Guide to the WMO Information System

2019 edition

WEATHER CLIMATE WATER

WORLD
METEOROLOGICAL
ORGANIZATION

WMO-No. 1061

Guide to the WMO Information System

2019 edition

WORLD
METEOROLOGICAL
ORGANIZATION

WMO-No. 1061

EDITORIAL NOTE

METEOTERM, the WMO terminology database, may be consulted at http://public.wmo.int/en/resources/meteoterm.

Readers who wish to copy hyperlinks or technical examples from the text should be aware that the PDF version of this publication contains invisible spaces following http://, https://, ftp://, ftps://, sftp://, mailto:, and after slashes (/), dashes (-), periods (.), colons (:) and unbroken sequences of letters and numbers. These additional spaces should be removed from the pasted text. For URLs, the correct URL is displayed when hovering over the link or when clicking on the link and then copying it from the browser. An editable version of the English text is provided at https://wis.wmo.int/WIS-Guide-Editable for those users that need to copy technical examples.

WMO-No. 1061

Chair, Publications Board
World Meteorological Organization (WMO)
7 bis, avenue de la Paix
P.O. Box 2300
CH-1211 Geneva 2, Switzerland

Tel.: +41 (0) 22 730 84 03
Fax: +41 (0) 22 730 81 17
Email: publications@wmo.int

ISBN 978-92-63-11061-9

NOTE

The designations employed in WMO publications and the presentation of material in this publication do not imply the expression of any opinion whatsoever on the part of WMO concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The mention of specific companies or products does not imply that they are endorsed or recommended by WMO in preference to others of a similar nature which are not mentioned or advertised.

PUBLICATION REVISION TRACK RECORD

Date	*Part/ chapter/ section*	*Purpose of amendment*	*Proposed by*	*Approved by*

CONTENTS

Page

Page

Page

INTRODUCTION

Purpose of this Guide

1. In conjunction with the *Manual on the WMO Information System* (WMO-No. 1060) (*Manual on WIS*), the *Guide to the WMO Information System* (*Guide to WIS*) is designed to ensure adequate uniformity and standardization in the data, information and communication practices, procedures and specifications employed by Members of the World Meteorological Organization (WMO) in the operation of the WMO Information System (WIS) as it supports the mission of the Organization. The *Manual on WIS* contains standard and recommended practices, procedures and specifications. The *Guide to WIS* contains additional information concerning practices, procedures and specifications which Members are invited to follow or implement in establishing and conducting their arrangements in compliance with the WMO Technical Regulations and in developing meteorological and hydrological services.

2. Because WIS cuts across all related WMO disciplines, many other WMO practices, procedures and specifications intersect WIS. These are described in the relevant publications, for example, the *Guide to the Global Data-processing System* (WMO-No. 305) and the *Guide to the Global Observing System* (WMO-No. 488).

Benefits of WIS

3. The WMO Information System provides an overarching approach to data and information management for all WMO and related international programmes, leveraging the long-standing collaborative culture of WMO, as well as new technologies.

4. WMO Members expect to realize specific benefits from WIS:

- Enhanced collection of critical data needed to monitor and predict aspects of the environment, including hazards;

- A catalogue of the full range of data and products, simplifying search and ensuring equitable access consistent with WMO policies;

- Enhanced availability of time-critical data and products at centres in all countries, ensuring the effective provision of services to their populations and economies;

- WMO private network (the WMO Global Telecommunication System (GTS)) open to other types of environmental data so that all programmes have stronger infrastructural support;

- Opportunities exploited with technological innovations as they become available.

Procedures for amending the Guide

A detailed explanation of the procedures for amending WMO Guides that are under the responsibility of the Commission for Basic Systems can be found in the appendix to the General Provisions of the *Manual on the WMO Information System* (WMO-No. 1060).

PART I. ORGANIZATION AND RESPONSIBILITIES

1.1 ORGANIZATION OF WIS

WMO Members implement and operate WIS using existing centres with some additional or modified capabilities. Centres participating in WIS are categorized as follows:

- Global Information System Centres (GISCs);
- Data Collection or Production Centres (DCPCs);
- National Centres (NCs).

See the *Manual on WIS*, Part III, for a description of the functions of the three types of WIS centre.

1.2 COMPLIANCE WITH REQUIRED WIS FUNCTIONS

As required by the *Technical Regulations* (WMO-No. 49), Volume I, Part II, and the *Manual on WIS*, Part I and Part III, WIS centres shall comply with required WIS functions. This Guide contains additional guidance on practices, procedures and specifications for WIS functions, supplementing the standard and recommended practices, procedures and specifications set out in the *Manual on WIS*.

1.3 INTERACTION AMONG WIS CENTRES

As required by the *Manual on WIS*, 1.3, GISCs shall connect to each other through the WIS Core Network. Data, products and metadata shall flow to a GISC from DCPCs and from NCs within its area of responsibility. An illustration of likely interaction among WIS centres is provided in Figure 1 (below).

Note: Named centres are illustrative examples and do not amount to a complete list of likely WIS centres.

1.4 IMPLEMENTATION OF WIS

As required by the *Manual on WIS*, 1.4, WIS is implemented in two parallel parts: continued evolution of the GTS, and extension of WMO services through discovery, access and retrieval (DAR) facilities, as well as flexible timely delivery.

1.5 DISCOVERY, ACCESS AND RETRIEVAL FUNCTION

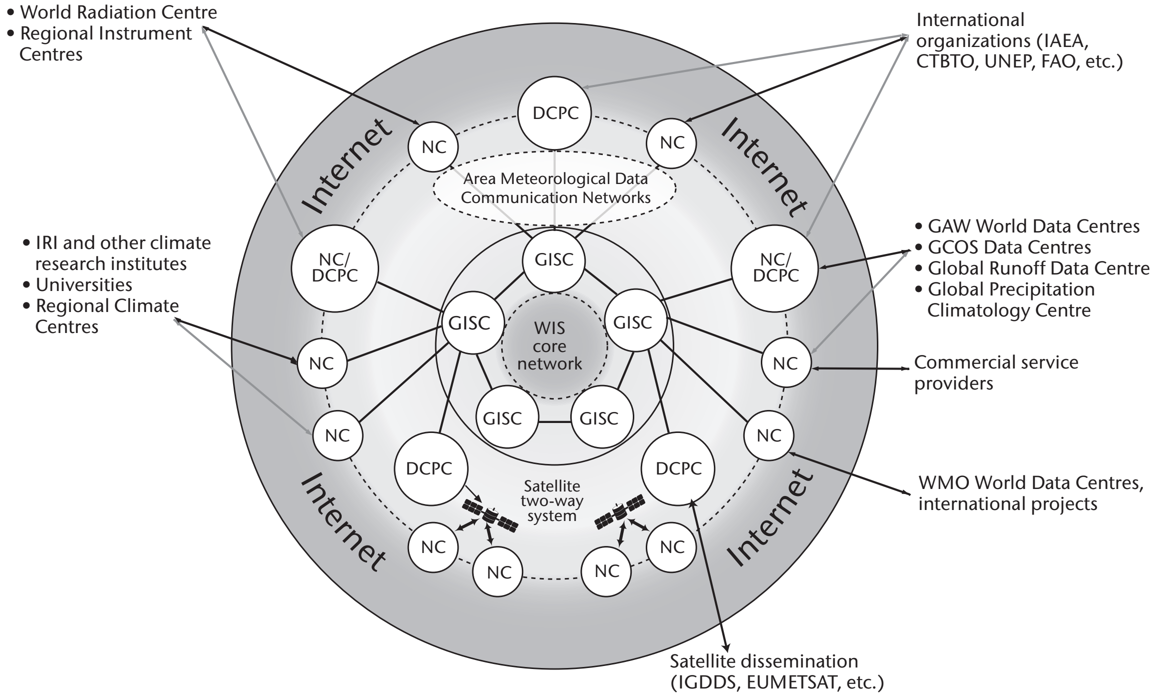
1.5.1 As required by the *Technical Regulations* (WMO-No. 49), Volume I, Part II, and the *Manual on WIS*, 1.5, WIS is based on metadata catalogues describing data and products available across WMO, plus metadata describing dissemination and access options. The DAR function of WIS is the primary realization of the WIS comprehensive catalogue, maintained collaboratively by all WIS centres.

1.5.2 A typical user of WIS DAR should find available data and products using a web browser or other Internet tool. The searcher should be able to discover available data and products either by browsing the catalogue or by searching it, using discovery concepts such as subject keywords, geographic extent or temporal range.

1.5.3 A typical user of WIS DAR should first receive a list of relevant items with associated metadata such as originator, data type, generation date and use constraints. Once the desired data or products have been identified, a user may request immediate retrieval (“pull”) or subscription for recurring delivery (“push”) if locally available, or be referred to another centre holding the item. The WIS centre having the item should then facilitate delivery through any of a broad range of online and offline transmission options. In the case of a subscription, the WIS centre should maintain further information to support recurring delivery.

1.6 ROBUSTNESS AND RELIABILITY OF COMPONENTS

As required by the *Manual on WIS*, 1.6, highly robust and reliable WIS components are essential to the operation of WIS. Indicators of performance are evaluated in the designation procedure for WIS centres to include assurance that data content flowing via WIS network technologies fully satisfies requirements for security, authenticity and reliability. Some specifications of service levels are identified within the *Manual on WIS* and this *Guide to WIS*, but further specifications can be anticipated.


