possible to specify whether the module, or alternatively the personal user, that is registered as being responsible for a file or record is to have read and write access to the file or folder *automatically*, or whether explicit rights specifications are also required for the person responsible for the file/record.	O	
6.6.12	For a series, it must be possible to specify whether access rights are inherited downwards in the hierarchy by default, or whether explicit access rights must be specified at each level.	O	

Requirement no.	Requirements for security configuration	Type	Remarks
6.6.13	For a series, it should be possible to specify whether it will be permissible to specify that *all* authenticated external modules – both existing and future ones – have read or write access to an object. (If this recommendation is not implemented, this must be understood as indicating that it is *not* permitted to specify that all modules have access and that only certain specified modules have access to an object).	V	

Rights specifications can be linked to each of the five levels: series, class, file, record and document description. It is worth noting that there are no references to roles, profiles or other authorisation mechanisms in the core because it is assumed that these are handled in the external modules. The basic principle is a specification of which module or modules have read and write access to each object in the fonds. How flexibly or rigidly this can be specified will vary with the configuration selections that are made for the series.

If the module that is specified as being responsible for a file or record is to have automatic access (requirement 0), all actions that are authorised in the external module concerned will be accepted by the core. Other modules can also gain access, but only if they are individually specified (or if it is specified that "all modules" have access; cf. requirement 0).

If access rights are inherited downwards in the hierarchy by default (requirement 0), it will for example be possible to give a particular external module access to the entire series. The same module will then have automatic access to all underlying files, with the exception of the files for which specific restrictions concerning the rights are specified. Not giving any rights as high up in the hierarchy as the series can also be chosen. In this case, the rights will have to be specified individually for each file, and inherited by each underlying record (each with its own underlying documents), with the exception of any records for which specific rights are indicated. If the series is instead configured to require explicit access, no access rights will be inherited from higher levels in the hierarchy.

The same principles for rights specifications and the relationship between configuration selections and rights specifications also apply if the recommended requirement no. 4.406 (identification of each personal user) is selected for a series.

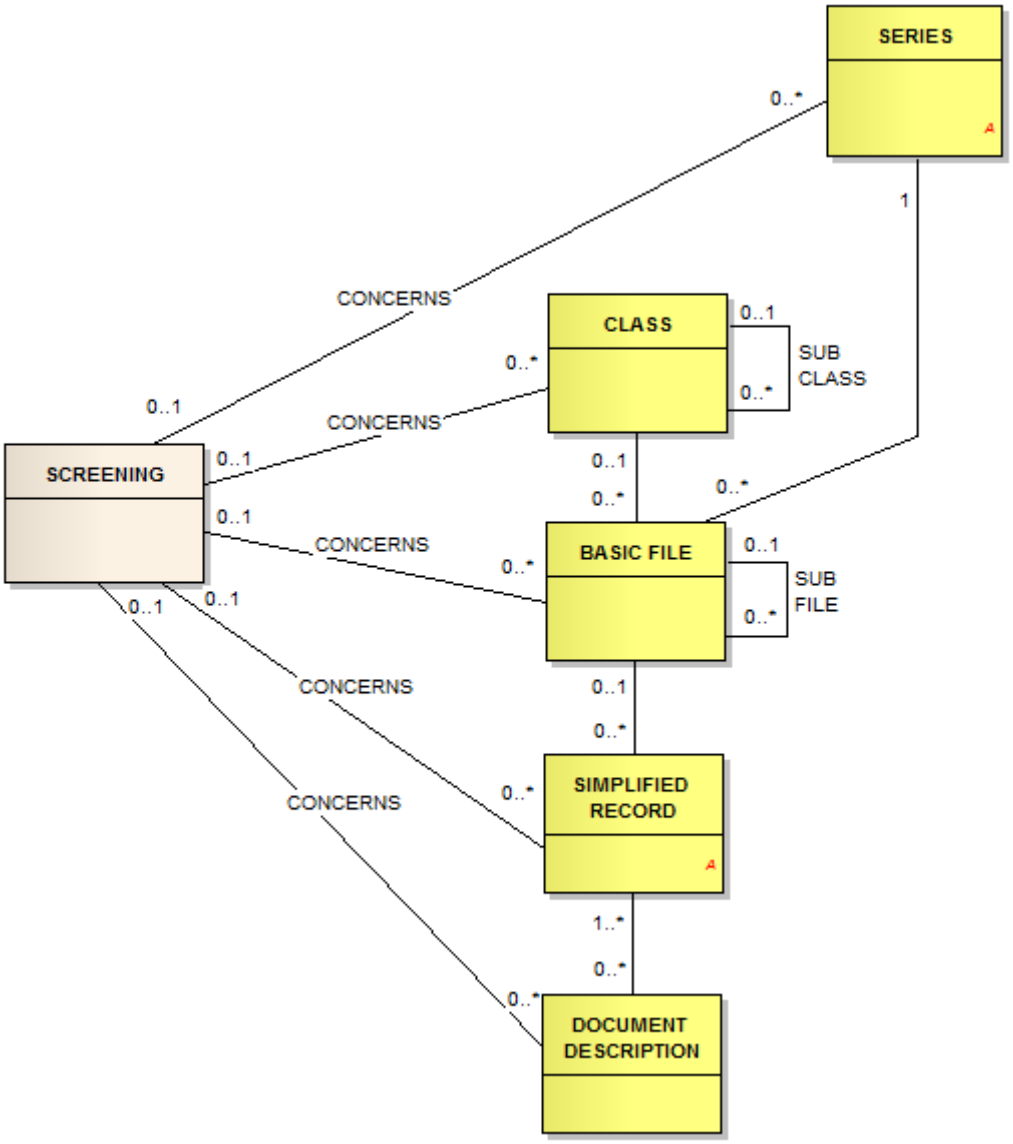
Requirement no.	Requirements for rights specifications	Type	Remarks
6.6.14	For each series, class, file, record and document description, it must be possible to register which external modules have read access.	O	
6.6.15	For each series, class, file, record and document description, it must be possible to register which external modules have updating access.	O	

Requirement no.	Requirements for rights specifications	Type	Remarks
6.6.16	For each series, file, record and document description, it should be possible to specify read access for "*all*" external modules (both existing and future ones); cf. requirement 0	V	
6.6.17	For each series, file, record and document description, it should be possible to specify updating access for "*all*" external modules (both existing and future ones); cf. requirement 0	B	If 6.6.13 is met, 6.6.17 must also be met.
6.6.18	For each series, class, file, record and document description, it should be possible to register which personally identified users have read access.	V	
6.6.19	For each series, class, file, record and document description, it should be possible to register which personally identified users have updating access.	V	

6.6.1 Screening

Screening is used to screen registered information or individual documents. The screening takes effect when an access code is assigned to the individual folder, record or individual document.
The solution's users must be cleared for certain access codes and authorised for a predefined part of the cases and registry entries and associated documents that are screened.

Conceptual model for Screening



<Screening in the model structure>

Metadata for screening

Metadata for screening must be grouped into metadata for series, class, file, record and document description. Metadata for screening are optional and can occur once.

In Noark 4, these attributes have different names depending on the level in the fonds structure to which they are linked. References to attributes at registry entry level are shown below.

No.	Name	Type	Occ.	Trans.	Remarks
M500	accessrestriction	O	One	A	?
M501	screeningauthority	O	One	A	?

No.	Name	Type	Occ.	Trans.	Remarks
M502	screeningMetadata	O	One	A	?
M503	screeningDocument	O	One	A	?
M504	screeningduration	O	One	A	?
M505	screeningCeasesDate	O	One	A	?

Metadata for grading

Metadata for grading must be grouped into metadata for file, record and document description. Grading is optional and can occur once.

No.	Name	Type	Occ.	Trans.	Remarks
M506	grading	O	One	A	
M624	gradingdate	O	One	A	
M625	gradedBy	O	One	A	
M626	downgradingdate	O	One	A	
M627	downgradedBy	O	One	A	

Remarks

1. *These metadata are also copied down into the classes that can be subject to screening.*

Requirements for *Screening*

Requirement no.	Structural requirements for *Screening*	Type	Remarks
6.6.20	A *Series* can have registered no or one *Screening value* and a *Screening value* can form part of no, one or several *Classes.*	O	
6.6.21	A *Class* can have registered no or one *Screening value* and a *Screening value* can form part of no, one or several *Classes.*	O	
6.6.22	A *Basic file* can have registered no or one *Screening level* and a *Screening level* can be included in no, one or several *Basic files.*	O	
6.6.23	A *Simplified record* can have registered no or one *Screening level* and a *Screening level* can be included in no, one or several *Simplified records.*	O	

Requirement no.	Structural requirements for *Screening*	Type	Remarks
6.6.24	A *Document description* can have registered no or one *Screening level* and a *Screening level* can be included in no, one or several *Document descriptions.*	O	

Requirement no.	Functional requirements for *Screening*	Type	Remarks
6.6.25	There must be a service/function for updating information concerning screening code (screening degree, screening authority and screening duration) for a value of *Series, Basic file, Simplified record* and *Document description.*	O	
6.6.26	It must be possible to inherit screening to file, registry entry, document description and document object. It must be possible to override inherited values.	O	
6.6.27	It must be possible to inherit the screening of *Class* to file, registry entry, document description and document object. It must be possible to override inherited values.	O	
6.6.28	There must be a service/function for entirely or partially screening File description.	O	
6.6.29	It must be possible to inherit the screening of *Basic file* to *registry entry*, *document description* and *document object*. It must be possible to override inherited values.	O	
6.6.30	It must be possible to inherit the screening of *Basic file* to *registry entry*, *document description* and *document object*. It must be possible to override inherited values.	O	
6.6.31	There must be a service/function for entirely or partially screening description in a *Record*.	O	

Requirement no.	Requirements for Access codes for exemptions from public registry	Type	Remarks
6.6.32	It must be possible for access codes to be registered on files, records and document descriptions. This indicates that registered information or archived documents must be screened from public access.	O/B	

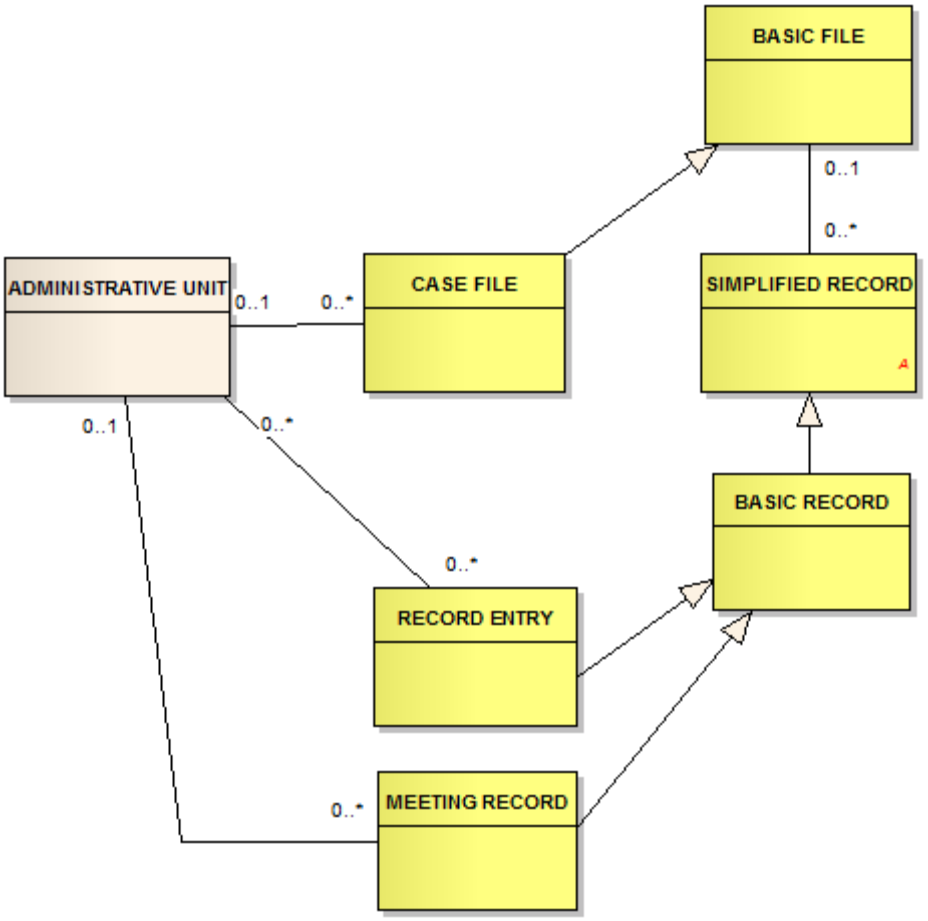
Requirement no.	Requirements for Access codes for exemptions from public registry	Type	Remarks
6.6.33	All access codes that are to be used must be predefined in the core. The access codes are global, i.e. the same codes are used for the entire archive regardless of which external modules make use of the archive.	O/B	
6.6.34	The core must contain a full history of all access codes that are currently or have previously been valid in the archive.	O/B	
6.6.35	For each access code, it must be possible to register an indication of whether a document that has been marked with this access code can be classified as exempt from public access in its entirety, or whether there is reason to only exclude certain information from the document in line with the authority provision in the Freedom of Information Act.	O/B	
6.6.36	There should be a dedicated access code for "temporarily exempt", which can be used until the need for screening has been assessed.	V	
6.6.37	In connection with an access code, it must be possible to mark the following file information in the core as "screened", so that external modules that read from the archive have the following restrictions when the access code is used: • Parts of the file title: The solution must permit either the screening of everything except the first part of the title (e.g. the first line), or alternatively the screening of individual words highlighted by the user. • Classification: This is primarily intended for the screening of object codes that are personal names or national identity numbers. • Information that identifies parties in the case.	O/B	

Requirement no.	Requirements for Access codes for exemptions from public registry	Type	Remarks
6.6.38	In connection with an access code, it must be possible to mark the following file information linked to records in the core as "screened", so that external modules that read from the fonds have the following restrictions when the access code is used: • Parts of the contents description: The solution must permit either the screening of everything except the first part of the contents description (e.g. the first line), or alternatively the screening of individual words highlighted by the user. • Information that identifies the sender and/or recipient.	O/B	
6.6.39	It must be possible to screen document descriptions linked to a record. It must be stated that the record contains document descriptions that are screened in the registry.	O/B	
6.6.40	It must be possible to screen the following information concerning electronic documents using an access code: • all information concerning a document, including different formats and versions of the document.	O/B	
6.6.41	If the access code is marked with an indication that there is reason to only exempt certain information in the document from access, an "official variant" of the document may be created which does not contain this information and which can therefore be exempted from screening.	V	

6.7 Administrative structure

Noark 5 is based around the assumption that it must be possible to carry out administration of the organisation's structure in external solutions. In spite of this, to ensure appropriate recordkeeping, the core imposes certain requirements on these solutions and the way in which the core should be able to relate to them.

Conceptual model for Administrative unit



< Administrative unit>

Metadata for administrative unit

In Noark 5, information concerning administrative structure is not considered to be part of the fonds structure. Such information does not need to be stored in the Noark 5 core, nor should it be transferred to a repository on transfer. However, if the name of the responsible unit is registered on a file or a record (registry entry), this must be included as metadata for these record units.

No.	Name	Type	Occ.	Trans.	Remarks
M583	administrativeUnitName	O	One		
M600	createdDate	O	One		
M601	createdBy	V	One		
M602	finalisedDate	B	One		
M584	administrativeUnitstatus	V	One		
M585	referenceGeneral Unit	B	One		

Requirements for administrative structure

Requirement no.	Requirements for administrative structure	Type	Remarks
6.7.1	All administrative units that are to have access to objects in the core must be identified and recognised by the core.	B	Obligatory for solutions in which administrative units are to have access to objects in the core.
6.7.2	An administrative unit that is no longer to have access to objects in the core must still be identified in the core, but with a status that indicates that it is "Passive".	B	Obligatory for solutions in which administrative units are to have access to objects in the core.
6.7.3	There must be an overview of the period or periods during which each administrative unit has been active.	B	Obligatory for solutions in which administrative units are to have access to objects in the core.

6.8 User administration

Noark 5 is based around the assumption that it must be possible to carry out administration of users of the solution in external systems. Nevertheless, to ensure appropriate archiving, the core imposes certain requirements on these systems and the way in which the core should be able to relate to them.

Metadata for user

Metadata for user should not be transferred, but it must be possible to migrate them between solutions.

No.	Name	Type	Occ.	Trans.	Remarks
M580	userName	O	One		
M581	userRole	O	One		
M600	createdDate	O	One		

No.	Name	Type	Occ.	Trans.	Remarks
M601	createdBy	V	One		
M602	finalisedDate	B	One		
M582	userstatus	V	One		

Requirements for user administration

Requirement no.	The core's requirements for user administration	Type	Remarks
6.8.1	All users that are to have access to units in the core must be identified and recognised by the core.	B	Obligatory for solutions where personally identified users are to be identified in the core.
6.8.2	The core must be able to recognise the administrative context in which the user is working at any time.	B	Obligatory for solutions where personally identified users are to be identified in the core.
6.8.3	A user that is no longer to have access to units in the core must still be identified in the core, but with a status that indicates that it is "passive".	B	Obligatory for solutions where personally identified users are to be identified in the core.

Requirement no.	The core's requirements for user administration	Type	Remarks
6.8.4	There must be an overview of the period or periods during which each user has been active.	B	Obligatory for solutions where personally identified users are to be identified in the core.

6.9 Roles and associated rights

Noark 5 is based around the assumption that each individual public body must be able to define the roles and associated rights that users of the solution are to have, within the framework that is established through the general restrictions in the standard with regard to the freezing of documents and metadata. General administration of the various roles need not be performed in the core. The core only requires the external system to have a solution for administrating access to the core.

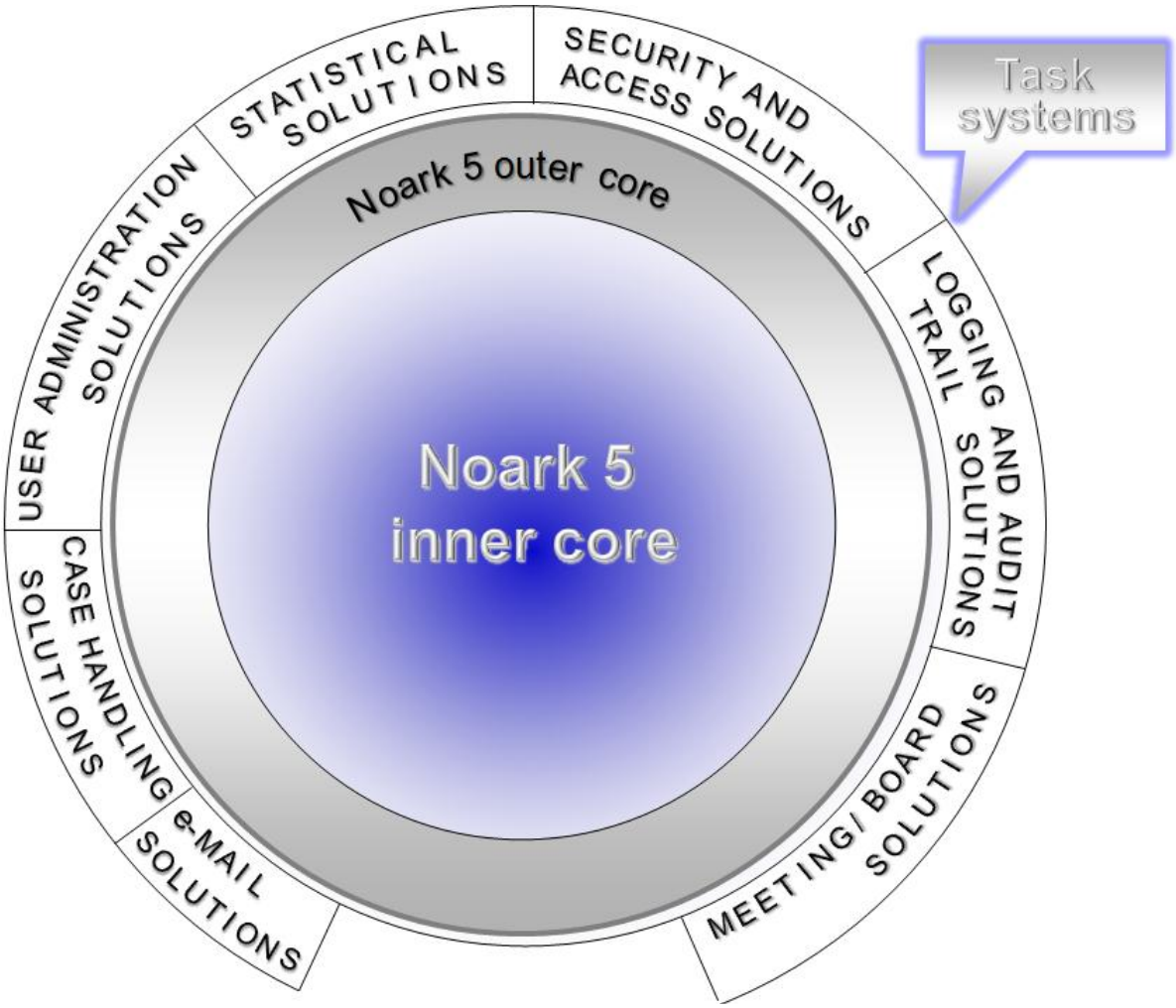
6.10 Use functionality

In order for a task or pre-system to fulfil requirements concerning universal design as set out in legislation and regulations, the outer core must provide for this. An example is the way in which the outer core provides for the appropriate distribution of document content to people with disabilities.