• World Radiation Centre
• Regional Instrument Centres
International organizations (IAEA, CTBTO, UNEP, FAO, etc.)
DCPC
NC
NC
Internet
Internet
Area Meteorological Data Communication Networks
• IRI and other climate research institutes
• Universities
• Regional Climate Centres
NC/ DCPC
GISC
NC/ DCPC
• GAW World Data Centres
• GCOS Data Centres
• Global Runoff Data Centre
• Global Precipitation Climatology Centre
GISC
WIS core network
GISC
NC
NC
Commercial service providers
GISC
GISC
NC
NC
DCPC
DCPC
WMO World Data Centres, international projects
Satellite two-way system
Internet
Internet
NC
NC
NC
NC
Satellite dissemination (IGDDS, EUMETSAT, etc.)

Key:

CTBTO	= Comprehensive Nuclear-Test-Ban Treaty Organization	GISC	= Global Information System Centre
DCPC	= Data Collection or Production Centre	IAEA	= International Atomic Energy Agency
EUMETSAT	= European Organization for the Exploitation of Meteorological Satellites	IGDDS	= Integrated Global Data Dissemination Service
		IRI	= International Research Institute for Climate and Society
FAO	= Food and Agriculture Organization of the United Nations	NC	= National Centre
		UNEP	= United Nations Environment Programme
GAW	= Global Atmosphere Watch	⟷	= Real-time “push”
GCOS	= Global Climate Observing System	⟷	= On-demand “pull”

Figure 1. Types of WIS centres and typical interactions

1.7 COLLECTION AND DISSEMINATION SERVICES

1.7.1 See *Manual on WIS*, Part I, 1.7 for standard and recommended practices, procedures and specifications on this topic.

1.7.2 With regard to satellite-based data and products, the WMO Integrated Global Data Dissemination Service (IGDDS) addresses: user requirements; data concentration; interregional data exchange; data dissemination; data discovery; data access on request; data delivery to authorized users; and data management, including interoperable catalogue, quality of service monitoring and user support.

1.7.3 In addition to satellite-based data and products, IGDDS should distribute a basic subset of the information intended for global exchange.

1.7.4 The Integrated Global Data Dissemination Service calls for regional dissemination components linked in a global network for interregional data exchange. Each regional component should include a DCPC and should ensure routine dissemination by various means, including a satellite-based Digital Video Broadcast service covering its region.

1.7.5 Guidance on the use of the direct broadcast network (DBNet) for near-real-time relay of low Earth orbit satellite data is provided in the *Guide to the Direct Broadcast Network for Near-real-time Relay of Low Earth Orbit Satellite Data* (WMO No. 1185), which is an attachment to this Guide.

1.7.6 Guidance on the use of satellite telecommunication systems is provided in *Satellite Data Telecommunication Handbook* (WMO-No. 1223); this is an attachment to the present Guide.

1.8 COMPETENCIES OF PERSONNEL

1.8.1 The *Manual on WIS*, Part I, 1.8, recommends that Members operating WIS centres ensure that their centres have access to an adequate number of staff who have the required level of the WIS competencies defined in the *Technical Regulations* (WMO-No. 49), Volume I, Part V, and in the *Manual on WIS*, Appendix E.

1.8.2 WMO Information System centres need access to generic Information Technology and management competencies. Many training and development resources for these competencies are available from government or commercial sources, from libraries and the Internet.

1.8.3 WMO Information System centres also need access to competencies that are specific to the WIS. Guidance on how these competencies may be assessed and developed is provided in Appendix A to this Guide.

PART II. DESIGNATION PROCEDURES FOR WIS CENTRES

2.1 GENERAL

Designation procedures for WIS centres are defined in the *Manual on WIS*, Part II. The Commission for Basic Systems (CBS) reviews relevant aspects of the *Manual on WIS* to ensure alignment of WIS user requirements, the WIS functional architecture and WIS compliance specifications. The Commission for Basic Systems is also developing monitoring procedures to complement the designation procedures of WIS and to ensure ongoing compliance of WIS centres with the agreed standards and practices.

2.2 PROCEDURE FOR A GLOBAL INFORMATION SYSTEM CENTRE

The procedure for designating a GISC is given in the *Manual on WIS*, Part II, 2.2, in keeping with *Technical Regulations* (WMO-No. 49), Volume I, Part II. During the initial phase of WIS centre designation, CBS analyses GISC service offers and formulates a recommendation for designation.

2.3 PROCEDURE FOR A DATA COLLECTION OR PRODUCTION CENTRE

The procedure for designating a DCPC is given in the *Manual on WIS*, Part II, 2.3, in keeping with *Technical Regulations* (WMO-No. 49), Volume I, Part II. During the initial phase of WIS centre designation, CBS determines which centres should be integrated in WIS, analyses DCPC service offers and formulates a recommendation.

2.4 PROCEDURE FOR A NATIONAL CENTRE

2.4.1 The procedure for designating an NC is given in the *Manual on WIS*, Part II, 2.4, in keeping with *Technical Regulations* (WMO-No. 49), Volume I, Part II.

2.4.2 National Meteorological Centres are expected to be NCs. A WMO Member may also designate other centres as NCs.

2.4.3 In addition to the data and metadata requirements of an NC set out in the *Manual on WIS*, a typical NC should collect, generate or disseminate observational data and products, and provide certain observations and products intended for global dissemination or for regional or specialized distribution to other WIS centres.

2.4.4 The Study on Policy-level Implications of the Future WMO Information System (described in the *Abridged Final Report with Resolutions of the Fourteenth World Meteorological Congress* (WMO-No. 960), 3.1.2.11 of the general summary) asserts that the introduction of WIS will not result in new responsibilities or additional resource requirements for most Members. The stated expectation was that WIS would result in lower costs, especially for least-developed countries, through expanded use of commercial off-the-shelf technology and increased use of the Internet.

PART III. FUNCTIONS OF WIS

3.1 ROLES IN AND REVIEW OF WIS FUNCTIONS

3.1.1 Roles in and review of WIS functions are given in the *Manual on WIS*, Part III, 3.1.

3.1.2 Each relevant process for establishing user requirements across WMO should link to the WIS user requirement process. For instance, observing programme needs should be incorporated into WIS requirements through linkage with the Rolling Review of Requirements in the *Manual on the Global Observing System* (WMO-No. 544).

3.1.3 Current WIS user requirements are described in a technical document available at http://wis.wmo.int/WIS-RRR.

3.2 LIST OF WIS FUNCTIONS

The WMO Information System centres collectively support the major WIS functions as described in the *Manual on WIS*, Part III, 3.2. The required standard interfaces to these functions are described in the *Manual on WIS*, Part IV.

3.3 FUNCTIONAL ARCHITECTURE OF WIS

The functional architecture of WIS is provided as supplementary guidance for WIS centres in a technical document available at http://wis.wmo.int/WIS-FuncArch. As shown in that document, the following list provides one possible method for dividing the required major WIS functions into more detailed functions.

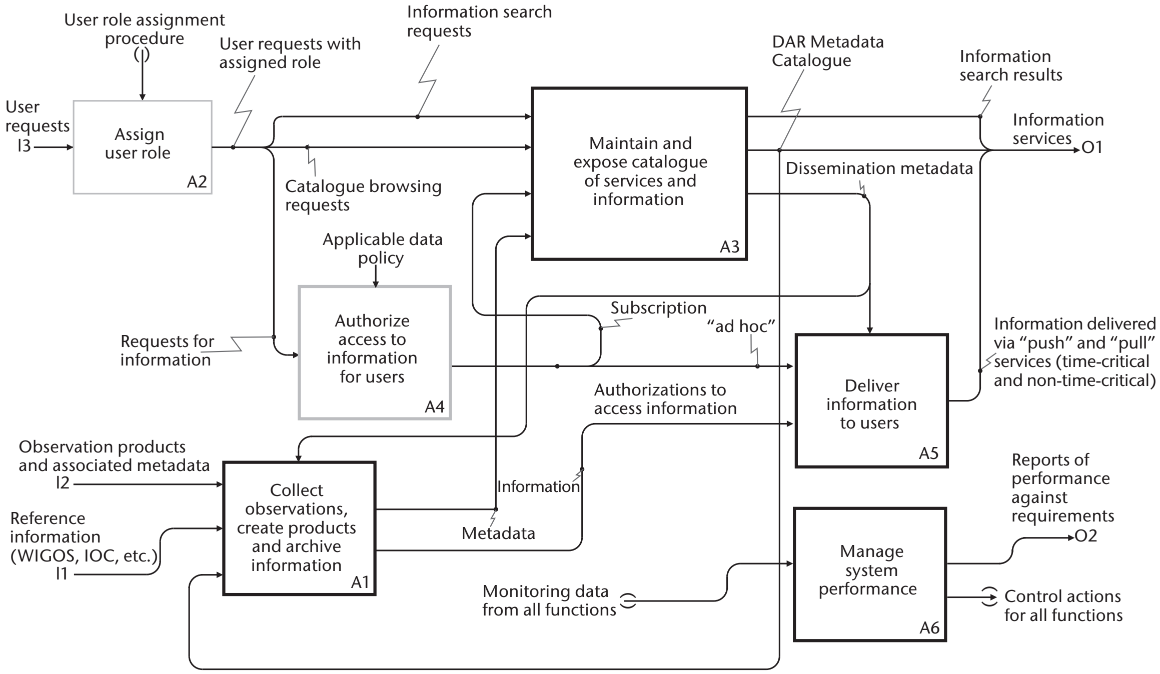
A1	Collect observations, generate products, create metadata and archive information
A11	Collect, generate and archive national information and create metadata
A111	Collect national observations
A112	Check meteorological content of products and observations
A113	Archive
A114	Generate national products
A115	Generate metadata
A116	Unpack information
A117	Verify correct telecommunication attributes of information
A12	Collect, generate and archive regional, programme-related and specialized information, and create metadata
A121	Collect regional, specialized and programme-related observations
A122	Check meteorological content of observations
A123	Archive
A124	Generate regional, specialized and programme-related products
A125	Generate metadata
A126	Unpack information