Requirement no.	Functional requirements for use functionality	Type	Remarks
6.10.1	Provision must be made to ensure that the requirements for *Universal Design* as set out in applicable legislation and regulations are fulfilled.	O	
6.10.2	It should be possible to receive messages and texts in both Norwegian language forms (Bokmål and Nynorsk).	V	

Part 3: Noark 5 complete

The following sections contain requirements concerning functions, content and use of external (optional) system solutions that naturally form part of a complete Noark 5 archive solution.
These solutions are no more independent of Noark than they were previously. Each organisation should be able to introduce the task system that best meets its needs.
In relation to Noark 5 inner and outer core, these requirements will act more as guidelines aimed at ensuring good recordkeeping and archiving, than as requirements which must be fulfilled in order to obtain Noark 5 status for the solution.



7 Case handling functions

The principal vision for Complete Noark 5 is that the solution that is introduced must support general case handling (and therefore managers and executive officers) in a functional, user-friendly and effective way, so that the solution is seen as an everyday support tool.

The requirements are not restrictive in the sense that it is these and only these requirements that must be satisfied. In order to establish a solution based on Complete Noark 5, it will also be appropriate to offer entirely different types of functionality than those that are covered in this section. For example, functions for customer care, automated processing of job applications, executive officer portals or the use of cooperation rooms are not considered. This does not mean that these solutions cannot be included as part of the case handling functionality in Complete Noark 5. Both this and other functionality should be offered to the organisations that require this type of functionality.

In other words, this section should not be interpreted as indicating that if a functionality is not required here, then the functionality is not to be developed in a Complete Noark 5 solution.

7.1 Requirements for address register in the case handling function

In order to handle a public body's regular clients, it should be possible to create an address register for the function.

Requirement no.	Requirements for address register in the case handling function	Type	Remarks
7.1.1	There should be functions for establishing a register with names and addresses of clients (address register). It must be possible to use this register to look up information in connection with the record of senders, addressees and parties to a case.	V	

7.2 Requirements for case follow-up in the case handling functions

The solution should have functionality for following up case handling deadlines.

Requirement no.	Requirements for case follow-up in the case handling function	Type	Remarks
7.2.1	There should be functions for retrieving external and internal documents from registry entries that have a processing deadline during a specified period of time.	V	

7.3 Document production

It must in principle be possible for a document that is being processed to be read by those who have this right through dedicated roles and those who have been given this right by the document owner.

Requirement no.	Requirements for document production	Type	Remarks
7.3.1	It should be possible for several people to prepare and edit a large document simultaneously.	V	
7.3.2	It should be possible to create documents and document templates that can freely be defined and sectioned into different parts for different users/authors.	V	
7.3.3	It should be possible to add metadata to a document in XML format. These forms should be documented.	V	
7.3.4	The person that creates a document, the document owner, should have the rights to split the document into sections and assign read, comment, consultation and write access for each of the individual sections.	V	
7.3.5	It should be possible to classify documents and sections according to separate classification forms which specify a reason for screening.	V	
7.3.6	It should be possible to specify whether marking should be shown for sections to which the user does not have read access. If so, the marking should indicate the reason for screening.	V	
7.3.7	The document owner should be able to assign another user the role of document and section owner.	V	
7.3.8	For people who have comment access for a document or section but not write access, it should be possible to link comment notes to the document. It should be possible to easily identify which part of the text has been commented on and who added the comments.	V	
7.3.9	For each section, the document owner should be able to assign read, comment, consultation and where appropriate write access to a unit/department, defined role or defined user, hereinafter jointly referred to as "user".	V	
7.3.10	In connection with the allocation of read and write access to a department, everyone in the department should be able to read, open and write/edit the document or section(s) to which access has been assigned.	V	

Requirement no.	Requirements for document production	Type	Remarks
7.3.11	In connection with the allocation of read and write access to a department, everyone in the department should be able to read, open and write/edit the document or section(s) to which access has been assigned.	V	
7.3.12	When a user has opened a section for writing/editing, it should not be possible for other people to open it, i.e. it is locked for reading and writing/editing by others.	V	
7.3.13	Sections for which the user only has read access should be shown with a special background.	V	
7.3.14	For sections for which the user only has read access, the user should not be able to copy the write-protected text and paste it into another document.	V	
7.3.15	Open sections or sections for which a user has been assigned write access should be displayed in the ordinary way.	V	
7.3.16	Sections for which the user does not have read access should be physically removed for the user.	V	
7.3.17	When the user has finished with the section and finalises it, the locking should be cancelled. Everyone with read access should be able to read the section, and users with write/editing access should be able to write in/edit the section.	V	
7.3.18	It should be possible based on the document overview to see who has been assigned and is working on a document and section.	V	
7.3.19	Only the person who has access to read one or more sections of the document should be able to open one or more sections in the document.	V	
7.3.20	Only users to whom the document owner has assigned access should be able to open a sectioned document.	V	
7.3.21	Individual users should only be able to see the parts of the document for which they have the appropriate access. The document is shown as a continuous document with the sections for which the user has the appropriate access.	V	
7.3.22	Only the defined document owner or the owner of the sections should be able to alter user access rights for the document or section.	V	

Requirement no.	Requirements for document production	Type	Remarks
7.3.23	Undefined users should be able to search freely in the document, but should only be given access to view the parts of the document that are open.	V	
7.3.24	It should be possible to limit the read access rights for a document that is being processed to roles and people who through the setting of parameters have general access to do this, or the roles and people to which the document owner assigns explicit access rights.	V	
7.3.25	There should be parameter-controlled options to define the read access rights for all documents that are being processed.	V	
7.3.26	There should be parameter-controlled options to define the read access rights for one or more specific documents that are being processed, specifically for each individual document.	V	
7.3.27	It should be possible for the document owner to override the parameter setting.	V	
7.3.28	When an inhouse-produced document that is being processed is sent on workflow, case flow or document flow, all recipients of the flow should automatically be authorised for read access for the document, irrespective of their role, administrative unit or authorisation.	V	
7.3.29	There should be access to functions for creating and pre-registering a document from either a word processor or Complete Noark 5.	V	
7.3.30	If documents are pre-registered from a word processor, it should not be necessary to switch to Complete Noark 5. When creating and closing a document, the user should automatically be asked for essential information for registering the document.	V	

7.4 Document templates

It must be possible to establish document templates for all document categories that an organisation uses. It must also be possible to define new document templates.

It must be possible to enter two categories of standard text in the document templates – text that can be altered by the executive officer and text that cannot be altered by the executive officer.

There should be access to functions for creating and pre-registering a document from either a word processor or from Complete Noark 5. If documents are pre-registered from a word processor, it must not be necessary to switch to Complete Noark 5. When creating and closing a document, the user must automatically be asked for information that is required for registering the document.

The document templates must contain fields that correspond to fields in Complete Noark 5. It must be possible to adapt these fields to the needs of the individual organisation. The fields must also be dynamic in relation to the document template that is brought into use. It must be possible to automatically transfer information from fields in Complete Noark 5 to the corresponding fields in the document template. It must be possible to automatically transfer information from one field in the document template to the corresponding field in Complete Noark 5.

In connection with the screening of documents, it must be possible for the executive officer to type in or freely select a reference to authority and for the solution to place the text in the specified place in the document template.

Requirement no.	Requirements for document templates	Type	Remarks
7.4.1	There should be functions for establishing document templates for all document categories that an organisation uses.	V	
7.4.2	There should be functions for formulating and using inhouse-defined document templates.	V	
7.4.3	There should be functions for establishing new document templates.	V	
7.4.4	There should be functions to enable the organisation to create/prepare document templates itself without external assistance.	V	
7.4.5	It should be possible to enter two categories of standard text in the document templates - text that can be altered by the executive officer and text that cannot be altered by the executive officer.	V	
7.4.6	It should be possible to automatically transfer information from fields in Complete Noark 5 to the corresponding fields in the document template.	V	
7.4.7	It should be possible to automatically transfer information from a field in the document template to the corresponding field in Complete Noark 5.	V	

Requirement no.	Requirements for document templates	Type	Remarks
7.4.8	In connection with the screening of documents, it should be possible for the executive officer to type in or freely select a reference to authority and for the solution to place the text in the specified place in the document template.	V	

7.5 Case and document history

It should be possible to easily trace facts for an individual case, whether unfinalised or finalised. This audit trail facility covers:

- What has been done concerning the case, when it was done and who (person or function) did it.

In order to obtain a good overview of case handling, it is also important that the solution presents an overview of the case portfolio, i.e. the stage which the handling process has reached and who is in possession of it. It is desirable to be able to see the following stages:

- New case files or documents that have not been distributed, started or opened.
- Case files or documents that are held by the executive officer and awaiting action from him or her.
- Case files or documents that are pending approval internally.
- Case files or documents that are to be processed by an external body, e.g. by an appeal body or another processing body or within the legal system.

It must be possible to have all documents in the case file and references to other documents (from the internet, case records, etc.) that form part of a case accompany the case file.

Requirement no.	Requirements for case and document history	Type	Remarks
7.5.1	It should be possible to easily trace facts for an individual case, whether unfinalised or finalised.	V	
7.5.2	It should be possible to see what has been done concerning the case, when it was done and who did it (person or function).	V	
7.5.3	It should be possible to view new case files or documents that have not been distributed, started or opened.	V	
7.5.4	It should be possible to view the status of the case file or document, i.e. whether it has the status “not distributed”, “not started” or “not opened”.	V	

Requirement no.	Requirements for case and document history	Type	Remarks
7.5.5	It should be possible to see that case files and documents are being held by the executive officer and awaiting action from him or her.	V	
7.5.6	It should be possible to see that case files and documents have been sent for approval internally.	V	
7.5.7	It should be possible to see that case files or documents are pending processing by an external body, e.g. by an appeal body or another processing body or within the legal system.	V	
7.5.8	It should be possible to have all documents in the case file and references to other documents (from the internet, case records, etc.) that form part of a case accompany the case file.	V	

7.6 Document flow

It must be possible to send a document that is in production forwards and backwards in the line the necessary number of times. The executive officer and line managers must be able to see where the document is at any time. It must be possible to define functions to enable the document to be locked for changes when it is sent (forwarded) or to enable a new version to be automatically created with each dispatch (forwarding). It must be possible to use all functionality for correction and remarks in the associated word processing system on a document that is under production.

The recipient of a document must be notified that he or she has received a document (e.g. through it being placed under a separate tab or being marked in some other way to indicate that it has been received).

In order to document that recipients in the flow have actually performed the task, it must be possible to give a binding "signature" at all stages. This "signature" will also have a non-repudiation function.

It must be possible to have appendices to the main documents and references to other appendices (from the internet, case records, etc.) accompany the document and it must be possible to register remarks in the registry entry.

Metadata for *Document flow*

Metadata for document flow must be grouped into metadata for registry entries. Document flow is optional and may occur one or more times in a registry entry.

No.	Name	Type	Occ.	Trans.	Remarks
M660	flowTo	B	One	A	Obligatory if documents are being sent in flow.
M665	flowFrom	B	One	A	Obligatory if documents are being sent in flow.
M661	flowReceivedDate	B	One	A	Obligatory if documents are being sent in flow.
M662	flowSentDate	B	One	A	Obligatory if documents are being sent in flow.
M663	flowStatus	B	One	A	Obligatory if documents are being sent in flow.
M664	flowRemark	V	One	A	

Requirement no.	Requirements for document flow	Type	Remarks
7.6.1	It should be possible to send a document that is under production forwards and backwards in the line the necessary number of times.	V	
7.6.2	Authorised roles and people should be able to see where the document is at any time.	V	
7.6.3	The document should be blocked for changes when it is sent (forwarded), and if appropriate a new version should be created with each dispatch (forwarding).	V	
7.6.4	It should be possible to use all functionality for editing and remarks in the associated word processing system on a document that is in production.	V	
7.6.5	It should be possible to register remarks concerning the document.	V	
7.6.6	The recipient of a document in flow should be notified that he or she has received a document.	V	
7.6.7	It should be possible to give a binding “signature” at all stages.	V	
7.6.8	It should be possible to have appendices to the main document and references to other appendices (from the internet, case records, etc.) accompany the document.	V	
7.6.9	It should be possible to send a document that is in production for approval in stages (sequential approval).	V	

Requirement no.	Requirements for document flow	Type	Remarks
7.6.10	It should be possible to send a document that is in production for consultation to several parties simultaneously (parallel consultation).	V	
7.6.11	For documents which are in production and sent on sequential or parallel document flow, it should be possible to set parameters to determine whether new versions are to be created for all recipients in the flow.	V	
7.6.12	It should be possible to specify parameters to determine whether versioning should occur for individual roles, units, groups or individuals only. It must be possible to do this on a fixed or ad-hoc basis.	V	

7.7 Workflow

Workflow is a type of functionality that makes it possible to distribute tasks electronically and to follow up and maintain an overview over where the tasks are at any one time. In this way, it enables organisations to have a controlled, internal work process across units and locations. In other words, workflow involves the control of communication between different people and roles and information systems that are affected by the work process.

It is important that functions for workflow can:

- Model processes simply and clearly.
- Provide templates and wizards that ensure consistent use and effective re-use.
- Log and report non-conformances and statistics.

The workflow function should also provide for:

- Integration with other functions
- Security
- Flexibility
- Scalability

It must be easy to expand the function with the organisation as changes are implemented in terms of the number of employees, the number of processes that are automated and the way in which communication and dialogue takes place.

The following minimum functionality must be available in a workflow:

Requirement no.	Requirements for workflow	Type	Remarks
7.7.1	It should be possible to dispatch (send) a task, case or document that the executive officer has completed on workflow internally.	V	

Requirement no.	Requirements for workflow	Type	Remarks
7.7.2	It should be possible to set up a workflow (either predefined or ad-hoc) with predefined activities and milestones.	V	
7.7.3	It should be possible to predefine both sequential workflow and simultaneous workflow.	V	
7.7.4	It should be possible to add control functionality for each activity, e.g. so that the task or case does not progress in the flow until all activities have been completed.	V	
7.7.5	It should be possible to add time-specific activities, e.g. if a case has not been opened for a given number of days, it must automatically be forwarded in the solution to an alias or similar.	V	
7.7.6	It should be possible to dispatch (send) a task, case or document that the executive officer has completed on workflow internally.	V	
7.7.7	It should be possible to dispatch (send) a task, case or document that the executive officer has completed, on staged workflow internally, i.e. it is automatically forwarded to the next stage when the previous stage has finished with the task.	V	
7.7.8	It should be possible for all recipients in the staged internal workflow to link a remark or document to the original task, case or document.	V	
7.7.9	When a document that the executive officer has finished with is sent on workflow internally, it must not be possible for the document that is in the workflow to be altered or deleted.	V	
7.7.10	It should be possible for authorised personnel to override the predefined workflow.	V	
7.7.11	It should be possible to give a binding “signature” at all stages.	V	

Requirement no.	Requirements for workflow	Type	Remarks
7.7.12	Audit trail elements from a workflow should be logged and preserved. These audit trail elements are: • Who has received the task/case/document • Who has read or edited the task/case/document • How each recipient has handled the task/case/document (e.g. approved/not approved). • What the people concerned have done (e.g. read/edited/forwarded). • Any binding "signature". • Remarks that have been entered in the workflow/task/case/document	V	
7.7.13	There should be a function for searching for and retrieving external and internal documents with a processing deadline during a specified period of time.	V	
7.7.14	It should be possible to limit the search based on the case handling unit and executive officer.	V	
7.7.15	There should be a function for the automated notification of internal or external deadlines that are in the process of expiring.	V	

8 E-mail functions

This chapter sets out the Noark 5 requirements for e-mail functions and integration.

Introduction

In recent years, electronic mail, e-mail, has become an important labour-saving tool for the public administration sector. Virtually every agency uses e-mail and the level of usage is constantly increasing. Requirements for the handling of e-mail in Noark 5 are therefore necessary.

For all documents of archival value that are received by or sent out by an organisation as e-mail, the recordkeeping obligation applies in the same way as for all other documents. The Archives Regulation permits public bodies that use e-mail to also have a central incoming e-mail system for
e-mail sent to the organisation. E-mail that is received by the central incoming e-mail system must be opened by the registry.

By placing the incoming mail systems with the units that have an archive function, e-mail will follow the same path as ordinary letter mail as closely as possible. This will ensure that an immediate assessment is carried out to determine whether or not the incoming e-mail is covered by the recordkeeping obligation. However, even with a central incoming e-mail system, e-mail is often sent directly to an executive officer. The executive officer concerned will then be obliged to register the e-mail if it is considered to be a document for the organisation.

Noark 5 takes into account the extensive use of e-mail as a method for sending documents, both internally within the organisation and to external parties. There is therefore a stronger focus on interaction between e-mail systems and Noark 5-based solutions in order to make the everyday tasks relating to record more efficient. A Noark 5 solution must satisfy the requirements for the record of documents in connection with receipt and sending by e-mail.

Definitions

The standard protocol for the use of e-mail is defined by the Network Working Group in standards RFC 2821 and RFC 2822. Noark 5 uses this as a basis as regards e-mail.

E-mail is normally referred to as a document captured from an application that contains a complete set of data from an e-mail transaction. Although RFC2822 defines the syntax for e-mail transactions, there is no standard that defines the data format that must be used when the e-mail transaction has been captured as documents.

Although e-mail applications from different suppliers can freely transfer messages between themselves (based on the e-mail protocols defined in RFC2821/2822), it is not possible to capture an e-mail transaction from an e-mail application as a document and guarantee that the other application will be able to read it, as different e-mail providers sometimes use their own proprietary formats to capture e-mail. The automated export of metadata from e-mail messages can therefore not be based on standards.

Terminology

E-mail function is a recurring term. In this context, it means the way in which Noark 5 is integrated with an e-mail system. This will appear as an e-mail function for the user. It is only intended that Noark 5 will be integrated with e-mail systems that read the e-mail addresses of the organisation, not private e-mail addresses. It is not the intention that Noark 5 should be integrated with e-mail systems other than the organisation's.

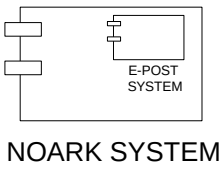
In this chapter, *file structure* means the structure of the various files or directories that a user has in the e-mail function. Examples of such files are Inbox and Outbox.

Modules are the various components in Noark 5, depending on how the supplier has decided to integrate the function with respect to the Noark 5 core. E-mail can for example be accessed via an external e-mail system, via the organisation's own case handling portal or via other functions.
In this context, references to *automatically* or *automatic* mean that an action will be performed by machine and checked by a user where appropriate. *Manually* on the other hand means an action that is performed by a user.

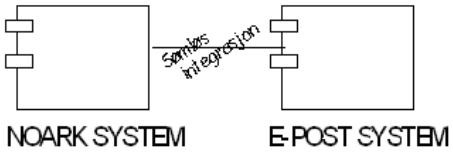
It must be possible to use an internal, in-built e-mail system (see Figure 10-1 "In-built e-mail") or an external e-mail system that is *seamlessly integrated*[11] with Noark 5; see Figure "Seamlessly integrated e-mail":

The following requirements concerning the use of e-mail functions in Noark do not distinguish between these implementations. For Noark 5, two principles apply:

1. From relevant modules in the Noark 5 solution, you must be able to send and dispatch documents as e-mail directly, without having to exit and enter modules.
2. From the organisation's e-mail system, you must be able to register incoming e-mail and attachments without having to exit and enter modules.



Inbuilt e-mail



Seamlessly integrated e-mail

8.1 General e-mail functionality

There are three main functions for e-mail integration in Noark 5.