A127	Verify correct telecommunication attributes of information
A13	Collect and cache global information
A131	Unpack information
A132	Associate information with DAR metadata
A133	Verify correct communication attributes of information
A134	Maintain and make available the cache of global information for 24 hours
A2	Assign user role
A3	Maintain and expose catalogue of services and information
A31	Search DAR Metadata Catalogue
A32	Maintain and expose consolidated DAR Metadata Catalogue
A33	Maintain dissemination metadata catalogue in accordance with authorized subscriptions
A4	Authorize access to information for users
A5	Deliver information to users (internal and external)
A51	Schedule and control activities
A511	Derive time-driven (synchronous) activity schedule and list of event-driven (asynchronous) activities
A512	Monitor events
A513	Resolve any activity scheduling conflicts, reflecting relative service priorities
A52	Package information for delivery
A53	Deliver information
A6	Manage system performance
A61	Non-real-time performance monitoring
A611	Analyse traffic trends
A612	Analyse performance against requirements and service-level agreements
A62	Real-time performance monitoring
A621	Real-time monitoring of telecommunication network
A622	Real-time monitoring of the application content

3.4 DATA FLOW AMONG WIS FUNCTIONS

3.4.1 The functional architecture of WIS (see 3.3 above) models data flow among required WIS functions and illustrative subordinate functions. The model uses Integration Definition for Function Modelling (IDEF0), a data-flow diagramming technique that illustrates relationships between system components, at levels ranging from general processes to specific technology interfaces.

3.4.2 Figure 2 presents an IDEF0 functional decomposition of the major WIS functions, labelled A1 to A6. Data flows are inherited between levels of the diagrams and are labelled as I1, I2, I3 for inputs and O1, O2 for outputs.


User role assignment procedure (I)
User requests with assigned role
Information search requests
DAR Metadata Catalogue
Information search results
User requests I3
Assign user role A2
Maintain and expose catalogue of services and information A3
Information services O1
Catalogue browsing requests
Dissemination metadata
Applicable data policy
Subscription
"ad hoc"
Requests for information
Authorize access to information for users A4
Information delivered via "push" and "pull" services (time-critical and non-time-critical)
Authorizations to access information
Deliver information to users A5
Observation products and associated metadata I2
Reference information (WIGOS, IOC, etc.) I1
Collect observations, create products and archive information A1
Information
Metadata
Reports of performance against requirements O2
Monitoring data from all functions
Manage system performance A6
Control actions for all functions

Key:
IOC = Intergovernmental Oceanographic Commission
WIGOS = WMO Integrated Global Observing System

Figure 2. Data-flow model of the WIS functional architecture

3.5 FUNCTIONAL REQUIREMENTS OF A GISC

There are no general recommendations in addition to the statements in the *Manual on WIS*, Part III, 3.5.

3.6 FUNCTIONAL REQUIREMENTS OF A DCPC

There are no general recommendations in addition to the statements in the *Manual on WIS*, Part III, 3.6.

3.7 FUNCTIONAL REQUIREMENTS OF AN NC

There are no general recommendations in addition to the statements in the *Manual on WIS*, Part III, 3.7.

PART IV. WIS TECHNICAL SPECIFICATIONS

4.1 GENERAL

As specified in the *Manual on WIS*, Part IV, 4.1, there are 15 WIS technical specifications (WIS-TechSpecs) that should be regarded as "mandatory if applicable", i.e. the technical specification is required wherever the interface applies. A summary of the applicability of each WIS Technical Specification by type of WIS centre is given in Table 1 below. Supplementary details are provided in WMO Information System Compliance Specifications of GISC, DCPC and NC (see also *Manual on WIS*, Appendix D). Use cases associated with each WIS Technical Specification are provided in Appendix B. They describe how the interface should behave. Test cases, which are designed to check whether the interface is working properly, are provided in Appendix C.

Table 1. WIS interface technical specifications

Interface technical specification identifier	*Interface technical specification name*	*Required for:*		
		NC	*DCPC*	*GISC*
WIS-TechSpec-1	Uploading of metadata for data and products	✓	✓	✓
WIS-TechSpec-2	Uploading of data and products	✓	✓	✓
WIS-TechSpec-3	Centralization of globally distributed data			✓
WIS-TechSpec-4	Maintenance of user identification and role information	✓	✓	✓
WIS-TechSpec-5	Consolidated view of distributed identification and role information			✓
WIS-TechSpec-6	Authentication of a user		✓	✓
WIS-TechSpec-7	Authorization of a user role		✓	✓
WIS-TechSpec-8	DAR Metadata (WIS Discovery Metadata) Catalogue search and retrieval		✓	✓
WIS-TechSpec-9	Consolidated view of distributed DAR Metadata (WIS Discovery Metadata) Catalogues			✓
WIS-TechSpec-10	Downloading files via dedicated networks	✓	✓	✓
WIS-TechSpec-11	Downloading files via non-dedicated networks	✓	✓	✓
WIS-TechSpec-12	Downloading files via other methods	✓	✓	✓
WIS-TechSpec-13	Maintenance of dissemination metadata		✓	✓
WIS-TechSpec-14	Consolidated view of distributed dissemination metadata catalogues			✓
WIS-TechSpec-15	Reporting on quality of service	✓	✓	✓

4.2 WIS-TECHSPEC-1: UPLOADING OF METADATA FOR DATA AND PRODUCTS

4.2.1 Applicable standards

The following information is in addition to the standard and recommended practices, procedures and specifications given in the *Manual on WIS*, Part IV, 4.2.

4.2.2 Types of collection and dissemination service

To provide a quality of service that meets user requirements, this interface should make use of a mix of dedicated and public network services, including public or private Internet with Transmission Control Protocol/Internet Protocol (TCP/IP), which may include encryption.

4.2.3 Function interfaces

In the WIS functional architecture, this WIS technical specification acts as an interface for two functions: A1 (A11 for NCs or A12 for DCPCs), which deals with collection of data, generation of information and creation of discovery metadata, and A3 (as carried by the GISC), dealing with maintenance and exposure of a catalogue of services and information.

4.2.4 Additional notes

This interface builds on existing GTS practice, adding the particular standard format for WIS metadata about data, products and services. Centres should be aware that metadata uploaded to a GISC could take up to 24 hours to be synchronized across all GISCs. Thus, when a datum or product has to be distributed less than 24 hours after publication of its metadata, a centre must transmit the metadata directly to its principle GISC via the GTS or using a method already agreed with the GISC.

4.3 WIS-TECHSPEC-2: UPLOADING OF DATA AND PRODUCTS

4.3.1 Applicable standards

The following information is in addition to the standard and recommended practices, procedures and specifications laid out in the *Manual on WIS*, Part IV, 4.3.

4.3.2 Types of collection and dissemination service

To provide a quality of service that meets user requirements, this interface is associated with dedicated bandwidth and high reliability and should make use of the GTS. This can incorporate private Internet with TCP/IP and may include encryption. In some cases, IGDDS satellite uplinks may be employed.

4.3.3 Function interfaces

In the WIS functional architecture, this WIS technical specification acts as an interface for two functions: A1 (A11 for NCs or A12 for DCPCs), which deals with collection of data, generation of information and creation of discovery metadata, and A5, dealing with delivery of information to users.

4.3.4 Additional notes

This interface builds on existing GTS practice, supplemented with other file-transfer mechanisms such as the Internet. Although it is required that data arrive only after their associated metadata, a grace period of two minutes is allowed before the data file is regarded as erroneous.

4.4 WIS-TECHSPEC-3: CENTRALIZATION OF GLOBALLY DISTRIBUTED DATA

4.4.1 Applicable standards

The following information is in addition to the standard and recommended practices, procedures and specifications laid out in the *Manual on WIS*, Part IV, 4.4.

4.4.2 Types of collection and dissemination service

To provide a quality of service that meets user requirements, this interface is associated with dedicated bandwidth and high reliability and should make use of the GTS. This can incorporate private Internet with TCP/IP and may include encryption.

4.4.3 Function interfaces

In the WIS functional architecture, this WIS technical specification acts as an interface for function A134 – Maintain and make available the cache of global information for 24 hours.

4.4.4 Additional notes

4.4.4.1 The set of WMO data and products required to be cached for 24 hours at the GISCs is information intended for global exchange. This does not encompass all the material handled by IGDDS.

4.4.4.2 Although the cache of data and products intended for global exchange is required to be current across all GISCs to within 15 minutes, warnings must be current to within two minutes.

4.4.4.3 The cache size is expected to grow by one gigabyte per day. The cache needs to be highly accurate and the system for logical centralization needs to be affordable and robust; single points of failure and complex procedures are not acceptable.

4.5 WIS-TECHSPEC-4: MAINTENANCE OF USER IDENTIFICATION AND ROLE INFORMATION

4.5.1 Applicable standards

The following information is in addition to the standard and recommended practices, procedures and specifications laid out in the *Manual on WIS*, Part IV, 4.5.

4.5.2 Types of collection and dissemination service

To provide a quality of service that meets user requirements, this interface should make use of public network services, including Internet with TCP/IP, which may include encryption and other privacy protection for identified individuals, as required by national legislation.

4.5.3 Function interfaces

In the WIS functional architecture, this WIS technical specification acts as an interface for two functions: A2 – Assign user role, and A4 – Authorize access to information for users.

4.5.4 Additional notes

For updating the identification and role information concerning candidate or current users of WIS, WIS centres should support two kinds of maintenance facility: a file-upload facility for batch updating (adding, replacing or deleting identification and role records treated as separate files), and an online form for changing individual identification and role entries (adding, changing or deleting elements in a record, as well as whole records).

4.6 WIS-TECHSPEC-5: CONSOLIDATED VIEW OF DISTRIBUTED IDENTIFICATION AND ROLE INFORMATION

4.6.1 Applicable standards

The following information is in addition to the standard and recommended practices, procedures and specifications laid out in the *Manual on WIS*, Part IV, 4.6.

4.6.2 Types of collection and dissemination service

To provide a quality of service that meets user requirements, this interface should make use of a mix of dedicated and public network services, including public or private Internet with TCP/IP, which may include encryption and other privacy protection for identified individuals, as required by national legislation.

4.6.3 Function interfaces

In the WIS functional architecture, this WIS technical specification acts as an interface for two functions: A2 – Assign user role; and A4 – Authorize access to information for users.

4.7 WIS-TECHSPEC-6: AUTHENTICATION OF A USER

4.7.1 Applicable standards

The following information is in addition to the standard and recommended practices, procedures and specifications laid out in the *Manual on WIS*, Part IV, 4.7.

4.7.2 Types of collection and dissemination service

To provide a quality of service that meets user requirements, this interface should make use of a mix of dedicated network and public network services, including public or private Internet with TCP/IP, which may include encryption and other privacy protection for identified individuals, as required by national legislation.

4.7.3 Function interfaces

In the WIS functional architecture, this WIS technical specification acts as an interface for function A2 – Assign user role.

4.7.4 Additional notes

In a typical design for this interface, the client sends to the authentication server a request for a particular user whose identification and credentials are included in the request. The authentication server checks the consolidated identification and role information resource for WIS and responds. That response either confirms or denies that the identified user has provided sufficient credentials.

4.8 WIS-TECHSPEC-7: AUTHORIZATION OF A USER ROLE

4.8.1 Applicable standards

The following information is in addition to the standard and recommended practices, procedures and specifications laid out in the *Manual on WIS*, Part IV, 4.8.

4.8.2 Types of collection and dissemination service

To provide a quality of service that meets user requirements, within the constraints of dedicated bandwidth and service reliability levels, this interface should make use of public network services, including Internet with TCP/IP, which may include encryption.

4.8.3 Function interfaces

In the WIS functional architecture, this WIS technical specification acts as an interface for function A4 – Authorize access to information for users.

4.8.4 Additional notes

In a typical design for this interface, the client sends to the authorization server a request for a particular user whose identification is included in the request. The authorization server checks the consolidated identification and role information resource for WIS and responds. That response either contains a list of the authorized roles for the user or denies that the identified user has any authorized role.

4.9 WIS-TECHSPEC-8: DAR METADATA (WIS DISCOVERY METADATA) CATALOGUE SEARCH AND RETRIEVAL

4.9.1 Applicable standards

The following information is in addition to the standard and recommended practices, procedures and specifications laid out in the *Manual on WIS*, Part IV, 4.9.

4.9.2 Types of collection and dissemination service

To provide a quality of service that meets user requirements, within the constraints of bandwidth and service reliability levels, this interface should make use of public network services, including Internet with TCP/IP, which may include encryption.

4.9.3 Function interfaces

In the WIS functional architecture, this WIS technical specification acts as an interface for function A3 – Maintain and expose catalogue of services and information.

4.9.4 Additional notes

The procedures for designation of a GISC or DCPC require that both types of WIS centre maintain data, product and service catalogues in the WMO-agreed standard format and facilitate access to them. Network services should therefore be treated as a type of WIS product that can be discovered through the DAR Metadata Catalogue.

Note: The WIS SRU Implementers Note is available at http://wis.wmo.int/WISSRU.

4.10 WIS-TECHSPEC-9: CONSOLIDATED VIEW OF DISTRIBUTED DAR METADATA (WIS DISCOVERY METADATA) CATALOGUES

4.10.1 Applicable standards

The following information is in addition to the standard and recommended practices, procedures and specifications laid out in the *Manual on WIS*, Part IV, 4.10.

4.10.2 Types of collection and dissemination service

To provide a quality of service that meets user requirements, this interface should make use of a mix of dedicated and public network services, including public or private Internet with TCP/IP, which may include encryption.

4.10.3 Function interfaces

In the WIS functional architecture, this WIS technical specification acts as an interface for function A3 – Maintain and expose catalogue of services and information.

4.11 WIS-TECHSPEC-10: DOWNLOADING FILES VIA DEDICATED NETWORKS

4.11.1 Applicable standards

The following information is in addition to the standard and recommended practices, procedures and specifications laid out in the *Manual on WIS*, Part IV, 4.11.

4.11.2 Types of collection and dissemination service

To provide a quality of service that meets user requirements, this interface is associated with dedicated bandwidth and high reliability and should make use of GTS and IGDDS satellite broadcast. This can incorporate private Internet with TCP/IP and may include encryption.

4.11.3 Function interfaces

In the WIS functional architecture, this WIS technical specification acts as an interface for function A5 – Deliver information to users.

4.12 WIS-TECHSPEC-11: DOWNLOADING FILES VIA NON-DEDICATED NETWORKS

4.12.1 Applicable standards

The following information is in addition to the standard and recommended practices, procedures and specifications laid out in the *Manual on WIS*, Part IV, 4.12.

4.12.2 Types of collection and dissemination service

To provide a quality of service that meets user requirements, this interface should not use a non-dedicated network for operation-critical data. Otherwise, within the constraints of bandwidth and service reliability levels, this interface should make use of public network services, including Internet with TCP/IP, which may include encryption. This interface should also make use of IGDDS satellite broadcast (at radio or television frequencies).

4.12.3 Function interfaces

In the WIS functional architecture, this WIS technical specification acts as an interface for function A5 – Deliver information to users.

4.13 WIS-TECHSPEC-12: DOWNLOADING FILES VIA OTHER METHODS

4.13.1 Applicable standards

The following information is in addition to the standard and recommended practices, procedures and specifications laid out in the *Manual on WIS*, Part IV, 4.13.

4.13.2 Types of collection and dissemination service

To provide a quality of service that meets user requirements, this interface should not use a non-dedicated method for operation-critical data. Otherwise, this interface is associated with requirements for delivery using methods other than data-telecommunication networks. Delivery via voice lines and postal services in paper or digital media are also included.

4.13.3 Function interfaces

In the WIS functional architecture, this WIS technical specification acts as an interface for function A5 – Deliver information to users.

4.14 WIS-TECHSPEC-13: MAINTENANCE OF DISSEMINATION METADATA

4.14.1 Applicable standards

The following information is in addition to the standard and recommended practices, procedures and specifications laid out in the *Manual on WIS*, Part IV, 4.14.

4.14.2 Types of collection and dissemination service

To provide a quality of service that meets user requirements, this interface should make use of a mix of dedicated and public network services, including public or private Internet with TCP/IP, which may include encryption.

4.14.3 Function interfaces

In the WIS functional architecture, this WIS technical specification acts as an interface for function A3 – Maintain and expose catalogue of services and information.

4.14.4 Additional notes

4.14.4.1 For updating the dissemination metadata, WIS centres should support two kinds of maintenance facility: a file-upload facility for batch updating (adding, replacing or deleting metadata records treated as separate files), and an online form for changing individual entries (adding, changing or deleting elements in a record, as well as whole records).

4.14.4.2 Initially, the first version of DAR metadata was created from *Weather Reporting* (WMO-No. 9), Volume C1, which is a form of dissemination metadata, and other sources. Because full transition of WMO centres to the discovery and dissemination metadata will occur over some time, it must be ensured that changes are recorded in both the DAR metadata and in Volume C1.

4.15 WIS-TECHSPEC-14: CONSOLIDATED VIEW OF DISTRIBUTED DISSEMINATION METADATA CATALOGUES

4.15.1 Applicable standards

The following information is in addition to the standard and recommended practices, procedures and specifications laid out in the *Manual on WIS*, Part IV, 4.15.