1. Send e-mail as a case document
2. Send case document by e-mail
3. Register incoming e-mail

[11] "Seamless integration" is an integration solution where the user does not need to do anything special when using the integrated function. It is also often used when two applications use the same physical underlying database.

Requirement no.	Functional requirements for general e-mail functionality	Type	Remarks
8.1.1	In a Complete Noark 5 solution, there should be full integration with the organisation's e-mail system, either with an internal (in-built) e-mail function or through a seamlessly integrated (external) e-mail function for the organisation.	V	
8.1.2	In the Noark 5 solution, it should be possible to dispatch e-mail as a case document.	V	
8.1.3	In the Noark 5 solution, it should be possible to dispatch case documents as e-mail directly from relevant modules.	V	
8.1.4	It should be possible to register incoming e-mail (with or without attachments) directly from the organisation's chosen e-mail function.	V	
8.1.5	In the Noark 5 solution, it should be possible to send case documents (as a copy) as attachments to an e-mail directly from relevant modules.	V	
8.1.6	There should be a service/function to enable the message text in an inhouse-produced e-mail to be sent on document flow internally within the organisation before dispatch in the same way as an ordinary text document.	V	

Document capture, e-mail header and e-mail message

An e-mail is often referred to as consisting of two parts: an *e-post header* and an *e-mail message*. An e-mail header normally consists of the sender, date and time of sending, the addressees to which it has been sent and a subject. The e-mail message is the actual content of the e-mail. If an e-mail has been sent with an empty message field but the e-mail contains an attachment, the e-mail message could in principle still be of archival value.

Requirement no.	Requirements for document capture, e-mail header and e-mail message	Type	Remarks
8.1.7	There should be a service/function which makes it possible to automatically register and archive documents received by e-mail.	V	
8.1.8	In connection with the archiving of e-mail in the Noark 5 solution, the e-mail and any attachments must be automatically archived in a consistent, integrated format that reproduces both the e-mail header and the e-mail message.	B	Obligatory for functions with e-mail integration

Requirement no.	Requirements for document capture, e-mail header and e-mail message	Type	Remarks
8.1.9	The e-mail header and e-mail message must be collated and archived as a single collective document that cannot be altered.	B	Obligatory for functions with e-mail integration
8.1.10	The following minimum metadata from the e-mail header must be included in the collated document: • Sent: date and time • Received: date and time (applies to incoming e-mail) • Addressee(s): All addressees: • CC addressees: All CC addressees • Sender: • Subject: Content of the subject line	B	Obligatory for functions with e-mail integration
8.1.11	There must be functionality for the automatic record and archiving of outgoing and incoming e-mail with or without attachments. It must be possible to register the following metadata automatically in the Noark 5 solution: • Sent: date and time • Received: date and time (applies to incoming e-mail) • Addressee(s): All addressees: • CC addressees: All CC addressees • Sender: • Subject: Content of the subject line • Electronic signature: Where it exists • Certificate(s): Where they exist	B	Obligatory for functions with e-mail integration
8.1.12	It should be possible to specify parameters to control the Noark 5 solution in connection with the dispatch of e-mail as case documents or the dispatch of case documents by e-mail, so that: • The Noark 5 solution automatically registers and archives the e-mail and any attachments. • The Noark 5 solution automatically handles the e-mail and any attachments in line with predefined rules in the solution. • The Noark 5 solution automatically gives a message to the user asking whether the e-mail and any attachments are to be registered and archived. • The Noark 5 solution is based on manual routines.	V	

Requirement no.	Requirements for document capture, e-mail header and e-mail message	Type	Remarks
8.1.13	It should be possible to specify parameters to control the Noark 5 solution in connection with the receipt of e-mail and any attachments so that: • The Noark 5 solution automatically registers and archives (and where appropriate also distributes) the e-mail. • The Noark 5 solution automatically handles the e-mail and any attachments in line with predefined rules in the solution. • The Noark 5 solution automatically gives a message to the user asking whether the e-mail and any attachments are to be registered and archived. • The Noark 5 solution is based on manual routines.	V	

8.2 Dispatching e-mail as case documents

"Dispatching e-mail as case documents" means that it is the e-mail itself and any attachments that constitute the public body's formal case document and that the case document is sent as e-mail. A function for dispatching e-mail as a document should be available and integrated in the Noark 5 solution.

Requirement no.	Requirements for dispatching e-mail as case documents	Type	Remarks
8.2.1	There should be a service/function for dispatching an e-mail and any attachments as the organisation's case document, directly from the Noark 5 solution.	V	
8.2.2	The dispatching of e-mail as case documents must be logged.	B	Obligatory for functions with e-mail integration
8.2.3	There should be a service/function for dispatching e-mail as a case document in connection with the use of exchange format.	V	

8.3 Dispatching case documents by e-mail

"Dispatching case documents by e-mail" means that the organisation's formal dispatch of the case document is as an attachment to an e-mail. The e-mail function is therefore the method of sending and the e-mail message itself can be either empty or contain a standard transmission text. A function for dispatching case documents by e-mail should be available and integrated in the Noark 5 solution.

Requirement no.:	Requirements for the dispatching of case documents by e-mail	Type	Remarks
8.3.1	There should be a service/function for dispatching case documents via e-mail from the Noark 5 solution.	V	
8.3.2	In connection with the dispatch of case documents by e-mail, the solution should complete the e-mail's subject field with the content description from *Record.*	V	
8.3.3	In connection with the dispatch of case documents by e-mail, the solution must comply with the applicable regulations as regards information that is screened or graded or other information that must or can be exempted from public access.	B	Obligatory for functions with e-mail integration
8.3.4	The dispatching of case documents by e-mail must be logged. *Remarks: Requirements for logging are also set out in a separate section.*	B	Obligatory for functions with e-mail integration

Specification of sender for dispatch

Requirement no.:	Requirements for the specification of sender for dispatch	Type	Remarks
8.3.5	In connection with the dispatch and other sending of case documents by e-mail, the record and the documents concerned must be assigned information that confirms "Sent by e-mail".	B	Obligatory for functions with e-mail integration
8.3.6	In connection with the dispatch of documents by e-mail, the solution should set the organisation's central e-mail address as the proposed sender.	V	
8.3.7	It should be possible to override the "sender's e-mail address", which is set automatically by the Noark 5 solution, to another e-mail address that an authenticated executive officer has access to and the rights for. *Remarks: This could for example be the case handling department's e-mail address or the executive officer's e-mail address.*	V	
8.3.8	It should also be possible to override the "sender's e-mail address" on a permanent basis.	V	

Specification of addressee(s) for dispatch

During the dispatch of case documents by e-mail, all predefined addressees in the record should normally receive the dispatch. It should be possible for the executive officer to override and expand the predefined information. If there are no e-mail addresses or the specified e-mail addresses are incorrect, the executive officer should be able to edit the e-mail addresses of the addressees concerned. Overriding and alteration of omissions and errors must be added to the information on the addressee.

Requirement no.	Requirements for the specification of addressee(s) for dispatch	Type	Remarks
8.3.9	In connection with the dispatch of case documents via e-mail, the solution should set up all "predefined addressees" (addressee list) that are linked to the relevant *Record* as suggested e-mail addressees.	V	
8.3.10	The option to alter the e-mail's addressee list should be available as a function during the dispatch of e-mail.	V	
8.3.11	If, in connection with a dispatch, the e-mail addresses are altered in relation to the standard addressee list, information on this alteration should be saved.	V	
8.3.12	It should be possible to manually override the predefined e-mail address in the addressee field in connection with dispatch.	V	

Case documents that are to be omitted from dispatch

Dispatches of case documents should in principle be complete, which means that they should include the main document and all appendices. If despite this it is not possible to enclose all case documents with the e-mail dispatch because of the document's format or for other reasons, the Noark 5 solution should be set up so that dispatch can be carried out, but it should also include functionality for notifying the user of documents (attachments) that are not included in the dispatch.

Requirement no.	Requirements for case documents that are to be omitted from dispatch	Type	Remarks
8.3.13	In connection with the dispatch of documents by e-mail, there should be a service/function for specifying which documents are to be *omitted* from the dispatch.	V	
8.3.14	There should be a service/function for registering remarks on the case documents that are not included in a dispatch.	V	
8.3.15	In connection with dispatch, the solution should generate a message text which gives brief information on any case documents that are not included in the e-mail dispatch.	V	

Requirement no.	Requirements for case documents that are to be omitted from dispatch	Type	Remarks
8.3.16	For the case documents that are *not* included in a dispatch, a system-generated message text and any remarks registered by the executive officer must *always* be included in the e-mail dispatch.	V	

8.3.1 Dispatch control

In connection with the dispatch of case documents, the Noark 5 solution should perform a series of predefined checks before the documents can be dispatched by e-mail. This involves checks on:

- Access/right data
- The case documents
- The exchange format

Requirement no.:	Requirements for dispatch control	Type	Remarks
8.3.17	The Noark 5 solution must not permit documents to be dispatched by e-mail contrary to the restrictions that are imposed by access and rights data and the addressee's authorisation for the same.	B	Obligatory for functions with e-mail integration.
8.3.18	The exchange format should be checked upon dispatch.	V	
8.3.19	If document formats and/or the use of electronic signatures do not correspond to the exchange format's information on the addressee, the dispatch must be cancelled and the user must receive an error message.	B	Obligatory for functions with e-mail integration.
8.3.20	Notwithstanding the above, it should still be possible to send a cancelled dispatch when it has been approved by an executive officer with authorisation to carry out this process.	V	Obligatory for functions with e-mail integration.

8.3.2 Formatting of case documents sent by e-mail

Requirement no.:	Requirements for the formatting of case documents	Type	Remarks
8.3.21	In connection with the dispatch and sending of case documents by e-mail, it must be possible to specify using parameters that the archival format is to be used as the standard format.	B	Obligatory for functions with e-mail integration.
8.3.22	It must be possible to choose whether the production format is to be used in connection with the dispatch and	B	Obligatory for functions with e-

Requirement no.:	Requirements for the formatting of case documents	Type	Remarks
	sending of case documents by e-mail.		mail integration.

8.4 Record of case documents received by e-mail

In a Noark 5 solution, there should be services/functions for the direct record and archiving of e-mail and case documents received by e-mail.

It should not be necessary to manually move or copy across documents from the e-mail module to the Noark 5 solution. It should be possible to register the entire e-mail message and attachments or certain attachments only. The e-mail message, including the e-mail header, should always be included as a separate case document, as it provides information on the dispatch.

A distinction is made between registering and archiving incoming e-mail and documents with and without exchange format.

Requirement no.:	Requirements for the record of case documents received by e-mail	Type	Remarks
8.4.1	Information from the e-mail, the e-mail header, e-mail message and attachments should be presented clearly in a way which facilitates further record of all or part of the e-mail dispatch.	V	
8.4.2	It should be possible for the executive officer to view the contents of the attachments of an e-mail via a quick-view function, or via a link to the program that can read the files.	V	
8.4.3	It should be possible for an executive officer to specify what is to be registered as the main document and what are to be attachments from a mail dispatch.	V	
8.4.4	It should be possible to specify that only certain attachments to a dispatch that is received must be registered. The e-mail itself must always be registered.	V	
8.4.5	It should be possible to document in the remarks field or elsewhere why certain attachments are not being archived, whether this is due to the document format or other reasons.	V	

Requirement no.:	Requirements for the record of case documents received by e-mail	Type	Remarks
8.4.6	It should be possible for an executive officer to set up a system parameter which results in the executive officer automatically either being set as the executive officer upon the creation of a new file or not being set as case-responsible upon the creation of a new file. It should be possible to override this.	V	
8.4.7	It should be possible to set up a system parameter which results in the executive officer automatically either being set as the responsible executive officer upon the creation of a new record, or not being set as the responsible executive officer upon the creation of a new record. It should be possible to override this.	V	
8.4.8	Noark 5 should have functionality which ensures that it is the "display name" of the sender/addressee/CC addressee (where one exists) that is included in the archived document that is created on the basis of an e-mail header and e-mail message.	V	
8.4.9	Noark 5 should have functionality which ensures that it is the "display name" of the sender/addressee/CC addressee (where one exists) that is included as the sender/addressee metadata in the registry.	V	

Creation of a new file

In many cases, it will be necessary to create a new file when registering incoming e-mail.

Requirement no.:	Requirements for the creation of a new file	Type	Remarks
8.4.10	It should be possible to specify whether a new file is to be created or whether an existing file via a directly accessible function is to be used during the record/archiving of incoming e-mail.	V	

Searching for files

If incoming e-mail and documents are to be registered on an existing file, there must be functionality for searching for a file from the e-mail function directly.

Requirement no.:	Requirements for searching of files	Type	Remarks
8.4.11	It should be possible to search for a file/record via a quick-search function based on case number, sender, date	V	

Requirement no.:	Requirements for searching of files	Type	Remarks
	or subject (content) in order to register e-mail. This option should be directly available as a function during the record of e-mail.		

8.5 Copy of case documents by e-mail

It must be possible for an organisation to send a copy of one or more case documents by e-mail.

Requirement no.:	Requirements for copy of case documents by e-mail	Type	Remarks
8.5.1	It must be possible to send a collective copy of one, several or all case documents linked to a record with e-mail in a single dispatch.	B	Obligatory for functions with e-mail integration.
8.5.2	It must be possible for the sending of documents as a copy to be logged in the Noark 5 solution.	B	Obligatory for functions with e-mail integration.
8.5.3	It must be possible to send a copy of a file, i.e. all main documents and appendices from all records in the file.	B	Obligatory for functions with e-mail integration.
8.5.4	It should be possible to retain the structure in connection with such a dispatch, so that it is possible to see which case documents are linked together.	V	
8.5.5	It should be possible to send a copy and specify that only the main document is to be sent.	V	

8.6 E-mail security

The requirements for security in connection with the dispatch and receipt of e-mail are intended to take into account considerations relating to:

- Availability – that information is available to authorised users
- Confidentiality – that information is not disclosed to unauthorised persons
- Integrity – that information is not altered without authorisation

The following security requirements are not intended to be obligatory for all Noark 5 solutions. Each administrative body must itself assess which of the security requirements are relevant, based on the organisation's security policy.

The general principle behind the security requirements in this section is that each organisation must be able to choose its own security policy, within the framework of the various regulations that apply to the organisation.

Requirement no.:	Requirements for security	Type	Remarks
8.6.1	There must be functions which enable a public body to establish the required level of security.	O	

8.6.1 Security management concerning incoming and outgoing e-mail

In order to increase the level of confidence of the sender and the addressee that the e-mail has been received by the organisation, it must be possible to establish routines that utilise the option of sending a rapid response to incoming e-mail.

Requirement no.:	Requirements for security management for incoming and outgoing e-mail	Type	Remarks
8.6.2	Incoming e-mail should always be checked against the security mechanisms that are defined for the Noark 5 solution.	V	
8.6.3	The Noark 5 solution should be able to acknowledge incoming e-mail with or without attachments (based on acknowledgement rules in the solution).	V	
8.6.4	It should be possible to use automatic acknowledgement of e-mail (e.g. when the e-mail/document is registered).	V	
8.6.5	Acknowledgement that the addressee has received the e-mail should be available and comprehensible to the executive officer who sent the e-mail.	V	
8.6.6	If automatic acknowledgement of the receipt of e-mail is used, it should be stated that the acknowledgement is automatic.	V	
8.6.7	The Noark 5 solution should have a function for adding acknowledgement information (delivered, opened/read, failed) from the e-mail system to the Noark 5 solution's addressee information for the record.	V	
8.6.8	Outgoing e-mail should always be checked against the security mechanisms that are defined for the Noark 5 solution.	V	
8.6.9	The level of security in the Noark 5 solution should make it possible to prevent documents being sent by e-mail.	V	
8.6.10	The executive officer should be notified of the access code and general restrictions that have been set for certain documents (files, classifications) if an attempt is made to dispatch these documents by e-mail.	V	

Requirement no.:	Requirements for security management for incoming and outgoing e-mail	Type	Remarks
8.6.11	It should be possible to set up roles and users of the Noark 5 solution in such a way that they can override blocks on dispatch that are defined as standard.	V	
8.6.12	Within fonds, it should be possible to specify blocks on dispatch at any hierarchical level in the fonds structure. Blocks on dispatch must be inherited by underlying levels.	V	
8.6.13	It should be possible to set up the Noark 5 solution so that screened documents can be sent to certain, predefined addressees.	V	

8.6.1.1Time-stamping of e-mail

In connection with electronic communication, notation indicating when an electronic document was sent or received by an organisation can be ensured through the use of logs (time-stamping). The log function can be performed by one or more of the parties in the communication and/or a third party.

Requirement no.:	Requirements for the time-stamping of e-mail	Type	Remarks
8.6.14	The Noark 5 solution should have security functions that can manually or automatically retrospectively document when an e-mail was sent or received by the organisation based on defined logging rules in connection with fonds, series, file or document.	V	

8.6.1.2 Non-repudiation in connection with the use of e-mail

Non-repudiation means that the sender/addressee cannot subsequently deny having performed actions that they have actually performed. Another aspect of non-repudiation is that the sender or addressee may need to document to a third party the communication that has taken place between the parties.

Requirement no.:	Requirements for non-repudiation in connection with the use of e-mail	Type	Remarks
8.6.15	It should be possible for the Noark 5 solution to have security functions which ensure that the message was actually delivered to the addressee (“proof of delivery”).	V	

8.6.16	It should be possible for the Noark 5 solution to have security functions that can verify that the sender actually did send the e-mail concerned even though the sender may wish to deny that he or she did so ("non-repudiation of origin").	V	
8.6.17	It should be possible for the Noark 5 solution to have security functions that can verify that the addressee has actually received the e-mail concerned, even though the addressee may wish to deny that he or she did so ("non-repudiation of delivery").	V	

8.6.2 Requirements for confidentiality

In the same way as with ordinary letter mail, a high level of security must be created in connection with the use of e-mail, so that unauthorised persons cannot read or alter the content of other associated information concerning the e-mail message.

Requirement no.:	Requirements for confidentiality	Type	Remarks
8.6.18	It should be possible for the Noark 5 solution to have security functions which ensure that only the addressee can read the e-mail message and associated documents ("content confidentiality").	V	
8.6.19	It should be possible for the Noark 5 solution to have security functions which can ensure that all users can have their own e-mail address list ("message flow confidentiality").	V	
8.6.20	It should be possible for the Noark 5 solution to have security functions which can ensure that no one can use other people's e-mail addresses without being given authorisation ("secure access management").	V	
8.6.21	It should be possible for the Noark 5 solution to have security functions that can manually or automatically address addressees in a "blind copy" (bcc=blind carbon copy)[12] for outgoing e-mail with documents based on defined addressing rules in connection with fonds, file or document.	V	

[12] When sending an e-mail to many addressees, it may be appropriate to use a blind copy. A blind copy or bcc (Blind Carbon Copy) makes it possible to "hide" the addressees of the e-mail message. Unlike addresses in the "To:" and "Copy to" fields, the addresses in the blind copy field are not visible to other recipients of the e-mail.

Requirement no.:	Requirements for confidentiality	Type	Remarks
8.6.22	An organisation must have the facility to deselect the function in order to address e-mail to addressees in "blind copy".	V	

8.6.3 Encryption of e-mail

The encryption of documents distorts the content of an e-mail so that unauthorised persons cannot read it.
Encryption makes the documents illegible for everyone except those with the correct "key" with which to "open" the document.

Requirement no.:	Requirements for the encryption of e-mail	Type	Remarks
8.6.23	It should be possible for the Noark 5 solution to have security functions that can manually or automatically handle the encryption of outgoing e-mail and documents (attachments) and the decryption of incoming e-mail and documents based on defined encryption rules in connection with fonds, files or document.	V	
8.6.24	Within fonds, it should be possible to specify rules for the encryption of documents at each hierarchical level in the fonds structure in the Noark 5 solution.	V	
8.6.25	Rules for the encryption of documents must be inherited by underlying levels in the fonds structure.	V	
8.6.26	It should be possible to set up both roles and users of the Noark 5 solution in such a way that they can override the rules for encryption in connection with dispatch which are defined as standard.	V	

8.6.4 Integrity protection through electronic signing

Electronic signature is a collective term for a number of technologies that can be used for authentication and where appropriate other security functions. Section 3(1) of the Act on electronic signatures defines an electronic signature as: "data in electronic form which are linked to other electronic data and which are used to check that these data originate from the person who is stated as the signatory".

Digital signature, which is a form of electronic signature, is a technology based on cryptographic methods, which provides support for authentication, integrity protection, non-repudiation and confidentiality protection, i.e. encryption.