4.15.2 Types of collection and dissemination service

To provide a quality of service that meets user requirements, this interface should make use of a mix of dedicated and public network services, including public or private Internet with TCP/IP, which may include encryption.

4.15.3 Function interfaces

In the WIS functional architecture, this WIS technical specification acts as an interface for function A3 – Maintain and expose catalogue of services and information.

4.16 WIS-TECHSPEC-15: REPORTING ON QUALITY OF SERVICE

4.16.1 Applicable standards

The following information is in addition to the standard and recommended practices, procedures and specifications laid out in the *Manual on WIS*, Part IV, 4.16.

4.16.2 Types of collection and dissemination service

This interface should make use of public network services, including Internet with TCP/IP, which may include encryption.

4.16.3 Function interfaces

In the WIS functional architecture, this WIS technical specification acts as an interface for function A6 – Manage system performance.

4.16.4 Additional notes

4.16.4.1 Agreements on service levels can be anticipated eventually for WIS operations. These should include data and network security, as well as performance and reliability.

4.16.4.2 Performance reports could be generated efficiently by having each WIS centre upload its reports to a single analysis site within a fixed-time window.

PART V. GUIDANCE FOR CREATING WMO CORE METADATA PROFILE IN VERSION 1.3

Note: Resolution 12 (EC-68) designated Part V as technical specifications for the purpose of managing amendments.

5.1 INTRODUCTION

5.1.1 Metadata records play a very important role in the WIS by providing the information that will allow WIS users to discover, access and retrieve products.[1] Metadata records have to adhere to standards (such as standard vocabularies and schemas) to ensure product definition homogeneity and make systems interoperable. There are a number of metadata standards that address the needs of meteorological and hydrological communities. The WIS discovery metadata standard (for dataset discovery catalogues) is called WMO Core Metadata Profile 1.3 (WCMP 1.3). It is a profile of the International Organization for Standardization (ISO) 19115:2003 metadata standard (*ISO 19115:2003 Geographic information – Metadata*), with its associated ISO 19139 XML mapping. ISO 19115 is a complex standard, thus both organizational and subject expertise may be required to create high-quality ISO 19115 metadata records that clearly describe an object in the context in which it is used.

5.1.2 This part of the Guide is intended for metadata authors and product or infrastructure specialists who create WCMP 1.3 metadata records for making their datasets discoverable within the WIS catalogue(s). It will also assist those who wish to create high-quality WIS metadata records for data that will be ingested and distributed by a GISC.

5.1.3 The WCMP templates and relevant documentation listed below should be used together with the guidance information provided in this part of the Guide, which also contains a set of recommendations to be followed in order to provide the right level and granularity of product information in the WCMP metadata records:

- WCMP 1.3 Template XML records: Template records containing placeholders (to be replaced with information related to the specific product described by the WIS discovery metadata record) are available from http://wis.wmo.int/MD-Templates. A valid example of an XML record, with field content (to be replaced) is also available there;

- WIS Wiki Page on WIS discovery metadata: http://wis.wmo.int/MD_Index;

- WCMP documentation: Part 1: http://wis.wmo.int/WCMPpart1; Part 2: http://wis.wmo.int/WCMPPart2;

- Additional guidance WCMP documentation: http://wis.wmo.int/MD_Index or http://wis.wmo.int/WIS-Manual (for a summary of changes);

- Additional examples of WCMP metadata (for particular product types): https://wis.wmo.int/MD-Examples.

5.2 WIS DISCOVERY METADATA

5.2.1 Presentation of the WMO Core Metadata Profile

5.2.1.1 The WCMP 1.3, while sometimes referred to as "discovery" metadata, is also aimed at providing catalogue users with sufficient information for them to decide on the suitability of the data and at providing access to or details on how to access the data. Some of the information

[1] Throughout Part V, the term product is used to describe a set of information that might be a product, data set or any other type of information that is considered as a single entity.

contained in a WCMP metadata record is vital for optimizing the searching functionality offered by the WIS product catalogues. In the WIS, users typically need to search one of the catalogues for discovering and accessing products.

5.2.1.2 A discovery metadata record has to contain the following information to help users understand a product: what, when, where, who and how. A summary is provided below, and details are provided in section 5.8.1.

(a) Product information:

What: This is the product content which is mainly defined by the product title and the product abstract fields, though additional fields can be used. The information in the title and abstract is very important because the Product Title and Abstract are indexed by any product catalogue and are thus searchable. In addition, the title and part of the abstract are presented to users in the search results of each WIS catalogue; so good content here can enhance users' efficiency as they follow the sequence search, view search results, and decide.

When: This is the temporal coverage of the dataset or product, and is captured in the temporal extent section of the metadata record. It is possible to describe ongoing, finite, or rolling-window datasets.

Where: This is the geospatial extent of the dataset, describing which geographical area(s) the product covers, over the Earth or atmosphere. It can be the whole Earth, a region or a specific place. In the WCMP, for geographical data, the metadata record must contain at least one bounding box with latitude and longitude coordinates, but that information can also be enhanced by using geographical identifiers for geographical regions, features (such as coastlines) and the like.

Who: The contact details of the organization responsible for the product, of the organization responsible for the metadata, and (optionally) the name of the party that should be cited when referencing the data. It is possible, but not necessary, for the same party to be responsible for both the product and metadata.

How - Data access and use: This consists of the distribution information, but also includes the data policy (the terms and conditions for accessing the product). Where possible, the distribution section provides a URL linking to a data access service. The data access service might require registration and might offer subselects or subsamples of the product. Users wishing to access information that has the WMOAdditional data policy (shown in “resourceConstraints”) must be registered with their regional GISC. Data with a WMOEssential or NoLimitation data policy can be accessed without restriction. Users wishing to set up a subscription (see Use Case B.5 in Appendix B) must register regardless of the type of information they require.

(b) Necessary technical information related to WIS: Section 5.8.2 defines the information required to have a functioning, distributed WIS infrastructure. This includes, for instance, the WIS unique identifier for each metadata record.

5.2.2 **WMO Core Metadata Profile and International Organization for Standardization standard**

The WCMP 1.3 is a customization, also called a profile, of the more generic ISO 19115 discovery metadata standard. It allows the meteorological community to better define meteorological products (terrestrial, Earth observations, numerical weather prediction model outputs). The ISO 19115 structure is detailed and complex because it was designed to accommodate a wide range of information resources with different characteristics. The WCMP, as well as providing more targeted searching, aims to remove the need to understand some of the intricacies of ISO 19115. This Guide sets out to simplify the knowledge needed by users who are starting to create WCMP 1.3 metadata records.

5.2.3 WMO Core Metadata Profile granularity and scope

5.2.3.1 One difficulty, when creating a metadata record, is to understand what level of detail of a dataset should be described in the record for a particular product. Some products of the same type are continuously produced for an extended period, such as those from a satellite mission, or as model forecast outputs. Creating a new metadata record for each individual satellite instrument measurement granule (produced every three minutes) or for each forecast run (produced three times a day) would make the content of WIS catalogues grow at an extremely fast rate, and the thousands of new metadata records would contain the same information, except for the measurement time. This would drastically hinder the ability of users to find information when searching the catalogue.

5.2.3.2 To solve that problem, the creation of one metadata record for an entire collection of similar products is generally recommended, provided that effective searching and other WIS infrastructure needs are not compromised. A collection of products that might be considered similar is a set of products where only one or two dimensions vary (such as time and geographical position) but the products still come from the same measurement instrument or station.

5.2.3.3 An example of this approach is the EUMETSAT Meteosat Second Generation (MSG) Seviri Level 1.5 dataset which includes all the Level 1.5 radiances over the entire MSG mission with a global coverage and is described by one unique metadata record. The user discovering this product collection, via the WIS portals, is redirected to a EUMETSAT service offering subsampling capacities for selecting the required time period and geographic region.

5.2.3.4 That said, it is up to the data provider to decide what constitutes a valid collection. Additional guidance on choosing the granularity criteria for collection metadata records can be found in the annex to this Part.

5.3 WIS PRODUCT CATEGORIES

Two categories of information (and corresponding transport protocols) are used in WIS catalogues:

(a) Routinely distributed information (GTS-delivered information): This is mainly, but not exclusively, traditional WMO bulletins.

  This category is governed by the set of regulations described in the *Manual on the Global Telecommunication System* (WMO-No. 386). It includes the bulletin header (abbreviated header line) which identifies a bulletin like ISMS01 AMMC, and a file naming convention.

  Metadata records for GTS bulletin datasets need to follow a set of additional rules and require an understanding of the GTS regulations. Non-bulletin files can also be distributed via the GTS.

  The most notable feature is the store-and-forward delivery mechanism for bulletins and other data on the GTS. This is the reason why there may be no URL for a bulletin – once a bulletin is delivered, it is not retained for later reference.

  Today, GISCs serve bulletins issued in the past 24 hours, but the common practice is still that a metadata record for bulletins does not include the access URL(s). Global Information System Centres do, however, add links to search results pointing to information that is in their cache.

(b) Information that is not routinely distributed (non-GTS-delivered information): This can include both data stored as files and data as services.

This category includes datasets that are described and searchable in the WIS catalogues but are served by different responsible organizations, via their own infrastructure and data access services. WCMP 1.3 metadata records for this second category have to follow a minimum set of rules to be compliant with the standard. This is a subset of the rules that apply to routinely distributed information.

Typically, these metadata records include a URL for access to the data.

This part of the Guide provides extensive support for creating the different parts of a metadata record, for both non-GTS and GTS-delivered datasets. When necessary, an additional section for creating metadata records for GTS bulletins has been added in each information category (for example, the product information abstract).

5.4 COMPLIANCE WITH ADDITIONAL METADATA STANDARDS

5.4.1 This part of the Guide provides information to help create metadata records that comply with WCMP 1.3. This profile is based on ISO 19115 which provides two profiling mechanisms:

(a) A more constrained use of ISO 19115 (either by recommending use of fewer fields, making an optional element mandatory, or constraining the expected content of a field) to suit the needs of a particular community;

(b) In addition to (a), the possibility of defining additional non-ISO 19115 fields (and field content) to be added to any record.

Examples of type (a) ISO 19115 profiles, in addition to the WCMP, include the Infrastructure for Spatial Information in the European Community (INSPIRE) Metadata Profile, the North American Profile, the Australian and New Zealand Information Council (ANZLIC) Metadata Profile and UK GEMINI. An example of (b) is the Marine Community Profile. For more information see also http://www.dcc.ac.uk/resources/metadata-standards/iso-19115.

5.4.2 Each ISO 19115 profile defines specific rules that should be met. For example, to comply with the INSPIRE metadata profile, the additional requirements to be met include the provision of one keyword from the general environmental multilingual thesaurus (GEMET), a lineage statement and a statement of conformance with European Commission Regulation (EC) No. 1205/2008.

5.4.3 The content of a WCMP 1.3 metadata record, defined according to this part of the Guide, can be extended so that the record also supports additional profiles (such as INSPIRE or ANZLIC). In such a case, the metadata author is required to implement any additional requirements specified in the corresponding profile documentation. The extended WCMP 1.3 metadata record can still be published in the WIS.

5.5 WMO CORE METADATA PROFILE – VALIDATION TOOLS

5.5.1 Metadata publishers are required to ensure that created metadata records conform to relevant technical specifications. For example, XML documents need to be well-formed, validated against the schema, and compliant with other requirements imposed by the specifications.

5.5.2 A set of ISO and WCMP validation tools can be used to ensure that a created WCMP record is correctly formatted (syntactically and semantically) and can be ingested by a GISC.

5.5.3 In most cases, a metadata author will validate a metadata record using a validation tool. That tool may be either a web service or locally installed software. Usually, metadata records to be validated may be stored either locally or at a URL accessible to the validation tool.

5.5.4 Online validation services can automatically evaluate the content of the metadata in terms of completeness, accuracy and conformance. Some validation tools, such as the one developed by the National Oceanic and Atmospheric Administration (NOAA) (http://www.ngdc.noaa.gov/docucomp/recordServices) may give a score based on different aspects, including content and quality of metadata.

5.5.5 It is recommended to test the metadata with one of the available tools. It is also always possible to seek assistance from your principal GISC.

5.5.6 Below is a list of web services and tools used to validate WCMP 1.3 and ISO 19115/19139 metadata records.

WCMP 1.3 validation services and tools:

- NOAA's WMO validation service: https://www.ngdc.noaa.gov/docucomp/validationServicesWmo;

- GeoNetwork-ANZMEST, with WCMP validation tool: https://sourceforge.net/projects/anzmest/files/bom-releases/.

  This directory contains the Australian Bureau of Meteorology releases of ANZMEST 2.10.x (based on GeoNetwork), which include the WCMP 1.3 editing and validation tool.

  For instructions on running the software and validation tool, see the WIS Wiki page on validation tools below;

- WIS Wiki page on validation tools: http://wis.wmo.int/MD-Validate.

ISO 19115/19139 validation services and tools:

- NOAA ISO validation page: https://www.ngdc.noaa.gov/docucomp/recordServices;

- GeoNetwork-ANZMEST – BOM branch: https://sourceforge.net/projects/anzmest/files/bom-releases/ (includes 19115:2006, 19115:INSPIRE).

5.6 PRINCIPLES OF METADATA MANAGEMENT IN THE WIS

5.6.1 The Global Information System Centres are responsible for the management of metadata. According to the WMO Technical Regulations, each GISC shall:

- Provide a comprehensive metadata catalogue with discovery services for all information provided by NCs or DCPCs across the WIS;

- Support the Search and Retrieve via URL (SRU) protocol;

- Ensure the synchronization of metadata among GISCs, using the Open Archives Initiative Protocol for Metadata Harvesting (OAI-PMH);

- Support user's identification and authorization, including in terms of metadata maintenance;

- Provide metadata publishing facilities using uploading/harvesting metadata publishing or online metadata editing tools to allow metadata authors to create metadata records.

How to publish metadata

- Metadata could be published at DCPC or GISC level;

- Find out which GISC you belong to (i.e. which is your principal GISC). The official reference for WIS centres (GISCs and affiliated DCPCs and NCs, and their areas of responsibility) is the *Manual on WIS*, Appendix B. The list of GISCs and related links is also available online on the WMO portal at http://wis.wmo.int/WIScentresDb. The procedure for metadata management (account creation and editing facilities) may vary from one centre to another, but will usually be via the GISC portal (at least as a first point of contact);

- Proceed to register with your principal GISC (this could be done online, depending on the capabilities and policies of the GISC) after which you will be assigned a username and a role;

- Publish your metadata via your principal GISC. In order to publish your metadata records, use the appropriate method among those allowed by the GISC (import/insert metadata or harvest metadata using OAI-PMH).

Note: For a limited number of records, it is also possible to use the online editing services of a GISC.

5.6.2 For more comprehensive information regarding the WIS and publishing metadata on the WIS, please consult the *Manual on WIS* (https://wis.wmo.int/WIS-Manual).

5.7 GENERATING METADATA RECORDS COMPLIANT WITH THE WMO CORE METADATA PROFILE

5.7.1 This part of the Guide is intended to help product specialists create WIS metadata records that are compliant with the WCMP 1.3. It provides practical guidance on key information needed in WCMP metadata creation (such as describing how and where to insert the necessary product information into a template record, and the WIS specific information required in the XML metadata record), while abstracting (as much as possible) the WCMP standard, the ISO 19115 standard and its XML mapping (ISO 19139).

5.7.2 Section 5.8 below defines a set of recommendations for adding each individual piece of information regarding a product (for example, title, abstract, party responsible for the product, access to the product).

5.7.3 Although metadata authors will not normally need to work with XML directly because the GISC provides form-based editing tools, this part of the Guide uses an approach based on an XML template. A metadata author who needs to work directly with XML should use a copy of the template XML record(s) (see section 5.1) in conjunction with this part of the Guide, especially section 5.8.

5.7.4 The template-based approach allows a person without any knowledge of ISO 19115 to create an XML WCMP metadata record populated with the key information needed to make the record easily searchable and accessible within a WIS portal.

5.7.5 The template files can also be used as the foundation for building a Web-based editing tool where the user completes a web form, and the content is used to overwrite the placeholders and create the final WCMP 1.3 compliant metadata record. Such tools are provided by the GISCs.

Template-based principle

5.7.6 The template XML files are metadata records encoded as XML. These contain placeholders, that is generic text that should be replaced with information related to the specific product described by the WIS discovery metadata record.

5.7.7 The template WCMP XML metadata records, listed in section 5.1, are WCMPv1.3_MAND-Template.xml and WCMPv1.3_OPTandMAND-Template.xml.

5.7.8 There is also a WCMPv1.3_OPTandMAND-Content.xml file, which has sample content rather than placeholders. This is a valid WCMP record, which can be loaded into any editor and then modified, or can be manually edited.

Placeholders in the two template files are all in capital letters, as in the following example:

```
ADD-ORGANISATION-NAME*M
```

is a placeholder that might appear in the XML template as:

```
<xml field name>ADD-ORGANISATION-NAME*M</xml field name>
```

As well as placeholders, the two template files contain hints and comments, formatted as follows:

```
<!--  this is a comment : use this XML block, if ….., otherwise, remove it    -->
```

5.7.9 Metadata content discussed in this part of the Guide (and for which there are placeholders) includes all mandatory WCMP content, identifiable through the suffix *M and some key content that is optional. The optional elements can be identified as follows:

(a) Highly recommended *HR

(b) Conditionally mandatory *C

(c) Likely to be needed *O

Note: Other ISO 19115 elements, while not mentioned in the WCMP 1.3 documentation, may also be useful and can be used within a WCMP record. An example might be the DataQuality section, or the SupplementalInformation field. For brevity, however, these have been omitted here.

An example of (a) is the element described in section 5.8.1.5, which, while optional, is highly recommended.

An example of (b) is the information described in section 5.8.1.6, which is mandatory only if the dataset is geospatial, or in section 5.8.1.10, which, while optional, is mandatory if the product is GTS data.

An example of (c) is the element described in section 5.8.1.7.

5.7.10 Note that many optional subsections of a WCMP record contain elements that are mandatory only if that subsection is used. These are marked with “-MW”, meaning mandatory within subsection.