Signing is based on the document being marked with an encrypted checksum and a "code" which indicates who sent the document and ensures that the document has not been altered since it was sent.

Requirement no.:	Requirements for integrity protection through electronic signing	Type	Remarks
8.6.27	It should be possible for the Noark 5 solution to have security functions that can manually or automatically digitally sign outgoing e-mail with documents based on defined signing rules in connection with fonds, file or document ("authenticity")[13].	V	
8.6.28	It should be possible for the Noark 5 solution to have security functions that can verify that the sender of an incoming e-mail is who he claims to be ("authenticity").	V	
8.6.29	It should be possible for the Noark 5 solution to have security functions which can verify that the documents have not been altered since dispatch by e-mail ("content integrity")[14].	V	

[13] In this context, authentication is used in the sense of: verifying (confirming) the claimed identity of the sender or recipient in a communication system.
[14] "Content integrity" or data integrity means that the recipient can verify that the content of a document has not been altered from the time the message was sent until it was received.

9 Meeting and board functions

The need for an electronic function that can facilitate meeting and board handling is particularly great in the municipal administration sector. This section is therefore particularly aimed at the needs of the municipal sector and we have chosen to use examples from this sector in order to demonstrate how a meeting module is set up.

Public bodies other than municipal and county councils (e.g. committees, boards and councils within universities and government bodies) usually need a simpler function for meeting handling than that described here. Non-municipal bodies will also use very different terminology for their meeting handling than that used by municipal organisations. It must therefore be possible for each individual public body to select only parts of the functions that are described, so that functions that are optimised for each organisation are established.

Meeting and board handling will often take place outside the general case records system and there will be a need for special technical and structural functions for this type of case handling.

The requirements concerning meeting handling only cover electronic documents and electronic case handling.

Information and documents that are generated in connection with meeting handling must be preserved in the form of:

- documents and associated metadata in a series
- decision-making body and associated metadata

Each organisation can decide whether information that is of archival value should be stored in a separate series in the meeting handling module or in the case records, or whether the documents should be assigned a separate class in the classification system. It is not obligatory to create a separate series for meeting documents, but it must be possible to create such a series.

9.1 Functional description

9.1.1 Terminology in meeting handling

There are significant differences between municipal and government bodies as regards the use of the terminology presented below. We have however decided to define selected terms in order to create a consistent structure in the chapter. In Noark 5, the following terminology linked to the meeting handling module will be used.

Term	Explanation
Decision-making body	Collective term for boards, committees, councils, meetings, etc.
Decision-making body type	Political body, body with decision-making authority, advisory body

Term	Explanation
Delegated case	Case where a subcommittee, the spokesman or head of administration (deputy mayor) has been given authority to assess an enquiry and reach a decision.
Interpellation	Interpellation/enquiry from a member of the committee which can be presented either in writing or verbally in the course of the meeting.
Queue list	Cases that have been fully processed by the administration are declared as being ready for processing by the decision-making body by placing them in a queue list.
Meeting	A meeting within a decision-making body in order to process cases in a case list.
Meeting folder	A meeting folder can contain collated documentation from the processing and history of one or many cases. This could concern the following information elements: Case lists, case plans, case drafts, minutes and approval of minutes, case documents with or without appendices. Section 30 of the Local Government Act: A meeting folder must be kept of the discussions that take place in all publicly elected bodies. The municipal executive and county council must establish rules concerning the creation of meeting folders.
Meeting minutes	Collation of one or more case minutes in connection with an individual meeting. Comprises shared information, such as time, place, attendance, etc. and case minutes for the cases being considered.
Meeting case	A delimited problem that a decision-making body must consider in a meeting.
Meeting case status	For case plan, case plan locked, case rejected, case finalised (“reported”) *case deferred*
Meeting case type	Political case, delegated case, referred case, interpellation (in N4, this is called “Enquiry”) and unregistered case “any other business”), directors’ meeting, etc.
Political case	Cases that are subject to political handling, prepared by the administration.
Referred case	Documents that have been presented to a committee for information purposes. The documents can, but do not need to, belong to a case in the fonds. Normally specified in the meeting minutes.

Term	Explanation
Case plan	Collective document which can contain a case list, case draft, case documents and, where appropriate, the final processing from the recommendation committee.
Case list	List of meeting cases from the queue list that are to be considered at a given meeting.
Case minutes	Minutes from an individual case that is to be considered by a committee/meeting. In Noark 4, case minutes are defined as a separate document. It should also be possible to define it as such in Noark 5.
Unregistered case	Arises outside the administration, often as an "any other business" item for a meeting. Such a case can either be decided on in the meeting or it can be referred for further investigation and case handling within the administration.

A meeting case within the municipal administration can have one of two origins:

1. The case is an *administrative case,* also known as a "political case", i.e. the result of the administration's work, which is to be submitted to one or more decision-making bodies.
2. The case is an *unregistered case,* i.e. it arises outside the administration, often as an "any other business" item for a meeting. Such a case can either be decided on in the meeting or it can be referred for further investigation and case handling within the administration.

Within government administration, other definitions of what a meeting case is and how they arise are used.

A more detailed description of the two case types used within municipal administration appears below.

If a meeting case originates from an administrative case, the meeting case must retrieve all information concerning the case from the administrative case. The case draft should be completed by the executive officer before the case can be referred to the decision-making body.

An unregistered case is a case which has no previous case handling in an ordinary administrative case and which must therefore be created in connection with the meeting. It must be possible to create it as an independent document or a registry entry (if it is to be registered). The decision-making body will be the owner of the case.

Within government bodies, other designations and case types will be used. In connection with the development of functions for these, it is important to define and use these distinct terms.

It must be possible to periodise and transfer information and documents that form part of meeting handling in line with the requirements in sections 4.2.8 Document capture, 4.2.10 Periodisation, 4.2.11 Preservation and disposal and 4.2.12 Transfer.

9.1.2 Information elements in the meeting handling

A list of information elements that are important in meeting handling is presented below. The list is not exhaustive and must also be viewed in context with the Noark 5 specification in general.

Information element	Content	Storage place
Decision-making body	Name, members, administrative position (in accordance with the administrative structure).	In administrative structure
Meeting	Numbering, participants	In the meeting file
Meeting summons	Can specify the time and place of the meeting and a case list showing which cases are to be considered. As part of the document, the case draft and recommendations belong to the individual cases shown in the case list, plus any appendices. Shows who is to participate in the meeting.	In the meeting file
Case list	Numbered case list, links to cases	In the meeting file
Case draft	Text presentation of the case, recommendation text	Administrative case: as an ordinary case document linked to the case, and in the meeting file. Other meeting types: in the meeting file.
(Meeting) decision	Text presentation of the decision taken concerning a case during the meeting.	Document linked to the case that the decision concerns. Can also be included in the meeting file.
Meeting folder	Collation of all information elements in a meeting.	In the meeting file or as a separate case.

The way in which the information elements in the series for meeting handling can be structured viewed in the light of the fonds structure in general is shown below. This is intended simply as an example and does *not* describe the actual implementation of this structure.

- Information on each individual meeting is stored as a meeting file and associated metadata concerning the meeting.
- The file ***Delegated cases*** contains administrative cases that have been handled as delegated cases.
- The file ***Referred cases*** contains cases that are to be referred.
- The file ***Case list*** contains cases that are to be included in the case list. These cases can be of any type, either of administrative origin or others which have their origin in other decision-making bodies for example.
- The file ***Interpellations*** contains documents in interpellation cases that are to be considered at the meeting.

- …etc.

9.2 General requirements

Requirement no.	Requirements for administrative case	Type	Remarks
9.2.1	It must be possible to manage meeting and board handling in accordance with Noark 5 core requirements.	B	Obligatory for function for meeting and board handling.
9.2.2	It must be possible to define separate requirements for services/functions that extend beyond what is required under this section. It is assumed that these requirements will not conflict with Noark 5's core requirements.	B	Obligatory for function for meeting and board handling.

9.3 Meeting case types

9.3.1 Administrative case

Requirement no.	Requirements for administrative case	Type	Remarks
9.3.1	There should be functions for ensuring that a meeting case can retrieve all information on the case from the administrative case.	V	
9.3.2	It should be possible to specify that the case draft must be completed by the executive officer before the case is referred to the decision-making body.	V	

9.3.2 Unregistered case

Requirement no.	Requirements for unregistered case	Type	Remarks
9.3.3	The decision-making body should be listed as the owner of the unregistered case.	V	

9.4 Expanded meeting handling

In Noark 5, all information elements in a case that are generated in the meeting handling must be stored in the Meeting file. The Meeting file can be stored in a separate series or in the same series as the general case records.

Information elements can also be registered and stored in the case that forms the basis for the meeting case handling.

9.4.1 Administration of decision-making body

Administration of decision-making bodies involves the following tasks:

1. Creating and maintaining a decision-making body
2. Making corrections in a decision-making body
3. Placing a decision-making body in the organisational structure

The following functions must be available in order to handle the decision-making bodies:

Requirement no.	Requirements for administration of decision-making body	Type	Remarks
9.4.1	There should be a service/functions for creating, changing and closing decision-making bodies. Changes must be logged.	V	
9.4.2	There should be a service/functions for placing a decision-making body in the organisation structure.	V	
9.4.3	There should be a service/functions for linking the decision-making body to the administrative structure in Noark 5.	V	
9.4.4	There should be a service/functions for placing representatives and deputy representatives in the decision-making body.	V	
9.4.5	There should be a service/functions for registering information concerning representatives and deputy representatives in a decision-making body.	V	
9.4.6	There should be a service/functions for retrieving information concerning representatives and deputy representatives in a decision-making body.	V	
9.4.7	There should be a service/functions for altering information concerning representatives and deputy representatives in a decision-making body. Changes must be logged.	V	
9.4.8	There should be a service/functions for registering the date on which representatives and deputy representatives become part of a decision-making body.	V	
9.4.9	There should be a service/functions for registering the date on which representatives and deputy representatives leave a decision-making body.	V	
9.4.10	It should not be possible to delete information concerning representatives and deputy representatives who either are or have been members of a functioning decision-making body.	V	
9.4.11	There should be a service/functions for assigning roles to representatives in the decision-making body (manager, assistant manager, secretary, etc.).	V	

Requirement no.	Requirements for administration of decision-making body	Type	Remarks
9.4.12	There should be a service/functions for saving a history of who has been a member/participated in different boards and positions.	V	
9.4.13	There should be a service/functions for retrieving one or more decision-making bodies.	V	
9.4.14	There should be a service/functions for registering the date of creation of a decision-making body.	V	
9.4.15	There should be a service/functions for registering the date of closure of a decision-making body.	V	
9.4.16	It should not be possible to delete a decision-making body that either is or has been functional.	V	

9.4.2 Preparation of meeting

The following functions must be available in order to prepare a meeting:

Requirement no.	Requirements for preparation of meeting	Type	Remarks
9.4.17	There should be a service/functions for scheduling meetings in the future.	V	
9.4.18	There should be a service/functions for preparing a case list on the basis of a case draft and appendices that have been saved under the case.	V	
9.4.19	There should be a service/functions to indicate that a case for the meeting must be closed, i.e. take place behind closed doors.	V	
9.4.20	There should be a service/functions for setting up a handling process for each case that is to be processed, i.e. which decision-making bodies the case is to be processed by.	V	
9.4.21	There should be a service/functions for handling deputy representatives for ordinary representatives who cannot attend.	V	
9.4.22	There should be a service/functions for distributing meeting invitations to all the meeting participants.	V	

9.4.3 The actual meeting

It must be possible for authorised roles (e.g. a meeting secretary) to register decisions during a meeting. These decisions must be saved in connection with the case as information elements of the type MV ("meeting decision") with the status *not approved decision.* The decision document must be given the status *approved decision* when the minutes have been approved in accordance with the approval routines.

Requirement no.	Requirements for the actual meeting	Type	Remarks
9.4.23	There should be a service/functions which enable authorised roles or persons to register decisions during a meeting.	V	
9.4.24	There should be a service/functions which ensure that decisions that are registered during a meeting are saved in connection with the case as information elements of the type MV ("meeting decision").	V	
9.4.25	There should be a service/functions to ensure that decisions that are registered during a meeting are saved in connection with the case with the status *not approved decision*.	V	
9.4.26	There should be a service/functions to ensure that a decision document is given the status *approved decision* when the minutes are approved in accordance with the approval routines.	V	

9.4.4 After the meeting

The decision-making body's members are given a short deadline to submit their comments on the minutes, either during or after the meeting. The minutes can also be presented for approval at the next meeting.

Approval of the minutes must appear as information in the minutes, e.g. an endorsement in the minutes to the effect that they have been read out/presented to the appropriate representatives. Approval will/can then be a separate case in the next meeting.

Requirement no.	Requirements for after the meeting	Type	Remarks
9.4.27	There should be a service/functions to allow the decision-making body's members to submit collective remarks on the minutes by a defined deadline.	V	
9.4.28	There should be a service/functions to allow the decision-making body's members to submit individual remarks on the minutes by a defined deadline.	V	
9.4.29	There should be a service/functions to allow the approval of the minutes to be registered.	V	
9.4.30	There should be a service/functions to allow record of the individual meeting participant's approval/non-approval of the minutes.	V	

9.4.5 Administration of the meeting handling

Meeting handling covers the following administrative functions:

1. Create case plan. Retrieve case draft and appendices. Manage meeting participants (including deputy representatives). Send meeting summons to the meeting participants.
2. Write case minutes. Can be saved in both the records case and in the meeting file with reference to the case draft.
3. Where applicable: Archive meeting documents and associated metadata and prepare meeting documents for publication.
4. Conclude the meeting.

The following functions must be available in order to facilitate meeting handling:

Requirement no.	Requirements for administration of meeting handling	Type	Remarks
9.4.31	It should be possible to log the processing levels that have processed a Meeting file or Meeting record.	V	
9.4.32	All information elements in the meeting handling should have available information on the status of the element in the case handling process.	V	
9.4.33	It should not be possible to register meeting handling for a decision-making body that has been closed.	V	
9.4.34	There should be a service/functions for creating case lists.	V	
9.4.35	There should be a service/functions for retrieving case lists.	V	
9.4.36	There should be a service/functions for altering case lists up until the time of the meeting. Changes must be logged.	V	
9.4.37	It should not be possible to alter a case list after the meeting has ended.	V	
9.4.38	It should not be possible to delete a case list after the meeting has ended.	V	
9.4.39	There should be a service/functions for retrieving case drafts and appendices.	V	
9.4.40	It should not be possible to alter a case draft and appendices after the meeting has ended.	V	
9.4.41	It should not be possible to alter a case draft and appendices after the meeting has ended.	V	
9.4.42	There should be a service/functions for sending meeting summons to meeting participants.	V	
9.4.43	There should be a service/functions for writing case minutes.	V	
9.4.44	There should be a service/functions for altering case minutes before they have been approved.	V	

Requirement no.	Requirements for administration of meeting handling	Type	Remarks
9.4.45	It should not be possible to alter case minutes after they have been approved.	V	
9.4.46	There should be a service/functions which ensure that case minutes can automatically be linked to the case from which they originate.	V	
9.4.47	It should not be possible to delete case minutes that have been approved.	V	
9.4.48	It should not be possible to delete a meeting folder.	V	
9.4.49	There should be functions for creating an official variant of a meeting folder through the screening of confidential information and information exempt from public access.	V	
9.4.50	There should be functions for publishing the official variant of the meeting folder on the internet.	V	
9.4.51	There should be a service/functions for registering and archiving the official variant of the meeting folder.	V	
9.4.52	There should be a service/functions for closing a meeting case.	V	

9.5 Relationship to Noark 4

The section on meeting handling represents a reworking of Chapter 9 Module for board handling in Noark 4. As the need for an electronic function for handling meeting and board handling is particularly great within municipal administration, the chapter in Noark 5 is also particularly aimed at municipal authorities. Specific examples have primarily been taken from municipal and county council meeting case handling.

Public bodies other than municipal and county councils will also require a more structured management of meeting documents, as well as a far simpler function than that in a complete meeting module. A more general description of meeting handling has therefore been provided, and it must be possible for an individual body to select only the functions that meet its everyday needs.

Although Chapter 9 in Noark 4 has been reworked, this does not mean that the substance itself has been significantly altered. Some simplifications have been made, but this does not mean that the functions that have already been developed on the basis of Noark 4 cannot be continued. The formulations in this chapter do not preclude the maintenance of existing functions, or the development of more comprehensive solutions than those specified above.

The expanded meeting handling that is described is based on the municipal model that is specified in Noark 4. Most information elements have been retained, but many have been renamed. The most important change concerns where the various information elements are stored.

10 Statistics

10.1 Recommended statistics and reports

The purpose of a statistic is to describe the size and composition of a group of units (e.g. an overview of the number of back logs per administrative unit during a given period), how size and composition change over time and how this compares with other, similar groups of units. All the statistics are recommended reports. The requirements that have been set up for each statistic are linked to an assessment of the structure that the statistic should have and what information should be included in order for it to be of use to the user.

The following description of the statistics uses the statistical terms *scope, text column attribute* and *table header attribute. Scope* means the selection criteria that define which units (documents, cases, etc.) are included in each particular statistic. *Text column attribute* means the categories that are presented to the left of each line in the statistical table (leader texts). *Table header attribute* means the categories that are presented at the top of each column in the statistical table (column headings). Table headers are often split into two. This means that each of the categories is subdivided further on the line below. Noark 5 sets no limits on the statistics that can be generated. All statistics in Noark 5 are recommended.

Requirement no.	Requirements for recommended statistics	Type	Remarks
10.1.1	The report *Case file and document summary* is recommended.	V	Noark-4 K11.47
10.1.2	The statistic *Processing and back log statistics for registry entries* is recommended.	V	Noark-4 K11.80
10.1.3	The statistic *Back log statistics for case files* is recommended.	V	Noark-4 K11.80
10.1.4	The statistic *Case handling time for registry entries* is recommended.	V	Noark-4 K11.80
10.1.5	The statistic *Case handling time for case files* is recommended.	V	Noark-4 K11.80
10.1.6	The statistic *Number of registered registry entries over time* is recommended.	V	Noark-4 K11.80
10.1.7	The statistic *Number of case files created over time* is recommended.	V	Noark-4 K11.80
10.1.8	The statistic *Processing of access requests* is recommended.	V	New

10.1.1 Case file and document summary

The purpose of the report is to provide a tool for the registry in its efforts to maintain an overview of the fonds material.

Requirement no.	Requirements for the report Case file and document summary	Type	Remarks
10.1.9	The report *Case file and document summary* is obligatory.	V	
10.1.10	*Selection:* It must be possible to select the report freely on the following metadata elements: • *fileID* from *Case file* (it must be possible to specify an interval) and thereafter *recordID* from *registry entry* • *disposaldecision* from *Case file* (optional value) • *precedentStatus* from *Case file* • *referenceFondssection* from Case file • *administrativeUnit* from *Case file* • *administrativeUnit* from *Registry entry* • *depreciationmethod* from *Registry entry* (optional value, including the value "not depreciated") • *registrymanagementunit* from *Registry entry* (one or several) • *classID* from *Class* (one or several).	V	
10.1.11	*Sorting:* The report must have optional sorting. The report should by default be sorted according to the metadata element *fileID* from *Case file* and thereafter *recordID* from *Registry entry*.	V	
10.1.12	*Report content:* Which case file information is to be included in the report must be optional, but Noark 5 recommends the following metadata elements (from *Case file* unless specified otherwise): *referenceFondssection* *fileID* *title* *administrativeUnit* *case-responsible* *classID* (from *Class*)	V	

Requirement no.	Requirements for the report Case file and document summary	Type	Remarks
10.1.13	If listing of all the case's documents is selected, which registry entry information is to be included in the report should be optional, but Noark 5 recommends the following (from *Registry entry* unless specified otherwise): *recordID* *title* *registrydate* *documentDate* *numberofAppendices* *registryentrytype* *clienttype* *clientName* *administrativeUnit* *executiveofficer* *registrymanagementunit*	V	
10.1.14	It should be possible to extract the report for the results of a search.	V	

10.1.2 Processing and back log statistics for registry entries

The statistic is intended to act as a supplement to the regular back log checks. The purpose is to provide managers with a tool for assessing the work situation and thereby (re)distributing tasks; cf. also *6.5.4 Back log* list

.

The statistic is based on data from the record type "registry entry". It contains an overview of the number of registry entries that have been processed during a given period for each individual administrative unit and for the entire organisation, together with the number of back log for both the current back log period and previous periods.