An example of that is the identifier, authority and title segments, as shown in lines 53–57 in the hierarchical list of fields contained in the annex to this Part (see excerpt below), where identifier is optional ([0..n]) and, even if it is used, authority is also optional ([0..n]); however, if authority is used, then title is mandatory ([1..1]).

```
53 _ ._ ._ ._ ._ .identifier _ ._ .ISO[0..n]

54 _ ._ ._ ._ ._ ._ .MD _ Identifier

55 _ ._ ._ ._ ._ ._ ._ .authority _ ._ .ISO[0..1]

56 _ ._ ._ ._ ._ ._ ._ ._ .CI _ Citation

57 _ ._ ._ ._ ._ ._ ._ ._ ._ .title _ .char _ ._ .ISO[1..1]
```

The cardinality notation [x..y] indicates the minimum and maximum allowable times that the element may be used, within that part of the hierarchy or tree. For instance, [0..n] means that the element is optional but can be used any number of times; the notation [1..2] means that it is mandatory and may be used a maximum of two times. Refer to the annex to this Part for a hierarchical list of the main elements and their cardinality. Placeholders for WCMP mandatory content end with *M.

5.7.11 The WCMP1.3_OPTandMAND-Template.xml file contains placeholders for all mandatory and optional elements mentioned in this part of the Guide. The WCMP1.3_MAND-Template.xml file contains placeholders for all mandatory elements mentioned in this part of the Guide.

5.7.12 Where the metadata author chooses not to populate an optional field, the related XML block should be removed, as indicated in the comments in the two template files.

A metadata author can, by following placeholders in the template file and the recommendations in section 5.8, replace the different placeholders and follow `<!-- comments -->` in the template file, to create a WCMP 1.3 compliant record.

5.7.13 The two template WCMP XML metadata records (see 5.7.7 above), with only the placeholders, can be used as starting template records for automating the generation of metadata records.

5.8 NECESSARY INFORMATION TO CREATE A METADATA RECORD COMPLIANT WITH THE WMO CORE METADATA PROFILE

This section describes the information needed to build a meaningful metadata record. For each individual component, the following elements are provided:

- Template value: The template XML record's placeholder value that is to be replaced;
- Information: A summary of the type of information (from the metadata creator) that should replace the placeholder;
- Necessity: Whether the component is mandatory, conditionally mandatory, highly recommended or optional, within WCMP 1.3;
- XPath: Its location within the WCMP XML metadata record;
- An example of XML for that component, with content instead of placeholders.

The metadata creator should, when reading the documentation, open the relevant metadata template record and find the placeholder(s) to be replaced by the relevant product information.

For each component, this part of the Guide describes what is generally required for a product, followed, where relevant, by details of what is required in a WCMP record for GTS bulletin-specific metadata.

5.8.1 Product information

5.8.1.1 *Product title*

Product title	
Template value:	ADD-PRODUCT-TITLE*M, ADD-ALTERNATE-TITLE*O
Information:	Product name
Necessity:	Mandatory for WCMP 1.3
Category:	Product information
XPath:	*/gmd:MD_Metadata/gmd:identificationInfo/*/gmd:citation/*/gmd:title/*/text()* (line 45 in annex)

The product title and the product abstract are the two most relevant elements in the WCMP metadata record, in the context of WIS metadata catalogues, as they appear in search results and on the product description page. They assist users searching for relevant products and should, therefore, focus on the product's key characteristics.

The title should be as specific about the product as possible. If the product contains only one parameter, for instance, this can be stated in the title. However, if the product contains many parameters, the title should be more general and the parameters should be listed elsewhere in the metadata record (the abstract and/or the keywords). The title of a satellite product containing one main data parameter will typically describe that parameter and from which instrument or instrument type it originates, for instance, “AMSR-2 Sea Surface Temperature” or “SLSTR L1B radiances and brightness temperatures”.

Below is an example:

```
<gmd:identificationInfo>
   <gmd:MD _ DataIdentification>
      <gmd:citation>
         <gmd:CI _ Citation>
            <gmd:title>
               <gco:CharacterString>AMSR-2 Sea Surface Temperature</gco:CharacterString>
            </gmd:title>
            <gmd:alternateTitle>
               <gco:CharacterString>
               AMSR-2 Sea Surface Temperature SST
               </gco:CharacterString>
            </gmd:alternateTitle>
            . . . . . .
         </gmd:CI _ Citation>
      </gmd:citation>
      . . .. .
   </gmd:MD _ DataIdentification>
</gmd:identificationInfo>
```

Title for GTS bulletins

The title for a GTS bulletin should also aim to be specific about the product, describing as much as possible the type of observation and including the bulletin code or identifier and original distributor (for example, EREH RSMC Erehwon).

For instance:

```
<gmd:identificationInfo>
    <gmd:MD _ DataIdentification>
      <gmd:citation>
        <gmd:CI _ Citation>
```

```
          <gmd:title>
            <gco:CharacterString>Sea level observations data [SZPS01] for the South
Pacific area. CREX encoded. Every 3 minutes or as required (available from AMMC).
</gco:CharacterString>
          </gmd:title> …
```

5.8.1.2 ***Product abstract***

Product abstract	
Template value:	ADD-PRODUCT-ABSTRACT*M
Information:	Abstract describing the product
Necessity:	Mandatory for WCMP 1.3
Category:	Product information
XPath:	*/gmd:MD_Metadata/gmd:identificationInfo/*/gmd:abstract/*/text()*

The product abstract is important in the context of WIS catalogues, as it is part of the product information that is presented in the search results page. It should describe aspects that the data producer judges as important and that will help potential users understand the key characteristics and nature of the product, thus enabling them to quickly assess the suitability of that product for their needs.

In order to have a more coherent and homogeneous set of product descriptions on the WIS, it is recommended to use the structure of abstract described below. Product abstracts that have a similar structure will help users who are comparing related and different data products.

The product abstract should complement the title by more accurately explaining the content of the product, and should provide further detail, where appropriate, describing the product and in particular the source of the data (such as the instrument type or model when applicable), the coverage, the production frequency (hourly, every 3 minutes, etc.), the data processing level (near-real-time, derived, quality controlled), the available formats and the data access services when relevant.

Below are typical abstracts and titles for:

(a) A numerical weather prediction (NWP) product:

Title: Copernicus Atmosphere Service MACC-IFS near-real-time 5-day forecast of global black carbon aerosol concentration;

Abstract: This service provides pre-operational daily forecasts (up to 5 days) of global black carbon aerosol, using the IFS-LMD aerosol model. The product contains black carbon aerosol mixing ratios at 60 model levels. There are two forecasts per day, with base times of 00:00 UTC (5-day forecast) and 12:00 UTC (1-day forecast). Forecast steps are available at 3-hourly intervals and the spatial resolution is 0.75x0.75 degree. The forecast fields are generated in GRIB.

(b) A satellite observation product:

Title: IASI Atmospheric Temperature, Water Vapour and Surface Skin Temperature–Metop;

Abstract: The Atmospheric Temperature, Water Vapour and Surface Skin Temperature (TWT) product contains the vertical profiles of atmospheric temperature and humidity, with a vertical sampling at 101 pressure levels, and surface skin temperature. The vertical profiles are retrieved from the IASI sounder measurements (IASI L1C product) together with collocated microwave measurements (AMSU & MHS 1B) when available. The main objective of the Infrared Atmospheric Sounding Interferometer (IASI) is to provide high-resolution atmospheric emission spectra to derive temperature and humidity profiles with high spectral and vertical resolution and accuracy. Additionally, it is used for the determination of trace gases, as well as land and sea surface temperature, emissivity and cloud properties. The products are provided at the single IASI footprint resolution (which is about 12 km with a spatial sampling of about 25 km at Nadir). The quality and yield of the vertical profiles retrieved in cloudy instantaneous fields of view (IFOVs) are strongly related to the cloud properties in the IASI Cloud Parameter (CLP) product and the availability of collocated microwave measurements.

More examples of metadata titles and abstracts can be found in the WIS Wiki at http://wis.wmo.int/MD-Examples.

(c) GTS bulletin

Title: SMPS02 SYNOP reports (pressure, temperature and wind) – South Pacific area; available from NZKL (WELLINGTON/KELBURN) at 00, 06, 12 and 18 UTC;

Abstract: This bulletin dispatches synoptic data (pressure, temperature and wind) every 6 hours, starting at 0000 UTC. The bulletin includes reports from the following stations: 91823 (NIUE AERO AWS) and 91962 (PITCAIRN ISLAND AWS).

Data type: Surface data - Main synoptic hour - South Pacific area.

Actual data parameters sent include: pressure, pressure reduced to mean sea level, 3-hour pressure change, characteristic of pressure change (increasing or decreasing), temperature (dry-bulb and dewpoint), wind direction and wind speed.

Format: FM 12 (SYNOP - Report of surface observation from a fixed land station (see the *Manual on Codes* (WMO-No. 306)).

---- The SMPS02 TTAAii Data Designators decode as:

T1 (S): Surface data;

T2 (M): Main synoptic hour;

A1A2 (PS): South Pacific area.

(See the *Manual on the Global Telecommunication System* (WMO-No. 386), Attachment II.5.)