Requirement no.	Requirements for the statistic Processing and back log statistics for registry entries	Type	Remarks
10.1.15	*Scope (selection criteria) must be:* All incoming and outgoing documents and optionally all internal documents for follow-up, with an arbitrary registry date interval (=back log period) and optional depreciation date. In addition, all older incoming documents with a depreciation date during the period or with back log (e.g. a blank depreciation date) (cf. the metadata element *depreciationdate* in *Registry entry*).	V	

Requirement no.	Requirements for the statistic Processing and back log statistics for registry entries	Type	Remarks
10.1.16	*The text column attribute must be:* The case processing unit(s) at self-selected level(s), after self-selected sorting and with the option of totals per overall level.	V	
10.1.17	*The table header attribute must be split into two:* • CASE HANDLING, split between "Received", "Outgoing" and "Depreciated". • BACK LOG, split between "New during the period", "Older" and "Total" – "Received" is defined as "all incoming documents (and optionally internal documents for follow-up which have been received) registered during the back log period". – "Outgoing" is defined as "all outgoing documents (and optionally internal documents for follow-up which have been sent) registered during the back log period". – "Depreciated" is defined as "all incoming documents (and optionally internal documents) with a depreciation date during the back log period". – "New during the period" is defined as "all incoming documents (and optionally internal documents) with a registry date during the back log period and without a depreciation date". – "Older" is defined as "all incoming documents (and optionally internal documents) with a registry date before the back log period and without a depreciation date". – "Total" is defined as the sum of "New during the period" and "Older".	V	

10.1.3 Back log statistics for case files

The statistic is intended to act as a supplement to the regular back log checks. The purpose is to provide managers with a tool for assessing the work situation and thereby (re)distributing tasks; cf. also *6.5.4 Back log* list

.

The statistic is based on data at *case file level.* The statistic gives an overview of the number of case files that have arisen during a given period for each individual administrative unit and for the entire organisation, together with the non-finalised case files for both the current period and previous periods.

The statistic is intended for use in connection with planning work,

whether business plans, staffing plans or budgeting, in order to provide an overview for the management of the scope of case files and case file back log.

Requirement no.	Requirements for the statistic Back log statistics for case files	Type	Remarks
10.1.18	*Scope (selection criteria) must be:* All case files with an arbitrary case date interval and arbitrary date for case finalisation or depreciation of registry entries in the case. In addition, all older case files (=case date before the first date in the defined interval) which are subject to processing (i.e. which have not expired or been finalised and contain non-depreciated registry entries).	V	
10.1.19	*The text column attribute must be:* Case processing unit at self-selected level(s), after self-selected sorting and with the option of totals per overall level.	V	
10.1.20	*The table header attribute must be:* • "New case files during the period", "Of which, non-finalised", "Non-finalised older case files" and "Total non-finalised cases". – "New case files during the period" is defined as "all with a case date within the selected period that are to be followed up (i.e. which have not expired or been finalised and contain non-depreciated registry entries)". – "Of which, non-finalised" is defined as "all with a case date during the selected period which have not expired or been finalised and contain non-depreciated registry entries". – "Non-finalised older cases" is defined as "all older cases which have not expired or been finalised and contain non-depreciated registry entries". – "Total non-finalised cases" is defined as the sum of "Of which, non-finalised" and "Non-finalised older cases".	V	

10.1.4 Case handling time for registry entries

The purpose of the statistic *Case handling time for registry entries* is to see how long on average it takes from receipt of a document by the organisation until it has actually been answered. This could be a tool for managers to create a picture of any bottlenecks within the organisation.

The statistic is linked to Section 11a of the Public Administration Act, which states that the administrative body must prepare and reach a decision on the case without undue delay. In this context, it is useful for the administrative body to have an overview of the average processing time for registry entries in order to monitor the level of service provided to the public, customers, clients, etc. As the statistic is aimed at the public's requirement for a response without undue delay, the obligatory requirements for the statistic are limited to external correspondence, i.e. incoming documents which are answered in writing. Provisional responses are considered as indicating that the incoming document has not been answered.

The statistic is based on data from the record type "registry entry". The statistic gives an overview of the average time from receipt of a letter by the organisation until it has been answered in writing. The statistic is defined for a given period of time for the individual case handling unit and for the entire organisation.

The statistic is intended for use in connection with planning work, i.e. business plans, staffing plans or budgeting, in order to provide an overview of case handling time for the management.

In order for the report to give a realistic picture of the case handling time, it is assumed that the depreciation date for the incoming document that is answered is set as equal to the letter date for the outgoing document that depreciates.

The obligatory requirements for the report do not give an overview of enquiries that are not answered through outgoing documents.

Requirement no.	Requirements for the statistic Case handling time for documents	Type	Remarks
10.1.21	*Scope (selection criteria) must be:* Registry entry type Outgoing document, where the metadata element "*referenceDepreciatesRegistryentry"* contains a recordID and the associated incoming document has the depreciation method = "Answered by letter" or "Answered by e-mail" (i.e. the reply letter is not a provisional reply). Optional as to whether it is also to be possible to select other depreciation methods ("Answered by telephone", "Noted for information purposes", etc.). Registry date for received documents and any case type for the case file must be included.	V	
10.1.22	*Text column attributes must be:* Either case type or case processing unit at self-selected level(s), according to self-selected sorting and with the option of totals per overall level (cf. the metadata element *administrativeUnit*).	V	

Requirement no.	Requirements for the statistic Case handling time for documents	Type	Remarks
10.1.23	*Table header attributes must be:* Case handling time grouped into up to five self-selected time intervals defined as the time distance between the outgoing document's depreciation date (cf. the metadata element *depreciationdate* in *Registryentry*) and the associated incoming document's registry date (e.g. up to two weeks, two to four weeks, four to eight weeks, more than eight weeks. For different organisations, the time interval of interest will vary.)	V	
10.1.24	The report must also optionally be able to include internal documents for follow-up.	V	
10.1.25	There must be two-level text columns with both case handling unit and case type (i.e. the list of case types is repeated for each case handling unit at the selected level).	V	

10.1.5 Case handling time for case files

The purpose of the statistic *Case handling time for case files* is to see how long it takes on average from a case file arising within the organisation until it is finalised. In this way, it can be a tool for a manager to identify bottlenecks within the organisation.

The statistic is based on data at *case file level.* The statistic is defined for a given period of time for case types and/or the individual case handling unit and for the entire organisation.

The statistic is intended for use in connection with planning work, i.e. business plans, staffing plans or budgeting, in order to provide an overview of case handling time for the management.

In order for the report to give a real picture of the case handling time, it is assumed that the case file's status will be set to "Finalised" when it has been fully processed.

Requirement no.	Requirements for the statistic Case handling time for case files	Type	Remarks
10.1.26	*Scope (selection criteria) must be:* All cases with the case status "Finalised" which have a case date after a selected date, or *fileID* above a selected value.	V	

Requirement no.	Requirements for the statistic Case handling time for case files	Type	Remarks
10.1.27	*Text column attributes must be:* • either case type • or the case-responsible unit at self-selected level(s), according to self-selected sorting and with the option of totals per overall level.	V	
10.1.28	*Table header attributes must be:* Case handling time grouped into up to five self-selected time intervals defined as the time distance between the case file's *createdDate* and the last registry entry's *documentDate* (e.g. up to two weeks, two to four weeks, four to eight weeks, more than eight weeks. The time span of interest will vary for different organisations).	V	
10.1.29	The report must also optionally be able to include internal documents for follow-up.	V	
10.1.30	There must be two-level text columns with both case-responsible unit and case type (i.e. the list of case types is repeated for each case-responsible unit at the selected level).	V	

10.1.6 Number of registry entries registered over time

The purpose of the report is to obtain an overview of the number of registry entries registered per time unit and administrative unit in order to get a picture of changes in workload over time.

Requirement no.	Requirements for the statistic Number of documents registered over time	Type	Remarks
10.1.31	*Scope (selection criteria) must be:* All registry entries, with an optional registry date interval and optional delimitation of registry entry type.	V	
10.1.32	*Text column attributes must be:* Optional time unit (calculated from registry date) equal to the month or sum of the months (quarter, four-month period, half-year up to year).	V	
10.1.33	*Table header attributes must be:* Case handling unit at self-selected level(s)	V	

10.1.7 Number of case files created over time

The purpose of the report is to obtain an overview of the number of case files per time unit and administrative unit in order to get a picture of changes in workload over time.

Requirement no.	Requirements for the statistic Number of case files created over time	Type	Remarks
10.1.34	Scope (selection criteria) must be: All cases, with an optional case date interval (and the case containing at least one registry entry) and optional delimitation of case type.	V	
10.1.35	*Text column attributes must be:* Optional time unit (calculated from case date) equal to the month or sum of the months (quarter, four-month period, half-year up to year).	V	
10.1.36	*Table header attributes must be:* Case handling unit at self-selected level(s)	V	

10.1.8 Processing of access requests

The purpose of the report is to obtain an overview of the number of people that have requested access during a particular period of time and the type of results that processing of the requests produced.

Requirement no.	Requirements for the statistic Processing of access requests	Type	Remarks
10.1.37	It must be possible to obtain statistics concerning the number of access requests during a given period of time.	V	
10.1.38	In addition to the total number of access requests and period, the following information must be included in the results: • processing results (approval/rejection) • authority basis (for any rejection)	V	

10.2 Notification

It is important that the function has good functionality for setting up various notifications, i.e. for notifying users of the function when various deadlines are passed, milestones are reached, etc. In some cases, such notifications can replace traditional reports and statistics in the same way as predefined searches.

Requirement no.	Requirements for notification	Type	Remarks
10.2.1	It must be possible to set up notifications (e.g. in the form of message boxes) when deadlines are passed, etc.	V	

10.3 Changes in relation to Noark 4

A number of reports and statistics have been omitted.

- The report *Case and document summary* is now obligatory and has been renamed *Case file and document summary*.
- The report *(Re)activation list* has been omitted.
- The report *Lending list* has been omitted.
- The report *Case folder* has been omitted.
- The report *Document summary across cases* has been omitted.
- The report *Sender/addressee list* has been omitted.
- The report *Administrative subdivision* has been omitted.
- The report *List of Noark people* has been omitted.
- The report *Date control* has been omitted.
- The statistic *Statistics concerning clients* has been omitted.
- The statistic *Statistics concerning archive codes used* has been omitted.
- The statistic *Processing of access requests* is new.

11 User administration functions

Noark 5 facilitates the administration of organisational structure and users, and their links to roles, registry management units and series, by external solutions. The requirements in this chapter apply when user administration forms part of a Complete Noark solution. The module is optional.

The chapter does not contain requirements for any external user administration function, where such a solution is used. The requirements concerning the way in which external user administration solutions must function with respect to Noark 5 core are set out in section 4.3.

11.1 Administrative structure

The requirements for the way in which the administrative structure should be constructed and maintained in a Complete Noark 5 solution are set out below. These requirements are based on the assumption that a hierarchical line organisation is still the most common type of organisation. At the same time, consideration must also be given to the fact that more and more organisations are switching to network-based or project-oriented organisational structures. A Complete Noark 5 solution should be capable of handling all forms of organisational structure.

Requirement no.	Requirements for administrative structure	Type	Remarks
11.1.1	It should be possible to create a hierarchical, administrative structure with an unlimited number of levels.	V	
11.1.2	It should be possible to create an unlimited number of administrative units at the same level.	V	
11.1.3	It should be possible to create a matrix-based administrative structure which allows network-based or project-oriented organisational forms for example.	V	
11.1.4	It should be possible to create an administrative structure which allows a combination of hierarchical and non-hierarchical administrative structures.	V	
11.1.5	It should be possible to register the start and end date of an entire administrative structure.	V	
11.1.6	It should be possible to register the start and end date of parts of an administrative structure.	V	
11.1.7	It should be possible to retrieve one or more closed administrative structures.	V	
11.1.8	It should not be possible to delete an administrative structure.	V	
11.1.9	It should be possible to alter the administrative structure.	V	
11.1.10	It should be possible to add new administrative units at any level in the structure.	V	

Requirement no.	Requirements for administrative structure	Type	Remarks
11.1.11	It should be possible to alter information concerning a particular administrative unit. Changes must be logged.	V	
11.1.12	It should be possible to alter information concerning selected administrative units. Changes must be logged.	V	
11.1.13	It should be possible to register the following metadata for administrative unit: • The unit's current full name • The unit's short name • The date on which the unit was created • The date on which the unit expires • All previous names of the unit • All previous short names of the unit • Address of the administrative unit, including any e-mail	V	
11.1.14	It should be possible to alter information concerning the name of an administrative unit.	V	
11.1.15	It should not be possible to delete an administrative unit's name.	V	
11.1.16	There should be functions for preserving the original name(s) of administrative units in the event of name changes.	V	
11.1.17	It should be possible to set the start and end date of an administrative unit.	V	
11.1.18	It should not be possible to link new files or records to a closed administrative unit.	V	
11.1.19	It should not be possible to delete an administrative unit that has a file or record linked to it.	V	
11.1.20	It should be possible to use parameters to specify whether a search for administrative unit should also cover the same unit under previous names.	V	
11.1.21	In the case of a search for an administrative unit, the search should automatically also cover any subordinate units. It should be possible to override this.	V	
11.1.22	The administrative structure should be completely independent of the fonds structure. It should therefore be possible for fonds or a series to cover: • an entire administrative unit • parts of an administrative unit • a number of administrative units • non-hierarchical types of administrative structure	V	

Requirement no.	Requirements for administrative structure	Type	Remarks
11.1.23	It should be possible to have different kinds of *decentralised registry*, e.g.: • centralised record and decentralised filing • decentralised record and centralised filing • decentralised record and decentralised filing	V	

11.2 User administration

Complete Noark 5 should facilitate the administration of users and their links to administrative units. Users' rights should be linked to roles and administrative affinity.

11.2.1 User

Requirement no.	Requirements for user	Type	Remarks
11.2.1	It should be possible to create an arbitrary number of users.	V	
11.2.2	Users should only be able to use the functions and the information for which they are authorised.	V	
11.2.3	It should be possible to specify that a person can perform a record on behalf of someone else and with this person's rights.	V	
11.2.4	It should be possible to register the following metadata for user: • The user's current full name • The user's initials • The date on which the user was created • The date on which the user expires • All previous names • All previous initials	V	
11.2.5	It should be possible to alter information concerning selected users. Changes must be logged.	V	
11.2.6	It should be possible to alter information concerning a user's name and initials.	V	
11.2.7	It should not be possible to delete a user's name.	V	
11.2.8	There should be functions for preserving the original name(s) of the user in the event of name changes.	V	
11.2.9	It should be possible to preserve all names and initials in the function together with information on the period of use.	V	
11.2.10	The function should keep a record of names and initials that belong to the same person.	V	

Requirement no.	Requirements for user	Type	Remarks
11.2.11	It should be possible to use parameters to specify whether a search for user should also cover the same user under previous names.	V	
11.2.12	It should not be possible to link new files or records to a closed (expired) user.	V	
11.2.13	It should not be possible to delete a user who has a file or record linked to him or her.	V	
11.2.14	It should be possible to register an address and other office/administrative or private information linked to a user, e.g. telephone, fax, e-mail, office, home address, etc.	V	
11.2.15	It should be possible to change an address.	V	
11.2.16	It should be possible to delete an address.	V	
11.2.17	It should be possible to retrieve an address.	V	

11.2.2 Roles and associated rights

Requirement no.	Requirements for roles and linked rights	Type	Remarks
11.2.18	It should be possible to create different roles with specified rights and restrictions.	V	
11.2.19	It should be possible to obtain an overview of the various roles and specified rights and restrictions, either collectively or individually.	V	
11.2.20	It should be possible to alter roles and their specified rights and restrictions, either collectively or individually.	V	
11.2.21	It should be possible to set a start date and an end date for a role.	V	
11.2.22	It should not be possible to use a role after the end date has passed.	V	
11.2.23	It should be possible to reactive a closed role.	V	

Requirement no.	Requirements for roles and linked rights	Type	Remarks
11.2.24	For solutions that are to implement Complete Noark 5, it should be possible to define the following role hierarchy for standard roles and associated rights: • Fonds administrator • Fonds manager • Fonds personnel • Manager • Executive officer • Board secretary	V	
11.2.25	It should be possible to start from a standard role and make changes to it.	V	
11.2.26	It should be possible to define other roles in addition to these roles.	V	
11.2.27	It must not be possible to create roles that revoke the general restrictions that are defined in the function.	O	
11.2.28	Standard role - Fonds administrator • Rights: - access to all system and operating functions - right to authorise yourself and other users for all types of rights • Restrictions: - no access to functions for record or correction	V	
11.2.29	Standard role - Fonds manager • Rights: - access to create cases, registry entries and electronic documents - access to archive and dispatch electronic documents - access to all functions for record and correction (including the moving of registry entries) - right to assign yourself and other users rights for record and correction, and for access codes and affiliation to access groups - the rights apply globally • Restrictions: - the authorisation right for access codes only applies to the codes for which the user concerned is authorised - the right to perform records and corrections is limited by the rules for process control (cf. below) - the right to perform records and corrections does not include the right to alter archived documents and associated metadata for document description	V	

Requirement no.	Requirements for roles and linked rights	Type	Remarks
11.2.30	Standard role - Fonds personnel • Rights: - access to create cases, registry entries and electronic documents - access to archive and dispatch electronic documents - access to all functions for record and correction, including the moving of registry entries - access to link users to access groups • Restrictions: - the right to perform records and corrections is limited by the rules for process control (cf. below) - the right to perform records and corrections does not include access to alter archived documents and associated metadata for document description - all record functions and write access rights are limited to the units for which the user is authorised.	V	
11.2.31	Standard role - Manager • Rights: - access to create cases, registry entries and documents - access to functions for record and correction - access to register remarks - access to register an action plan for board handling of a case - right to authorise executive officers for record in accordance with rights and restrictions in the role of Executive officer, and for access codes and membership of access groups • Restrictions: - the authorisation right for access codes only applies to the codes for which the user concerned is authorised - access to create cases and registry entries is limited to the units of which the person concerned is manager, or units subordinate to these units, or cases where registry entries linked to this unit or these units already exist - all other record functions and write access rights are limited to the administrative units of which the person concerned is manager, or units subordinate to these units	V	

Requirement no.	Requirements for roles and linked rights	Type	Remarks
11.2.32	Standard role - Executive officer • Rights: - access to create cases, registry entries and electronic documents - access to functions for record and correction - access to register remarks - access to register an action plan for the board handling of a case (where the person concerned is case-responsible) - access to create ad hoc access groups that are linked to cases for which the person concerned is case-responsible, or registry entries for which the person concerned is executive officer • Restrictions: - access to create cases is limited to cases where the person concerned is case-responsible, or cases where registry entries for which the person concerned is executive officer already exist - access to create registry entries is limited to cases where the person concerned is case-responsible, or cases where registry entries for which the person concerned is executive officer already exist - all other record functions and write access rights are limited to cases for which the person concerned is executive officer, or registry entries and associated documents where the person concerned is executive officer	V	

11.2.3 Requirements for the user's relationship to role, administrative unit, registry management unit and series

Requirement no.	Requirements for the user's relationship to role, administrative unit, registry management unit and series	Type	Remarks
11.2.33	It should be possible to link a user to one or more roles, administrative units, registry management units and series.	V	
11.2.34	It should be possible to define a role, administrative unit, registry management unit or series as standard for the user.	V	
11.2.35	It should be possible to change a user's affiliation to a role, administrative unit, registry management unit or series. The change must be logged.	V	
11.2.36	It should be possible to set a start and end date for a user's affiliation to a role, administrative unit, registry management unit or series.	V	

Requirement no.	Requirements for the user's relationship to role, administrative unit, registry management unit and series	Type	Remarks
11.2.37	A user should not be able to have write access in a role, administrative unit, registry management unit or series which has been closed.	V	
11.2.38	It should be possible to retrieve a user's affiliations to a role, administrative unit, registry management unit or series.	V	
11.2.39	A single user should be able to act in different roles.	V	
11.2.40	It should be possible to preserve all roles that a user either currently holds or has previously held in the function together with information on the period of use.	V	
11.2.41	There should be functions for keeping a record of the roles that belong to the same person.	V	
11.2.42	It should be possible to define a user's rights in a role delimited within case type and classification value.	V	
11.2.43	It should be possible to assign all users to a role profile which specifies role, affinity, rights and restrictions.	V	
11.2.44	It should be possible to define standard values for role, administrative affinity and archival affinity (fonds-series-registry management unit) in the role profile.	V	
11.2.45	It should be possible for the "read fonds" function to be performed by all roles and users within the screening codes for which they are authorised.	V	
11.2.46	It should be possible for the "read series" function to be performed by all roles and users within the screening codes for which they are authorised.	V	

12 Security and access functions

12.1 Purpose and key principles

Public sector bodies are subject to various regulations concerning information security, depending on the type of information they process and the function of the body within society. A typical characteristic of many regulations concerning information security is that they are based on an internal control principle. This means that the regulations provide a framework for the body's own assessments of risk and decisions concerning the formulation and implementation of security measures. The aim of the measures is to ensure the confidentiality, integrity and availability of the information.

For a Noark solution, most security requirements concern control over access to, the use of and changes to metadata and documents. Other types of security measures, such as backup creation and measures aimed at countering malware are normally handled outside the Noark solution. It is not the aim of Noark 5 to cover all aspects of a public body's information security. The Noark solution must be integrated under and interact with other security measures and technical infrastructure. It must be possible to configure and use the Noark solution in a way which is compatible with the body's own goals and strategies concerning information security, adopted in line with relevant legal frameworks.

The security requirements for the Noark 5 core therefore consist of a relatively modest number of obligatory requirements, which are intended to ensure the confidentiality, integrity and availability of fonds, metadata and documents. The number of recommended security functions that a complete Noark 5 solution should have is however relatively high. Each public sector body must itself consider whether it needs to implement a particular recommended function in the requirement tables. Each individual body's need to implement different recommended functions will vary according to the sensitivity of the information, the work processes of the body concerned, interaction patterns, technical integration, the legal framework applicable to the area concerned, etc.

In most cases, the security requirements are purely functional requirements. Very few "strength requirements" are therefore imposed. This means that no measurable requirements are imposed concerning how strictly each security function is to be enforced by the solution or how difficult it must be to circumvent the function.

12.1.1 Security functions versus security goals

The requirements for information security in Noark 5 are function-oriented. This means that they are linked to "things that happen" in different parts of the solution, either in the core or in an external solution. Within the field of information security, it is perhaps more common to formulate requirements for security *goals.* These goals are often specified through requirements concerning the three aspects of confidentiality, integrity and availability. Goal-oriented requirements may be better suited to highlighting the individual body's need and responsibility to balance the requirements against each other. Goal-oriented requirements also give greater flexibility for finding different tools and measures to achieve adequate security.

Nevertheless, it is not appropriate to set up the requirement tables in a standard according to different goals which must be balanced against each other. The function-oriented subdivision of security properties in this section assumes that each body that is to use a Noark 5 solution will have decided on its own security policy *in advance.* The security policy will be based on the regulations that apply to the body and on the balance established by the body between the needs for confidentiality, integrity and availability.

12.1.2 Terminology: Security functions and properties

The requirements in this section largely specify *security functions.* One or more security functions can handle different *security properties,* which can be either implicit or explicit. The security functions can also overlap to some extent, in that a number of different functions can handle the same security property.

Here is an example which illustrates the use of the term: "Logging on with a password" is a *function,* which is primarily intended to handle the *property* "authentication of the user". "Logging on with a smart card and PIN code" would be another variant of the security function "logging on". It handles the same property (authentication), but to a stronger degree.

12.2 Controlling access to information

12.2.1 Identification of users

For all external solutions that are to be integrated with the Noark 5 core, users of the external solution must be individually and uniquely identified and logged on. The logging on can be validated either in the external solution concerned or in an integrated, external security solution. For a simple integration and a holistic security policy across the organisations' IT systems, security functions that provide for user directories outside the Noark 5 solution are generally recommended.

Requirement no.	Requirements for the identification of users	Type	Remarks
12.2.1	All users who are to have access to the Noark 5 solution must be individually identified and sufficiently authenticated.	O	
12.2.2	An external directory of identified users can be used, instead of explicit logging on to the Noark 5 solution.	V	
12.2.3	The user can be logged on to a linked external solution and allow the external solution to manage the rights that the user is to have.	V	
12.2.4	The user can be logged on in the solution's operating environment and have defined access rights in a resource directory. The Noark 5 solution can then be used provided the externally defined access rights are sufficient ("single sign-on").	V	

"External users" such as journalists, members of the public, parties to a case, collaborating enterprises, etc. outside the archive owner's instruction authority can be given access to content in the Noark 5 solution through customised external systems. An external solution intended for users external to the organisation should as a general rule have extremely limited functionality, in order to minimise the extent of damage in the event of a breach of security. For solutions which are intended to make content in the fonds available to the public, access should preferably be facilitated through special publication solutions. A publication solution contains custom exports of registry information and documents that are not to be exempted from public access. For the security requirements in this section, the publication export is not considered to constitute part of the Noark 5 solution.

Requirement no.	Requirements for the identification of external users	Type	Remarks
12.2.5	It should be possible to give external users, such as journalists, members of the public or citizens and organisations in their capacity as parties to a case, access to a custom external solution with functionality limited to that appropriate for the purpose concerned.	V	
12.2.6	Users of a custom external solution must be identified to this solution, either as individuals or as the representative of a registered organisation.	B	Obligatory if the above requirement is fulfilled.
12.2.7	External users can be authenticated via an external, third party log-on service. (This requirement is primarily intended to cover the public security portal for the service *Minside.no*, but can also be used for other log-on services.)	V	
12.2.8	The custom external solution must be able to mediate to a third party log-on service the requirements for identification and authentication level that are imposed in order for the external user to be given the requested access.	B	Obligatory if the above requirement is fulfilled.
12.2.9	It should be possible for unidentified or weakly authenticated external users to be given access to publication exports that are separated from the Noark 5 core, in order to provide access to cases and documents.	V	
12.2.10	Publication exports for access by unidentified users must be produced in such a way that the exports do not contain screened information.	B	Obligatory if the above requirement is fulfilled.

Passwords have a long tradition of being the minimum requirement for authentication in IT systems. Stricter requirements for authentication are however becoming increasingly

widespread, particularly for systems in heterogeneous environments and systems which are accessed by external users outside the system owner's instruction authority.

Requirement no.	Requirements for authentication strength	Type	Remarks
12.2.11	The minimum requirement for authentication strength for logging on which gives access to the Noark 5 solution is a personal password for the individual user.	O	
12.2.12	It should be possible to specify requirements for the strength of the password (complexity, length, duration, etc.).	V	
12.2.13	It should be possible to use other and stronger authentication methods as an alternative to passwords.	V	
12.2.14	If the solution gives the *option of* stronger authentication than a password, it must also be possible to *impose requirements for* stronger authentication in order for the log-on to be accepted.	B	Obligatory if the above requirement is met.
12.2.15	If weak authentication is deemed sufficient for using the Noark 5 solution, provision should also be made to ensure that a log-on by a user who has been authenticated more strongly than is actually necessary will also be accepted.	V	

If a user leaves his or her job, their access rights should normally be withdrawn. There may nevertheless be a need to know who had a particular access at a particular time and the identifier for a person who has previously had access should therefore not be deleted.

Requirement no.	Requirements for the handling of historic user identities	Type	Remarks
12.2.16	It must be possible to set a log-on identifier ("userident") which is no longer to have access to the function to the status "passive", which prevents logging on.	V	
12.2.17	There must be an overview of the period or periods during which the userident has been active.	B	Obligatory if the above requirement is fulfilled.

Requirement no.	Requirements for the handling of historic user identities	Type	Remarks
12.2.18	It should be possible to alter the user's "full name" and any initials that are used to identify the user as an executive officer in documents and screens for a given userident. A change of name and initials for a userident will only be relevant if the same person changes name, and not for assigning a previously used identifier to another person.	V	
12.2.19	In the event of access to alter the "full name" and/or initials for a given log-on identifier, it must be possible to preserve all names and initials in the solution together with information on the period or periods during which the various names or initials were in use.	B	Obligatory if the above requirement is fulfilled.

12.2.2 Authorisation

Authorisation is the filtering of what an individual logged-on user is actually permitted to do in the solution. There are two fundamentally different general principles for how authorisation can be expressed, often called "need to know" and "need to protect". As a general principle, "need to know" means that the general rule is that all access is closed and that authorisations must be explicitly expressed. "Need to protect" is authorisation with the opposite assumption: everything is open unless access is blocked or screened explicitly. "Need to protect" is principally relevant for access to read, search in and print out information. Editing access rights within public administration should always be based on the "need to know" principle.

Although "need to know" and "need to protect" are two fundamentally different initial assumptions, it is formally possible to practise the same permissions and restrictions within the framework of both principles. In practical use, it is nevertheless important to be aware of the approach that the organisation has adopted. The Freedom of Information Act and the obligation to give access to public registries are fundamentally "need to protect"-oriented. Most regulations which more specifically regulate information security are "need to know"-oriented.

Requirement no.	Requirements for basic principle for authorisation	Type	Remarks
12.2.20	All editing and write access in the Noark 5 solution must be based on a "need to know" basic principle.	O	Obligatory where such access is given from an external module.
12.2.21	A "need to protect" basic principle can be used for read access in one or more external solutions.	V	

Authorisations are composed of two main components: The first component consists of *functional rights*, access to perform specific actions – create, alter, read, search, etc. Functional

rights can often be linked to specific menu options, screens and commands, etc. in a user interface. Permission to carry out a function call from an external task system is also a functional right. The other component is object access, or the right's *footprint.* Object access rights are delimitations of the objects and people in the world, represented as data objects, for which the functional rights are to apply.

A *role* is a term used within access control which groups together similar tasks, so that an authorisation can be assigned to several people with the same role instead of being assigned to each individual person. It should also be possible to specify different types of context between roles. In many organisations, a person who has the role of "manager" of a unit will for example need access to the same information as all of his or her subordinates. Such an opportunity to inherit access rights from one role to another is however not universal for all relations between a manager and his or her subordinates in every organisation.

Requirement no.	Requirements for functional roles	Type	Remarks
12.2.22	It should be possible to compose different combinations of functional requirements that are imposed on the user's authorisation to form different functional roles, which express typical job categories or task portfolios within the organisation.	V	
12.2.23	For each functional role, it should be possible to define a set of rules for process-related rights (cf. the table below).	V	
12.2.24	It should be possible for a user to hold a number of different roles.	V	

Process-related rights are a tool for specifying different conditions for authorisation to perform a particular action. An example is where a person is to have a particular role (e.g. "manager") in order to alter the status of a record or a file to "finalised". (This requirement table is a generalisation of the concrete specified process-related rights in section 8.2.2.2 of Noark 4).

Requirement no.	Requirements for process-related functional rights and restrictions	Type	Remarks
12.2.25	The role profile's set of rules must not be able to expand the general functional rights. It must only be possible to express delimitations from the access rights that a user otherwise has.	O	
12.2.26	A set of rules should be able to specify permitted actions based on the status of the file, the record, the document description or the document.	V	
12.2.27	A set of rules should be able to specify permitted actions based on other metadata that are expressed through stringent, fixed code values.	V	

Requirement no.	Requirements for process-related functional rights and restrictions	Type	Remarks
12.2.28	The rules in a set of rules should be able to express a requirement for task differentiation ("separation of duties"), so that a requirement can be imposed which requires more than one user to approve a particular action.	V	
12.2.29	A rule concerning separation of duties can impose conditions which require an action to be confirmed before it is carried out with final effect. It should be possible to impose different types of requirement concerning who can confirm the action, e.g. one of the following people: • Any other authorised user • A user with a certain, specified role (e.g. "manager" or "controller"). • Another specified user who is registered as counter-signing at file or record level.	V	
12.2.30	Rules in a set of rules should be able to express a requirement according to which the party's consent must be obtained and registered in order for certain actions to be permitted. The requirement is most relevant to the provision of information to a third party, in cases where access to distribute such information would otherwise be limited by a secrecy obligation.	V	
12.2.31	Once obtained, consent can be registered specifically for the event concerned, or given as a "standing consent" (permanent) for all information in a case.	V	
12.2.32	If "standing consent" is given, there must be functions for withdrawing the consent.	B	Obligatory if 12.02.31 is fulfilled.
12.2.33	If a party is authenticated as an external user with cause to register information in a task system, it should be possible for the user concerned to register and withdraw consent him- or herself.	V	

In relatively large organisations, a person, or a person in a particular role, will generally only be authorised for access to a specific part of the information in the solution. Such delimitations can be termed the authorisation's "footprint". It should be possible to specify this "footprint" in a number of ways depending on the nature of the organisation.

Requirement no.	Requirements for delimitations concerning the authorisations' "footprints", access to data	Type	Remarks
12.2.34	It should be possible to restrict the access rights of a user in a role to within a specified element in the fonds structure. One of the following: • The entire Noark 5 solution • Logical archive • Series • File • Record	V	
12.2.35	It should be possible to restrict the access rights of a user in a role to within specified organisational boundaries in the fonds structure. One of the following: • The entire organisation • Own administrative unit without subordinate units • Own administrative unit and subordinate units • Another named administrative unit	V	
12.2.36	The solution should have a facility s a configurable option to specify that the person who is registered as the executive officer for a record must also have editing rights for it.	V	
12.2.37	It should be possible to restrict the access rights of a user in a role to certain classification values within a classification system.	V	
12.2.38	It should be possible to restrict the access rights of a user in a role to certain case areas and/or case types and/or to cases produced by a certain specified task system only.	V	
12.2.39	It should be possible to restrict access rights to special properties of the parties to the case. Such restrictions could for example concern: • The party's geographic affinity (residence, company address, etc.) according to postcode, municipal authority, county or similar. • Other defined party categories which can be specified in external party or sender/recipient directories, e.g. industry category, marital status, age group, profession, etc. • Specific registered assignment of the individual party/client with respect to a particular executive officer or administrative unit	V	
12.2.40	It should be possible to restrict the access rights of a user in a role to grading codes that have been specified for case, registry entry or document, so that personal clearance is required in order to gain access.	V	

Requirement no.	Requirements for delimitations concerning the authorisations' "footprints", access to data	Type	Remarks
12.2.41	It must be possible to organise grading codes hierarchically, so that it is possible to specify that a particular grading must be more or less strict than another particular grading.	B	Obligatory if 12.02.40 is fulfilled.
12.2.42	It should be possible to specify access to a specific object for a particular user, regardless of other restrictions in the footprint (but still dependent on the user's functional rights).	V	

The actual authorisation for the individual user is expressed through a combination of the person's functional rights and the footprint or footprints for which the functional right is to apply. A combination of functional role and footprint in this set of requirements is called an "access profile".

Requirement no.	Requirements for access profiles	Type	Remarks
12.2.43	Within each of a user's roles, it should be possible to define an access profile that consists of the role's functional rights in combination with the footprint for the role.	V	
12.2.44	If a log-on identifier has a number of different access profiles, the person concerned should be able to select from the access profiles that have been defined for him or her.	V	
12.2.45	It should be possible to switch between access profiles in a way which the user finds easy.	V	
12.2.46	It should be possible to specify one of the user's access profiles as the default profile, which is assigned when logging on unless specified otherwise.	V	
12.2.47	It should be possible to define access profiles which enable an individual user to have defined different footprints for one or more of his or her roles.	V	

Party-related rights restrictions take effect irrespective of the rights in the user's access profile. They act as further restrictions on the access profile's rights.

Requirement no.	Requirements for party-related rights restrictions	Type	Remarks
12.2.48	It should be possible to register potential conflicts of qualification between parties and executive officers.	V	
12.2.49	This requirement is deleted.		

Requirement no.	Requirements for party-related rights restrictions	Type	Remarks
12.2.50	It should be possible to specify different types of access restriction based on the nature of the disqualification situation: • The executive officer can prepare the case but not reach a decision • The executive officer may not take part in any stage of the case handling • The executive officer is denied access to the case and its documents.	V	
12.2.51	A party should be able to impose conditions which ensure that certain specified executive officers are not given access to cases to which they are a party (regardless of whether or not there is formal disqualification). This recommendation involves a general opportunity to specify that a file is to be screened from a particular specified executive officer, regardless of whether or not the person concerned would otherwise have had access based on his or her positively specified authorisation.	V	

A deputy, normally a person who acts on behalf of an absent manager, must be able to perform the appropriate deputy functions using his or her own log-on identifier. According to virtually every known regulation concerning information security, it would be unacceptable to "borrow" the log-on identifier and password from the person on behalf of whom the deputy is acting.

Requirement no.	Requirements for authorisation for deputies	Type	Remarks
12.2.52	It should be possible to register a user as a permanent deputy for another user.	V	
12.2.53	It should be possible to register a user as a temporary deputy for another user, valid from date to date.	V	
12.2.54	A deputy must be logged on with his or her personal log-on identifier, but can specify when logging on that the person concerned is acting as deputy for another specified user.	B	Obligatory for the use of deputy function.
12.2.55	Actions performed in the capacity of deputy must be registered with coding or text which indicates that they were "performed by a <*logged-on user*> as deputy for <*principal*>"	B	Obligatory for the use of deputy function.

Requirement no.	Requirements for authorisation for deputies	Type	Remarks
12.2.56	When logging on or in other user dialogues where a log-on identifier can choose from available roles or access profiles, a list should also be presented of the users that the person concerned has authorisation to act as deputy for, and choose to authorise him- or herself as one of these roles or profiles.	V	
12.2.57	The deputy should normally have the same authorisation as the person for whom he or she is acting as deputy.	V	
12.2.58	If the person a user is acting as deputy for has several roles, it should be possible to restrict the deputy's access rights to a limited number of these roles.	V	
12.2.59	For one or more specified roles, it should be possible to specify that it must *not* be possible to delegate a particular role to a deputy.	V	

Requirement no.	Requirements concerning time delimitation and authorisation history	Type	Remarks
12.2.60	Information must be stored on the access rights that a user has had and when they were valid.	O	Obligatory for personal identification.
12.2.61	It must be possible to restrict the access rights of an identified user in terms of time. It must be possible for the rights to be valid from date to date.	O	Obligatory for personal identification.
12.2.62	It should be possible to restrict access rights to a specified time cycle, e.g. times of the day, days of the week, working days only, etc.	V	

Requirement no.	Requirements concerning the disclosure of user authorisations	Type	Remarks
12.2.63	For a given, active log-on identifier, it should be possible to display or print out a summary of the rights and authorities that the person concerned has in the Noark 5 solution.	V	
12.2.64	It should be possible to show or print out a summary of the authorities that a particular role or access profile has in the solution.	V	
12.2.65	For a given object in the Noark 5 solution, it should be possible to display or print out a list of users who have the various types of functional rights to this object.	V	

12.2.3 Allocation and administration of access rights

In access control theory, a distinction is made between mandatory allocation and discretionary allocation of access rights. "Mandatory" means that all allocation of rights is exhaustively regulated. In principle, a central body within the organisation could then give an account of all assigned rights and ensure that they are in accordance with the relevant policy. "Discretionary" means that the allocation of rights is an authority which can be delegated without centralised control. Everyone who is the "owner" of a data object in the solution can assign access to this object to other users. This principle is for example extensively used for access rights management within file and directory systems in most operating systems.

It is an obligatory requirement that it must be possible to perform mandatory allocation. Organisations which need it and which have less strict requirements for their access control should however also be able to choose discretionary allocation, as this form of allocation is more flexible.

Requirement no.	Requirements concerning allocation principle for authorisations	Type	Remarks
12.2.66	It should be possible to perform mandatory, administrator-controlled allocation of rights ("Mandatory Access Control", MAC) throughout the entire Noark 5 solution.	V	
12.2.67	It should be possible to perform the discretionary/user-controlled allocation of rights ("Discretionary Access Control", DAC) throughout the entire Noark 5 solution or in selected parts of it.	V	
12.2.68	In the case of the discretionary/user-controlled allocation of rights, ordinary users (all roles that do not have administrator rights) must only be able to allocate the access rights that they themselves possess.	B	Obligatory for discretionary/user-controlled rights allocation.
12.2.69	In the case of the discretionary/user-controlled allocation of rights, a user should be able to assign access to cases and/or registry entries to global or self-defined groups of users.	V	

12.3 Provision of access and availability

The fundamental assumption according to the Freedom of Information Act is that post registries are public. The general public has a right of access. However, Section 2-7 of the Archives Regulation permits the *screening* of information in electronic fonds. The condition is that the information is subject to a secrecy obligation in a law or pursuant to a law, or that it can be exempt from public access for any other reason pursuant to the exemption provisions in the Freedom of Information Act. Access codes are the Noark standard's primary mechanism for screen registry information. Specification of an access code means that screening functions

will be triggered, so that certain information concerning the folder or record will not be shown in a public registry.

An important principle for the screening of information in Noark 5 is that all the various external solutions that use the same fonds must have access to, and adapt themselves to, the screening information contained in the fonds. Many of the requirements concerning screening therefore belong to the Noark 5 core (Chapter 4). Here in Chapter 11, further recommendations are given concerning screening codes and functionality.

Screening the information in a public registry is a measure that is intended to prevent certain information from being disclosed by being made known in the registry as such. However, the authority to screen registry information must not be specified in a public registry such that "exempt from public access" is automatically specified as a predetermined classification of the underlying document. The administrative body itself must assess the issue of full or partial access to the document when it receives a request for access, regardless of whether or not certain information is screened in the registry.

However, on occasions, it will be obvious in advance that it would be inappropriate to give full access to the document. There may then be a need to indicate this in the public registry by referring to the relevant exemption authority in the Freedom of Information Act. Such predetermined classification of the document may also be appropriate in some cases where there is no authority to screen registry information, e.g. when the document, but not the registry information, contains confidential information. Noark 5 therefore requires public registries to contain separate fields for screening authority and predetermined classification.

Requirement no.	Requirements for screening functions and methods for exemption from public registries	Type	Remarks
12.3.1	There should be an indication in the registry that a record with an access code contains one or more documents that are not marked with an access code.	V	
12.3.2	If the access code is marked with an indication that there is cause to only exempt certain information in the document from access, an "official variant" of the document may be created which does not contain this information and which can therefore be exempted from screening.	V	
12.3.3	The solution should indicate which types of information are specified as requiring screening. The fact that a given piece of information has been selected for screening should be indicated both to those who have access to view the screened information and to those who do not have access to view it.	V	
12.3.4	The document description should inherit the record's access code as the default value, unless the document description already has an access code or is already linked	V	

Requirement no.	Requirements for screening functions and methods for exemption from public registries	Type	Remarks
	to another record.		

The Public Administration Act and the Personal Data Act give special access rights (subject to certain restrictions) to anyone who is a party to a case and to anyone who is registered in the public body's information system. The electronic fonds must be able to realise individual access rights for an individual party/registered party without that party needing to have a detailed knowledge of the body's organisation and authorisation decisions.

Requirement no.	Requirements concerning the provision of access for involved parties	Type	Remarks
12.3.5	For a party that requests access under the Public Administration Act, it must be possible to produce an extract of all metadata and documents concerning the case in question. Information must be shown even if it has been assigned access codes.	O	
12.3.6	For a person who requests access under the Personal Data Act, it must be possible to produce an extract of all metadata concerning the cases to which the person concerned is a party, and the records and associated documents and remarks where the person concerned is the sender or recipient. Any screened information concerning other parties to the case must be screened in the extract.	O	
12.3.7	If a person is authenticated as an external user, it should be possible for the person concerned to extract the information to which he or she has access as a party or registered person through an customised task system or access solution.	V	

12.4 Securing electronically sent and received documents

The fundamental challenge in connection with the securing of electronic exchange is that the effect of the security measures will depend on a number of parties. The public body that uses the Noark 5 solution must also have a basis for trust in the interaction. This trust can either be anchored in mutual agreements between pairs of parties, or it can be anchored in technical mechanisms which reject electronic interaction which does not comply with "the rules of the game".

The needs to secure electronically sent and received documents can be divided into four categories, as shown in the figure below. The first category is communication with known players concerning known types of content. This will usually mean communication between two administrative bodies, but the communication may also be between an administrative body and a private enterprise. The second category is communication with external parties where the

players may be unknown to each other but the content has a common known form and structure. This will often concern communication between a public body and its users, where the content consists of application forms or other structured information. The third and fourth categories are communication where the content has an unknown form and structure (e.g. letters), but known and unknown players respectively. For these two categories, appropriate recordkeeping and archiving should be based on Noark 5 *exchange format. See section 6.3* **Electronic**.

	Content with known form and structure	Content with unknown form and structure
Known players	Bilateral agreements Possibly also with shared software	Exchange format, e-mail, etc. Low requirements for security in communication
Unknown players	Integrated framework for communication f.eks. sikre web-skjemaer, ebXml e.l.	Exchange format, e-mail, etc. High requirements for security in communication

Different grounds for trust in electronically sent and received documents

For the first category, there will be few technical security requirements, as the parties can agree on the level of security and relevant security mechanisms between themselves.

For the other three categories, the fundamental principles in Section 4 of the e-Administration Regulation apply: The general principle is that anyone can contact an administrative body using electronic communication without using security services or products. If necessary, in accordance with certain criteria in the e-Administration Regulation or other law, the administrative body may however require the use of security services or products which they make available.

The e-Administration Regulation, particularly Chapter 6, supplements the regulations in the Archives Act and the Archives Regulation concerning the public body's processing of messages that are encrypted or *electronically signed.* It is generally possible to choose between different strategies for processing encrypted or signed messages. The obligatory requirements are based on a strategy which can be said to have a low level of ambition. It is based on the public body decrypting the message upon receipt. The record and document description are then assigned metadata concerning the consignment. The received document is stored in unencrypted form in the Noark 5 core. Subsequent use of the document within the body will only be based on ordinary access control in the Noark 5 solution.

There are few metadata in this area which must be stored internally in the Noark 5 solution. Detailed verification data is written to the extent that logs are required; cf. section *13 Log and audit* trail functions

.

Requirement no.	Requirements for metadata for documents received or sent with an electronic signature	Type	Remarks
12.4.1	The Noark 5 solution should indicate whether an incoming encrypted document has been signed electronically by someone other than the party specified as the sender.	V	
12.4.2	If the document referred to above was sent with an exchange format that normally results in it being processed automatically, it should be transferred to manual processing.	V	
12.4.3	When the body sends out an electronic document which is a reply to an incoming electronic document, the document should be sent out with at least the same security level as that of the incoming document.	V	
12.4.4	If received documents are to be saved in encrypted form, they should first be decrypted and then re-encrypted with signatures over which the body itself has control, so that the body is not dependent on the sender's official key in connection with future use of the document.	V	
12.4.5	When transferring electronic fonds to an archival institution, all encrypted documents should preferably be decrypted.	V	
12.4.6	If encrypted documents are to remain encrypted upon storage by an archival institution, they should first be decrypted and then re-encrypted with signatures over which the archival institution has control.	V	

13 Log and audit trail functions

Audit trail information is the ongoing record of events that are carried out in or by the Noark 5 solution. This includes events carried out by users or administrators, and events that are automatically performed by the Noark 5 solution as a result of automated functions. Audit trail information describes and documents specific parts of the archival document's history.

The automatic record of events and actions fulfils a number of purposes. These purposes can largely be divided into two main categories, according to time phases: One category is administrative use, under archive creation. The purposes are then to audit or retrospectively assess the actions of users and communication parties. In this case, relevant audit trail information could be who opened or altered a document, or detailed information from digital verification mechanisms. The second category is authenticity-supporting information, in order to understand the context of which the documents were originally part, and retrospectively assess the grounds that the administrative body had to trust the authenticity of the documents. Relevant audit trail information could be information concerning the case handling process, changes to the document's organisational affinity, classification, file formats, who decrypted and verified electronically received documents, etc.

13.1 Principles for logging

13.1.1 A**Audit trail information in external logs**

The general principle, which is the most appropriate in most cases, is to store the audit trail information as external *logs*. An external log consists of automatic records which are written to separate files (possibly to special database structures) outside the Noark 5 solution. The log is not normally available to ordinary users in an ordinary use situation. It is used for auditing and retrospective testing only. Audit trail information can often consist of information that only exists in external task systems and not in the Noark 5 core, e.g. in the form of workflow and events which have documentation value.

13.1.2 Audit trail information as metadata or as a separate document in the fonds

For certain purposes, it may however also be appropriate to store audit trail information as metadata in the Noark 5 core. This particularly applies to automatic records to which it can be useful to have access together with documents and other case-related metadata. Audit trail information stored as metadata can be available during normal use of the solution, unlike logs which are only used for subsequent checks and auditing. This is an alternative strategy to external logs.

For example, process information from case handling which has taken place in an external task system may be stored as separate documents in the fonds. This could help to make information which is essentially specific to the task system available to any other users of the fonds who are not logged on via the same task system. This strategy means that audit trail information in the form of workflow and events which have documentation value are archived as a separate document type in the Noark 5 solution. This can take place upon the conclusion of processing. Depending on the type of processing that is concluded, the document can be linked to *either:*

a. The record, as a sort of attachment/appendix, with a description of the processes that the record was subject to before it was finalised

or:

b. The file level, which means that the document and audit trail information are linked together as a separate record/registry entry.

13.1.3 Configurability

The log could become very large if every single event were to be logged. Relatively modest obligatory requirements are therefore imposed on what must be logged. A public body should however be able to register significantly more audit trail information than the obligatory information if it needs to do so. Ideally, it should be possible to log all changes to metadata and documents in the Noark 5 solution if necessary.

It should also be possible to increase the number of events that are registered temporarily, for a shorter or longer period of time. This could help in the analysis of work processes, information flow and the use of access rights, etc., without the logs needing to grow uninhibited throughout the entire recordkeeping phase.

13.1.4 Special strength requirements, unchangeability

Noark 5 first and foremost sets out requirements concerning the audit trail information that must be registered. The requirements regarding function and content do not in themselves provide a basis for determining the level of confidence that other players can or should have that the logs provide an accurate picture of the registered events. For certain uses, there may be a need to prove that a log has not been, nor could have been, manipulated. Understanding what has happened in an error situation internally within the organisation does not impose such high requirements concerning proof. The requirements for ensuring non-refutability in electronic communication with other parties will be significantly higher.

"Unchangeability" is a requirement that cannot be given a fixed and unique definition. However, it can be demonstrated in different ways and to differing degrees. The minimum requirement according to Noark 5 is that the logs themselves are subject to access control. The use of "hash functions", which can generate an electronic checksum calculated on the basis of the content of documents or metadata, can give greater confidence that the contents have not been manipulated. Another example of a stricter requirement is to write logs to a "WORM" (write once, read many) storage medium. A third example is to transfer logs automatically to a neutral third party. Different measures to ensure unchangeability can also be combined if special needs apply. Each individual public body must itself decide and implement logging with the strength requirements that are appropriate given the nature of the organisation.

13.2 General requirements for audit trail information

The generation of audit trail information must be handled by identifiable functions in the solution, which are documented and configurable and can be covered by the solution's access control.

Requirement no.	Requirements for function for handling audit trail information	Type	Remarks
13.2.1	The Noark 5 solution should have functions which automatically register and store information concerning defined events that have occurred with documents and metadata in the solution.	V	
13.2.2	The Noark 5 solution should have a register which specifies the events (defined rules) that will trigger the record of audit trail information.	V	
13.2.3	For all events that are to be registered, the following information must always be logged: 1. SystemID for the data object (file, record, document, classification, organisational unit, etc.) which the event concerns 2. Reference to the defined rule which triggered the record (cf. the requirement above) 3. Event (full text description or code with reference to table) 4. Date and time of the event 5. Who triggered the event (identification of user, identification of the external system concerned, name of the system event concerned or batch run or similar)	B	Obligatory if 13.2.1 is fulfilled.
13.2.4	It should be possible to log different types of event to different external files or database tables. (It must be possible to delete certain types of logs, e.g. for the auditing of access controls after a defined time. Other types of log must be preserved for a long period of time. Logs that are to be deleted and logs that are to be preserved should be kept separate from each other).	V	
13.2.5	Access to logs and other audit trail information must be subject to access control.	O	
13.2.6	The logging should be configurable. As a minimum requirement, it must be possible for the system or fonds administrator to activate or deactivate recommended logging rules.	V	
13.2.7	Access to make changes to what is being logged must be subject to access control and require administrator rights.	B	Obligatory if 13.2.1 and 13.2.2 are fulfilled.
13.2.8	Audit trail information should be easy to browse, search and analyse, either with the aid of functionality in the Noark 5 solution or with the aid of a third party program.	V	

Requirement no.	Requirements for function for handling audit trail information	Type	Remarks
13.2.9	It should be possible to read or print out audit trail information sorted according to at least the following criteria: 1. Chronologically according to when an incident was actually registered in the log 2. According to the user's log-on identifier and then chronologically 3. According to organisational unit and then chronologically	V	
13.2.10	It should be possible to store external logs on a physical storage medium other than that on which the Noark 5 core and, where applicable, the task system concerned are located.	V	
13.2.11	As a configurable option, it should be possible to store audit trail information internally within the Noark 5 solution. This variant is an alternative to external logs. Logs that are stored internally within the fonds will primarily be relevant for events which it may be relevant to make available to users of different external task systems which use the same fonds, e.g.: • Storage of new or altered information in files, records, document descriptions, classification forms and fonds structure • Information on the conversion of document file format, storage of new variants or versions of documents	V	

13.3 Auditing and retrospective evaluation of access controls

Logs of log-ons and the use of access rights can be used for random samples, to investigate specific undesirable events or for more comprehensive audits. It will normally only be appropriate to preserve such a log for a limited period of time. It should therefore be saved in a separate file, which can be deleted without affecting other audit trail information.

Requirement no.	Requirements for controls concerning logging on and authentication of users	Type	Remarks
13.3.1	Audit trail information for the auditing and retrospective evaluation of access controls must be saved as external logs outside the Noark 5 core, in separate files, separate databases or similar.	B	Obligatory if 13.2.1 and 13.2.2 are fulfilled.

Requirement no.	Requirements for controls concerning logging on and authentication of users	Type	Remarks
13.3.2	All logging on by database administrators, users with the right to alter installation/program modules and other users with administrator rights in the Noark 5 core must be logged with the following information: • Log-on identifier • Date and time of logging on and off • Terminal identity, or alternatively MAC address or IP address, which can indicate where the person logged on from • Specification of new or deleted program modules • New and old version numbers of altered program modules • Commands that have been executed, or before value/current value in connection with configuration changes	B	Obligatory if 13.2.1 and 13.2.2 are fulfilled.
13.3.3	All correction of users and all allocations of or changes to the administrator rights of a user must be logged with the following information: • Log-on identifier of the user who performed the change • Log-on identifier and full name and any initials of the user that the change concerns • The rights that have been allocated or altered • Date and time of the change	B	Obligatory if 13.2.1 and 13.2.2 are fulfilled.
13.3.4	Allocation and withdrawal of rights for all users in ordinary roles. It should be possible for the following information to be logged: • Log-on identifier of the user who performed the change • Log-on identifier and full name and any initials of the user that the change concerns • The rights that have been allocated or altered • Date and time of the change	V	
13.3.5	Logging on of users who are given access to the Noark 5 core, either directly or indirectly via an external system. The following information must be logged: • Log-on identifier • Date and time of logging on and off	B	Obligatory if 13.2.1 and 13.2.2 are met.

Requirement no.	Requirements for controls concerning logging on and authentication of users	Type	Remarks
13.3.6	Logging on of users with ordinary roles who are given access to the Noark 5 core, either directly or indirectly via an integrated solution. It should also be possible for the following information to be logged: • Selected role or access profile for the user • Terminal identity, or alternatively the MAC address or IP address	V	
13.3.7	For all types of logging on, unsuccessful/rejected attempts must be logged with the following information: • Entered – valid or invalid – log-on identifier • Entered password or any other identification • -{}-Date and time of the log-on attempt • Terminal identity, or alternatively the MAC address or IP address	V	

It should be possible to log users' actions, for auditing purposes and for retrospectively evaluating whether they have acted according to their professional needs. For many administrative bodies, it would be impractical to allocate authorisations that are sufficiently precisely defined for each individual user's duties. Some users may therefore have authorisation in the solution to perform actions that do not fall within their actual duties or authorities.

Requirement no.	Requirements for controls to evaluate whether actions are in line with professional needs	Type	Remarks
13.3.8	Logging to evaluate whether actions are in line with professional needs should be configurable at a detailed level. • Specify/delimit the authorisations (roles, profiles, etc.) for which logging must be instigated • Specify whether only the fact that a change has taken place is to be registered or whether the old/new value must also be registered. • Specify whether the reading of objects must be logged. • Specify whether search hits must be logged • Specify whether the use of functions for extracts must be logged • Specify whether the use of functions for saving or exporting documents or metadata to a file path or other program outside the Noark 5 core is to be logged	V	

Requirement no.	Requirements for controls to evaluate whether actions are in line with professional needs	Type	Remarks
13.3.9	Logs of one or more types of events in the requirement above must contain at least the following information: • Log-on identifier • Date and time of the record • Role or access profile with which the person concerned is logged on • If the user is logged on as a deputy, the person for whom the user is acting as deputy • The program/screen/menu option or similar being used	B	Obligatory if 13.3.8 is fulfilled.

13.4 Requirements for audit trail information for different types of events

Here, obligatory requirements and recommendations concerning different types of events which must or should be logged are subdivided into three main groups. The first group consists of events during ordinary, internal use of the solution. This group gives audit trail information for quality assurance and troubleshooting. The next group consists of events linked to electronic communication. This group covers records from technical verification mechanisms and could to some extent be used to show what communication has taken place. The third group of events documents actions and changes linked to administration of the fonds.

Requirements and recommendations here specify only the type of content that must or can be registered. There are no format requirements for the logs, e.g. requirements for sequence, line breaks, tabulations or other guidelines concerning structure. Other content elements can be added freely to the log as necessary.

Requirement no.	Requirements for the logging of events during case handling, document handling and recordkeeping	Type	Remarks
13.4.1	The following must be logged when a new file, record or document description is logged for the first time: 1. Object identifier 2. Date and time of saving 3. User, role and organisational unit which created the object	B	Obligatory for case records.

Requirement no.	Requirements for the logging of events during case handling, document handling and recordkeeping	Type	Remarks
13.4.2	The following should be logged when a new incoming electronic document which is either scanned or received electronically is saved for the first time: 1. Identifier or file name and location of the document, which can be used for unique identification in the fonds 2. Date and time of scanning or receipt by the electronic reception unit (i.e. normally before the executive officer has begun the processing work) 3. Who: solution, organisational unit, any user or role who performed the save 4. Document format (file type, extension, mime attachment type or similar) 5. Any new document format if the document is converted upon receipt 6. Readable = Y/N, result of a check to determine whether a program for reading, viewing or editing the document format was available at the time of creation	V	
13.4.3	The following should be logged when a new document produced in the Noark 5 solution is saved for the first time: 1. Identifier or file name and location of the document, which can be used for unique identification in the fonds 2. Date and time of the first saving of the identifier referred to above 3. User and role who saved the document and, where applicable, the task system used 4. The document's production format (file type, extension, mime attachment type or similar)	V	
13.4.4	Deletion of metadata at all levels in the fonds structure must be logged. The following is in addition to the obligatory log data: 1. Identifier for deleted metadata 2. Specified reason for the deletion (any authority or order)	B	Obligatory for case records.

Requirement no.	Requirements for the logging of events during case handling, document handling and recordkeeping	Type	Remarks
13.4.5	Deletion of documents must be logged. The following should be logged in addition to the obligatory elements in the requirement above: 1. Identifier or specification of file name and location from which the document was deleted 2. Code or description of rule for routine, automatic deletion (cleanup of superfluous versions, etc.) 3. Any specified reason in connection with manual deletion	V	
13.4.6	Conversion of documents (format change) should be logged. The following is in addition to the obligatory log data: 1. Old file format 2. New file format 3. Time of conversion, duration of the task 4. Any status codes/error messages from the conversion program	V	
13.4.7	In the case of system-generated/batch conversion of documents (change of format), information on the selection criteria, start time and duration of the entire job should be logged.	V	

Noark 5 solutions will have different needs for the logging of changes and activities. The same public body could also have different needs for the logging of different series. In requirement no. 0, it is recommended that aspects of the logging should be configurable, i.e. the fonds administrator should be able to choose how much of what is done in the solution is to be logged. It will often be desirable to restrict the logging for capacity reasons and on the basis of an assessment of the usefulness of the logs. The table below contains minimum requirements for logging that must be configurable, if the Noark 5 solution provides for configurable logging.

Requirement no.	Requirements for configurable options for additional logging	Type	Remarks
13.4.8	Configurable option: It must be possible to log all finalisation of documents and metadata.	B	Obligatory for case records.
13.4.9	Configurable option: It must be possible to log all deletion of finalisation codes.	B	Obligatory for case records.
13.4.10	Configurable option: The solution must be able to log the setting of a document to approved.	B	Obligatory for case records.

Requirement no.	Requirements for configurable options for additional logging	Type	Remarks
13.4.11	Configurable option: The solution must be able to log the depreciation of a document.	B	Obligatory for case records.
13.4.12	Configurable option: The solution must be able to log the editing of a document after it has been approved.	B	Obligatory for case records.
13.4.13	Configurable option: It must be possible to log changes to classification value for an individual information object (within an existing classification).	B	Obligatory for case records.
13.4.14	Configurable option: It must be possible to log changes in depreciation method.	B	Obligatory for case records.
13.4.15	Configurable option: It should be possible to log the viewing, presentation and duplication of a document. The points below specify various events which it should be possible to log – where the events can be captured. The opportunities to capture these events will depend on the integration methods and other factors, and the strictness of the security regime under which the solution operates. 1. Viewing, in a read program *without* the option of editing, copying, exporting or saving to an external unit 2. Viewing, in a read program which facilitates copying, external storage or exporting 3. Opening in production software, but *without* the possibility of external storage or copying ("cut and paste") 4. Opening in production software, with provision for external storage or copying of content 5. Record of actual use of the document's content a. Shown on the screen b. Sent to printer or fax c. Copied in full or in part, or saved on another storage unit/storage medium d. Sent to an internal or external e-mail recipient without record	V	

Electronic exchange and communication can be carried out with different levels of security. Noark 5 provides no guidelines concerning the security level that must or should be used for different types of information or case handling processes. However, the requirements in the table give an overview of what should be logged in connection with the use of different levels of security in the communication. In general, higher security levels lead to more logging being

required than lower security levels. This is because a better audit trail is anticipated with higher security levels.

Requirement no.	Requirements for the logging of events in connection with electronic exchange and communication	Type	Remarks
13.4.16	If the sender of electronic documents is authenticated as an employee of a given organisation, it is the identification of the *organisation*, and where appropriate the anonymised employee number, which should be stored in the log. The full national identification number of a person who is authenticated as an employee of an external organisation should not be stored unnecessarily.	V	
13.4.17	The following should be logged upon receipt of unencrypted e-mail: 1. Any description of or reference to a description of the exchange format 2. The sender's e-mail address 3. The sender's e-mail server's message ID 4. Specified time of sending 5. Whether the message has attachments 6. Whether the sender has requested a delivery/read receipt 7. Time of receipt by the recipient's e-mail server 8. Recipient's e-mail address	V	
13.4.18	The following should be logged upon receipt of encrypted e-mail: 1. Identification of third party certification authority 2. Identification of who the certificate was issued to 3. Security level and any signature	V	
13.4.19	Upon the receipt of e-mail that is registered where the sender has requested a delivery or read receipt, a receipt message should be sent automatically. The time and reference to the correct message ID for the sent receipt message must be logged.	V	
13.4.20	The following must be logged upon the sending of unencrypted e-mail: 1. Any reference to exchange format 2. Sender's log-on identifier and role 3. Sender's e-mail address 4. Sender's e-mail server message ID 5. Time of sending 6. Whether the message has attachments 7. Whether the sender has requested a delivery/read receipt 8. Recipient's e-mail address	V	

Requirement no.	Requirements for the logging of events in connection with electronic exchange and communication	Type	Remarks
13.4.21	The following should be logged upon the sending of encrypted e-mail: 1. Identification of third party certification authority 2. Identification of who the certificate was issued to 3. Security level and any signature	V	
13.4.22	The following should be logged upon (any) receipt of a delivery or read receipt linked to e-mail that has been sent by the public body: Time, reference to the e-mail that the receipt concerns, and identification of the sender's e-mail server.	V	
13.4.23	Configurable option: Upon the sending of electronic documents, it should be possible to log the identifier or file name and the location of all documents that are sent as attachments.	V	
13.4.24	The following should be logged in connection with the use of web forms without authentication of external users and without secure communication (https protocol or equivalent): 1. IP address 2. URL where the web form was available to the external user 3. Time of submission 4. Any specified key information, such as the name that the external user entered in the form	V	
13.4.25	In addition to the recommendations in requirement 0, the following should be logged in connection with the use of web forms without authentication of external users but with secure communication (https protocol or equivalent): 1. Who the website certificate was issued by 2. Who the website certificate was issued to 3. The certificate's period of validity	V	
13.4.26	The following should be logged in connection with the use of web forms with authentication of external users and with secure communication (https protocol or equivalent): 1. The external user's electronic ID or other specified unique identification 2. Authentication method or security level 3. Identification of any third party which has authenticated the external user	V	

Requirement no.	Requirements for the logging of events in connection with electronic exchange and communication	Type	Remarks
13.4.27	In the event of the use of special security products which offer an integrated framework for electronic message exchange, the log requirements for the framework must be followed, where appropriate with relevant additions from other requirements in this table.	B	

The events in the table below originate from actions that can only be performed by users in administrator roles.

Some of this audit trail information should also be included in the fonds plan. Provision should therefore be made to ensure that appropriate "data capture" can be performed from relevant parts of this audit trail information (cf. the principles for logging at the start of the chapter).

Requirement no.	Requirements for the logging of events in the fonds' lifecycle, structure and classification system	Type	Remarks
13.4.28	Changes in the register of "events that trigger logging" (cf. requirement no. 0) must be logged.	B	Obligatory for case records.
13.4.29	Export/transfer of fonds or series to units outside the Noark 5 solution must be logged. 1. Date of export 2. From fonds 3. From series 4. Identified structural elements that are exported (fonds, series, grouped cases, classes) 5. Scope of exported/transferred structure (outer year from – to) 6. To fonds (if information is available on it) 7. To series (if information is available on it)	B	Obligatory for case records.
13.4.30	Changes to the transfer time must be logged. In addition to obligatory log data: 1. Old rule (code) and date of transfer 2. New rule (code) and date of transfer	B	Obligatory for case records.
13.4.31	Changes to lifecycle rules (deletion, preservation and remote storage) must be logged. In addition to obligatory log data: 1. Old rule (code) and date of deletion/preservation 2. New rule (code) and date of deletion	B	Obligatory for case records.

Requirement no.	Requirements for the logging of events in the fonds' lifecycle, structure and classification system	Type	Remarks
13.4.32	All changes to a classification system must be logged. The following belong to classification system: • Archive keys • Topic-based classification system • Object-based classification system • Topic map • Thesaurus • Ontology/taxonomy • Predefined file structures of other types • Other classification methods (unique, predefined ways of grouping documents)	B	Obligatory for case records.
13.4.33	In the event of changes to a classification that includes "counters" (e.g. case numbers = year + serial number), only changes in the classification's fixed elements should be logged. Changes in the counter should not be logged.	V	
13.4.34	Configurable option: In the case of the use of object codes as a classification method, e.g. national identification number, property or plot number or other object codes from external register administrators, additions (or data imports or look-ups in external registers) should be logged.	V	
13.4.35	The installation (or patching) of new program modules or new versions of program modules must be logged.	B	Obligatory for case records.
13.4.36	Changes in the location (to a new location in a logical file structure) of database and documents files should be logged.	V	
13.4.37	Information on changes in location must include: 1. from location/directory 2. to location/directory 3. the date on which the document was moved from its current location 4. date on which the document was received 5. who was responsible for the movement	B	Obligatory if 13.04.36 is fulfilled.

14 Terminology

The following list is restricted to terms that are used in the standard.

Term	Explanation
Archival format	Standardised format for electronic recordkeeping and prepared for long-term storage. Specified in Regulation No. 1566 of 1 December 1999 concerning supplementary technical and archival provisions regarding the handling of public fonds, Chapter VIII (the transfer provisions).
Archival repository	Institution where fonds material worth preserving is kept permanently. The archival repository relieves the fonds creator by storing older fonds material and serving users who are interested in the material.
Archive (archives as used in Norway and in this standard)	1. Documents created as part of an activity, i.e. documents which are received or produced by a single fonds creator and collated as a result of his or her activity (also known as a fonds entity). 2. Storage location for fonds . 3. Organisational unit that performs tasks linked to fonds, also known as a registry office. 4. The same as archival repository.
Authentication	The meaning of the term within the field of access control. A function that determines whether the information that a person enters in the IT system (user name, password, magnetic strip card, fingerprints, etc., depending on the individual solution's needs for secure authentication) provides sufficient security that the person is who he or she claims to be.
Authentication metadata	Metadata that are intended to support the document's authenticity and credibility, partly by giving the recipient information that can be utilised in connection with checks on the document's content and sender.
Authenticity	Authenticity means *genuineness* or *originality*, the opposite of a copy or forgery. In the context of fonds, this means that the document is what it claims to be, e.g. by the fact that the identities of the parties in an electronic communication are correct.
Authorisation	Authorisation consists of rules (which are preferably enforced electronically within the IT system) concerning the information to which an *authenticated* person has access and the actions that he or she can perform.
Back log	Received registry entry that has not been signed off. See Sign off.
Business analysis	See Decision support.

Term	Explanation
Case	1. Abstract: An issue for processing, based on an external enquiry or an initiative by the organisation itself (cf. the Public Administration Act and the Freedom of Information Act. The term is also used concerning the decision-making process itself. 2. Concrete: Cases include the case documents, records, notes, etc. which arise in connection with and are part of the decision-making process. 3. In electronic registry/record solutions (Noark): Cases consist of one or more registry entries and their associated documents, linked together under a common identity (case number). See Case file.
Case document	According to the Freedom of Information Act, the case documents of the administration are documents issued by an administrative body and documents received by or presented to such a body. In a recordkeeping context, the term is mainly used in a similar, but slightly more limited, manner. A case document is always a fonds document, but not all fonds documents are case documents. A case document is created when it is dispatched by the body. If this does not take place, the case document is considered to be created when it is finalised.
Case file	A specialisation of the record unit file in the fonds structure. See Case.
Case follow-up	To follow up the handling of a case, e.g. checks on the handling in relation to due date, back log checks, etc.
Case fonds	The portion of the fonds which consists of case documents, i.e. documents which have been received by or submitted to a body, or which the body has itself created, and which concerns the body's area of responsibility or operation.
Case handling	Evaluation of information relating to an internal or external issue with a view to making a decision.
Case list	List of meeting cases from the queue list that are to be considered at a given meeting.
Case-responsible	Executive officer who is responsible for processing the case as a whole. See also Executive officer.
Certificate	A certificate is information (which an independent third party can verify) which a recipient needs in order to decide whether he or she can trust the sender of electronically signed material.
Classification	Classification is dividing things or terms into classes, i.e. assigning a fonds document classification values that describe function, activity, topic or object.

Term	Explanation
Confidentiality	It must not be possible for unauthorised persons to read the meaningful content.
Content management	Management of all types of content (documents and data) within an organisation.
Co-sender	"Co-sender' means a sender who is not responsible if an incoming document has several senders.
Current fonds	Fonds in daily use by the fonds creator. The first phase of the fonds material's lifecycle.
Decision support	Collective term referring to solutions, applications and technology with the aim of collating, structuring and making available information. The aim is to give organisations the opportunity to improve the quality of decisions by providing the right information at the right time.
Decision-making body	Collective term for board, council, committee, political body, body with decision-making authority, advisory body, etc.
Digital signature	General term for technology, methods, regulations and administrative/supervisory tasks which collectively provide sufficient certainty that electronic information that has been "signed" originates from the specified sender and that the content has not been manipulated.
Dispatch date	Date which indicates when a document was sent.
Disposal	To dispose of, i.e. to remove material that has been subject to case handling or has had document value from the fonds and to destroy it; cf. Section 3-18 of the Archives Regulation.
Document	Logically delimited quantity of information which may be stored on a medium for future reading, listening, presentation or transfer. A document may be stored on paper, an electronic medium, micro-fiche or any other medium that can carry information. Documents can contain text, drawings, graphics, photographs, video, speech, etc.
Document description	A level in the fonds structure, a record unit. Metadata for fonds documents, which specify the content of the fonds document.
Document management	Record, storage, searching, presentation, management and control of documents. Management of all types of documents, unfinished documents, working documents and fonds documents, independent of recordkeeping.
Document object	A level in the fonds structure, a record unit. Metadata for document files. Document object is the lowest level in the fonds structure.
Electronic document	A document stored on an electronic medium in a format suitable for retrieval, processing and distribution with the aid of a computer.

Term	Explanation
Electronic fonds	Fonds which consist of electronic documents.
Executive officer	The person within the organisation who is responsible for following up and processing one or more documents in a case. See also Case-responsible.
File	A level in the fonds structure, a record unit. One or more fonds and associated fonds documents that are linked together under a common identity.
Fonds administrator	The Archives Regulation's term (§ 2-1) for the person who has day-to-day responsibility for recordkeeping in a public body and who manages the registry office. Also known as fonds manager.
Fonds capture	Identifying fonds worthy of recording, capturing them and archiving them, i.e. the documents are assigned metadata (registered) and frozen (archived), so that neither the document nor the associated authenticated metadata can be changed.
Fonds creation	The act of creating or generating fonds. Also used as a collective term for the initial phases of the fonds material's lifecycle (current fonds and remote storage fonds), i.e. the phases during which the fonds creator is responsible for the material (the fonds creation phase).
Fonds creator	An organisational unit or person who creates fonds as part of his/her/its work. A fonds creator may be a public body, a company, an organisation, a foundation, etc. or a part of such a unit. A public body may be one fonds creator and therefore have one fonds entity (central registry), or it could have several fonds creators (departments, agencies, etc.), each of which create their own fonds entities (partial fonds).
Fonds period	The period of time into which the fonds (1) are divided in connection with remote storage, etc.
Fonds series	Part of fonds, grouped according to a common classification scheme.
Fonds structure	The logical, hierarchical order of a fonds entity.
Fonds unit	An individual level in the fonds structure.
Fonds weeding	Excluding or removing from the fonds documents which are neither subject to processing (case handling) or of documentation value; cf. Section 3-18 of the Archives Regulation.
Form	Collection of questions and explanations which under a name enable the declaration of a limited set of information to be submitted by a single person in a single delivery or transmission.
Format	A single document can be stored in several formats. In terms of fonds, we principally refer to production format and fonds format.

Term	Explanation
Genuineness	See authenticity.
Greying out	The marking of possible passive responses or passive response fields or with associated header texts to indicate that they are not available in the current situation. The marking is indicated by a paler (generally grey) colour than the active characters/field.
Information management	Information management comprises all strategic and practical tasks that an organisation performs in order to enable the organisation to utilise the commercial potential that data, documents, information and knowledge offer.
Information provider	The (physical) person who goes through and answers the questions on a form, or who provides data from one or more files, for submission to task retrievers. This could be the information provider himself when the task obligation rests with a physical person. In other cases, the information provider will generally be an employee of the information provider or of the information provider's accountants, auditors, lawyers, etc.
Integrity	Linked to content, that data (the document) has not been altered or destroyed in an unauthorised manner or erroneously; a property in connection with data which makes it possible to discover whether data has been altered in an unauthorised manner or erroneously. In terms of fonds, integrity is an indication that the fonds document has not been "messed around with" and that the information reproduces the actual events and circumstances.
Internal document	A document prepared for an administrative body's internal preparation of a case, either by the body itself or by a subordinate unit, special advisors, experts or a ministry for use by another ministry.
Knowledge management	Organisational and technological measures for the preservation, refining and further development of "intellectual capital" within organisations.
Lifecycle	The sequence of development that a fonds document undergoes from its creation until it is stored for the future in an archival repository (or disposed of). It is normal to operate with three phases in the lifecycle of the fonds documents: active archive, remote-storage archive and archive repository. The first two come under archive creation.
Logging	Logging is the sequential storage of data, often in chronological order.
Meeting	A meeting within a decision-making body in order to process cases in a case list.

Term	Explanation
Meeting case	A delimited problem that a decision-making body must consider in a meeting.
Meeting case status	For case plan, case plan locked, case rejected, case finalised ("reported"), case deferred.
Meeting case type	Case draft from an administrative unit, delegated case, minutes case, interpellation and unregistered case ("any other business").
Meeting minutes	A report (minutes) from a specific meeting of a board. It consists of information such as time, place, attendance, etc. as well as reports/minutes for all cases that were considered during the meeting.
Memo	Internal document that is prepared within a body as part of the preparations for a case. See also Internal document.
Metadata	Metadata are data that serve to define or describe other data. In terms of fonds, this will for example be information on the structure, content and context of a document.
OAIS	ISO 14721: 2002 Reference Model for an Open Archival Information System (OAIS). This is an ISO standard for the preservation of records.
Overlap period	Transitional phase between an old and a new fonds period, usually the first two years of each new fonds period.
Paper document (Physical document)	Document in paper form.
Parameter	Variable that is assigned a value in connection with a particular use. Used concerning fixed options which must or should be available in the solution.
Periodisation	To define regular time intervals for the recordkeeping. This means that all cases containing documents which have been registered during a specific period of time (known as a "fonds period") are sent for remote storage simultaneously and comprise a unit in the remote-storage fonds.
Precedent	A (legal) decision which establishes a precedent for the processing of similar situations or cases. A precedent can also be a case that is governing for the handling of other similar cases. It usually concerns administrative resolutions, i.e. individual resolutions passed in accordance with the administration area of the body concerned which contain a legal view that is subsequently used as a basis in other similar cases.

Term	Explanation
PREMIS	Data Dictionary for Preservation Metadata: Final Report of the PREMIS Working Group (OCLC and RLG 2005). PREMIS stands for "Preservation Metadata: Implementation Strategies". The PREMIS Working Group describes a model – a core of metadata – which can be used for digital preservation, irrespective of the type of documents or preservation strategies.
Preservation	Storing fonds material for a long period of time. In the Archives Regulation, preservation means that the material is stored for the future and transferred to an archive repository; cf. Section 3-18.
Production format	The format in which an electronic document was produced, i.e. usually the storage format that was used by a word processing system.
Public registry	A copy of the registry that is made available to the public, from which information that is exempt from public access has been crossed out. See also Screening.
Queue list	Cases that have been fully processed by the administration are notified as ready for processing by the decision-making body by placing them in a queue list.
Record	Document received or produced as part of the activity which an organisation performs, and which is not subject to fonds weeding. Consists of one or more documents that are linked to metadata and frozen (i.e. neither the document nor the associated authenticated metadata can be changed). Corresponds to the Norwegian term "arkivdokument". See also Case document.
Record	The English term that corresponds to the Norwegian *arkivdokument.* Document created or received by a person or organisation as part of the activity which is maintained by the person or organisation (Moreq).
Record	Systematic and continuous logging of information in a registry. In accordance with Section 2-6 of the Archives Regulation, all incoming and outgoing documents that are used in case handling and have documentation value must be registered. Internal documents are registered where appropriate. In the legislation, the time of record is used as a basis for determining deadlines in connection with case handling.
Record	A level in the fonds structure, a record unit. Documentation of a transaction, including metadata for the record.

Term	Explanation
Record date	In principle, the registry/record date must be the date on which an incoming document is received by or presented to the body, i.e. the date of receipt of an incoming document. For inhouse-produced documents, the registry date will be the date on which the registry office quality-assured the document after it was sent or finalised. In accordance with Section 2-7 of the Archives Regulation, the registry date must be stated in the registry, and in the case of paper-based fonds, in accordance with Section 3-4 it must be a heading in the registry stamp. Registry date is also a selection criterion for the collective chronologically sorted report of all records during the period.
Registry	Register of case documents that are processed (sent, received) by a body.
Registry date	See record date.
Registry entry	An individual record (entry) in a registry, i.e. the information on a case document and any attachments.
Registry information	The information that is contained in a registry; cf. Section 2-7 of the Archives Regulation.
Registry management unit	Registry management unit is the name of the organisational unit that is responsible for the organisation's record and recordkeeping. Other names that are used are "registering unit" and "registry office".
Remote-storage fonds	Material which has been stored according to the principles described under remote storage. The second phase in the fonds material's lifecycle.
Reply data	The information provider's entries in free text fields and selections from single- or multiple-choice lists.
Role	Within access control, roles consist of groups of similar tasks, so that the *authorisation* can be assigned to several people with the same role instead of each individual person.
Screening	Use of neutral characters, omissions or strikethroughs on a copy of or extract from the registry to which the public may request access (cf. Section 2-7 third paragraph of the Archives Regulation).
Semi-current fonds	Removing after a certain period of time (normally a specific number of years) fonds material from the active fonds and storing it in an appropriate location; cf. fonds period.
Sender	A person who sends a letter, parcel, e-mail, electronic message, SMS or similar.

Term	Explanation
Series	A grouping of fonds (entity) constituted by a common classification scheme. Its definition is often, but not always, identical to that of a *fonds series.*
Sign off	Registering information in the registry as to when and how the processing of an incoming document has been completed. "Depreciation" as a suggested term is not used in this English version, the Norwegian term is "Avskrivning".
Transaction information	Information that is registered in connection with the use or transfer of data, including transactions that are added automatically.
Variant	An alternative edition of a fonds document, which is filed in addition to it. In a variant of a fonds document, the content of the document has been altered relative to the original document. The most common variant will be a publicly available version of the document from which confidential information has been removed, so that it can be made publicly available.
Version	An edition of a fonds document at a particular point in time. The most recent version will be the final version.

LAST PAGE OF THE STANDARD