5.8.1.3 ***Metadata responsible party***

Metadata responsible party	
Template value:	ADD-METADATA-CONTACT-ORGANISATION-NAME*M; ADD-ADDRESS-STREET*O; ADD-CITY*O; ADD-REGION*O; ADD-POSTCODE*O; ADD-COUNTRY*O; ADD-EMAIL-ADDRESS*HR; ADD-ORGANISATION-WEBSITE*O.
Information:	Party responsible for the created metadata record
Necessity:	Mandatory for WCMP 1.3
Category:	Administrative information
XPath:	*/gmd:MD_Metadata/gmd:contact/gmd:CI_ResponsibleParty*

This element describes the contact details (address, telephone, email) of the party responsible for the metadata. For example:

```
<gmd:MD _ Metadata>
   ….. .. .. .
   <gmd:contact>
      <gmd:CI _ ResponsibleParty>
          <gmd:organisationName>
              <gco:CharacterString>EUMETSAT</gco:CharacterString>
          </gmd:organisationName>
          <gmd:contactInfo>
              <gmd:CI _ Contact>
                  <gmd:address>
                      <gmd:CI _ Address>
                          <gmd:deliveryPoint>
                              <gco:CharacterString>EUMETSAT Allee 1</gco:CharacterString>
                          </gmd:deliveryPoint>
                          <gmd:city>
                              <gco:CharacterString>Darmstadt</gco:CharacterString>
                          </gmd:city>
                          <gmd:administrativeArea>
                              <gco:CharacterString>Hessen</gco:CharacterString>
                          </gmd:administrativeArea>
                          <gmd:postalCode>
                              <gco:CharacterString>64295</gco:CharacterString>
                          </gmd:postalCode>
                          <gmd:country>
                              <gco:CharacterString>Germany</gco:CharacterString>
                          </gmd:country>
                          <gmd:electronicMailAddress>
                              <gco:CharacterString>ops@eumetsat.int</gco:CharacterString>
                          </gmd:electronicMailAddress>
                      </gmd:CI _ Address>
                  </gmd:address>
                  <gmd:onlineResource>
                      <gmd:CI _ OnlineResource>
                          <gmd:linkage>
                              <gmd:URL>http://www.eumetsat.int</gmd:URL>
                          </gmd:linkage>
                      </gmd:CI _ OnlineResource>
                  </gmd:onlineResource>
              </gmd:CI _ Contact>
          </gmd:contactInfo>
          <gmd:role>
              <gmd:CI _ RoleCode codeList="http://standards.iso.org/ittf/
PubliclyAvailableStandards/ISO _ 19139 _ Schemas/resources/Codelist/gmxCodelists.xml#MD
_ ScopeCode" codeListValue="pointOfContact">pointOfContact</gmd:CI _ RoleCode>
          </gmd:role>
      </gmd:CI _ ResponsibleParty>
  </gmd:contact>
```

5.8.1.4 ***Product responsible party***

Product responsible party	
Template value:	ADD-PRODUCT-RESPONSIBLE-PARTY-ORGANISATION-SHORTNAME*M, ADD-PRODUCT-RESPONSIBLE-PARTY-EMAIL*HR
Information:	Organization responsible for the product described in the metadata record
Necessity:	Mandatory for WCMP 1.3
Category:	Product information
XPath:	*/gmd:MD_Metadata/gmd:identificationInfo/*/gmd:pointOfContact/gmd:CI_ResponsibleParty*

This element contains the contact details of the organization responsible for the product. At least a name and an e-mail address are required, and the role should be “pointOfContact”.

```
<gmd:MD _ Metadata>
   …..  ..  ..  .
 <gmd:identificationInfo>
   <gmd:MD _ DataIdentification>
      <gmd:citation>
```

```
         .. .. .. .. .
       </gmd:citation>
       .. . . . . . . .
       <gmd:pointOfContact>
        <gmd:CI _ ResponsibleParty>
           <gmd:organisationName>
                <gco:CharacterString>EUMETSAT</gco:CharacterString>
           </gmd:organisationName>
           <gmd:contactInfo>
                <gmd:CI _ Contact>
                    <gmd:address>
                        <gmd:CI _ Address>
                            <gmd:country>
                                <gco:CharacterString>Germany</gco:CharacterString>
                            </gmd:country>
                            <gmd:electronicMailAddress>
                                <gco:CharacterString>ops@eumetsat.int</gco:CharacterString>
                            </gmd:electronicMailAddress>
                        </gmd:CI _ Address>
                    </gmd:address>
                    <gmd:onlineResource>
                        <gmd:CI _ OnlineResource>
                            <gmd:linkage>
                                <gmd:URL>http://www.eumetsat.int</gmd:URL>
                            </gmd:linkage>
                        </gmd:CI _ OnlineResource>
                    </gmd:onlineResource>
                </gmd:CI _ Contact>
           </gmd:contactInfo>
           <gmd:role>
                <gmd:CI _ RoleCode codeList="http://standards.iso.org/ittf/
PubliclyAvailableStandards/ISO _ 19139 _ Schemas/
resources/Codelist/gmxCodelists.xml#MD _ ScopeCode" codeListValue="pointOfContact">
pointOfContact</gmd:CI _ RoleCode>
           </gmd:role>
         </gmd:CI _ ResponsibleParty>
     </gmd:pointOfContact>
```

5.8.1.5 *Temporal extent*

Product temporal information	
Template value:	ADD-TEMPORAL-INFORMATION*HR, ADD-TEMPORAL-INFORMATION-startDate*HR, ADD-TEMPORAL-INFORMATION-endDate*HR
Information:	Time period to which the product applies
Necessity:	Optional for WCMP 1.3
Category:	Product information
XPath:	*/gmd:MD_Metadata/gmd:identificationInfo/*/gmd:extent/*/gmd:temporalElement/*/gmd:extent/*

This element describes the period of time to which the product applies. Where the product has a clear start and end date, and where the entire set of data is available, the specific start date and end date should both contain a date or date and time. The date information is constructed as YYYY-MM-DD, while the date and time information is constructed as YYYY-MM-DDTHH:MM:SSZ (for UTC time) as in 2016-04-17T13:42:54Z. In the examples below, the start and end dates are indicated as beginPosition and endPosition.

Here are some examples of temporal extents whose meaning is described in the following paragraphs:

(a) [DateX] to [DateY] e.g.: beginPosition:2005-10-01 endPosition:2014-10-20

(b) [DateX] to [now] e.g.: beginPosition:2005-10-01 endPosition:now

(c) [Now] plus [period] e.g.: beginPosition:now endPosition:after duration:P1M (+1 month)

Where it is not possible to accurately capture the time period in the TemporalExtent (using the start date, end date and duration), record details that are as close as possible, and then explain the period in words, using the description field.

(a) [DateX] to [DateY] e.g.: beginPosition:2005-10-01 endPosition:2014-10-20

The following example shows a dataset with a known start date and a known end date:

```
<gmd:temporalElement>
  <gmd:EX _ TemporalExtent id="boundingTemporalExtent">
    <gmd:extent>
      <gml:TimePeriod gml:id="boundingTemporalExtentPeriod">
        <gml:beginPosition>2005-10-01</gml:beginPosition>
        <gml:endPosition>2014-10-20</gml:endPosition>
      </gml:TimePeriod>
    </gmd:extent>
  </gmd:EX _ TemporalExtent>
</gmd:temporalElement>
```

(b) [DateX] to [now] e.g.: beginPosition:2005-10-01 endPosition:now

It is also possible to describe an ongoing dataset with a known start date, but no known end date. In that case, the endPosition should contain the attribute “indeterminatePosition="now"”. For instance, where a dataset is from 2005-10-01 onwards, it would be encoded as follows:

```
<gmd:temporalElement>
  <gmd:EX _ TemporalExtent id="temporalExtent">
    <gmd:extent>
      <gml:TimePeriod gml:id="boundingTemporalExtentPeriod">
        <gml:beginPosition>2005-10-01</gml:beginPosition>
        <gml:endPosition indeterminatePosition="now"/>
      </gml:TimePeriod>
    </gmd:extent>
  </gmd:EX _ TemporalExtent>
</gmd:temporalElement>
```

The EX_TemporalExtent options for a TimePeriod hence include beginPosition, endPosition and duration, e.g.:

```
<gml:beginPosition> ..   …  …</gml:beginPosition>

<gml:endPosition> ..   …  …</gml:endPosition>

<gml:duration> ..   …  …</gml:duration>
```

For a TimePeriod, the begin and end positions must always be included whereas duration is optional.

The encoding of duration [(- or +) PnYnMnDTnhnmns] allows the expression of time intervals such as: a number of years (nY), and/or months (nM), and/or days (nD), or hours (nh), or minutes (nm), or seconds (ns), where "n" represents a number.

For example, a duration of 4 hours is expressed as P0Y0M0DT4h0m0s or PT4h.

Note that duration can be expressed using either the long form (e.g.: P0Y5M0DT0h0m0s) or the short form, but the latter must include "T" for intervals of hours, minutes or seconds (e.g.: P5M is 5 months, PT5m is 5 minutes).

For more information on encoding of duration, see the Durations segment at https://en.wikipedia.org/wiki/ISO_8601;

(c) [Now] plus [period] e.g.: beginPosition:now endPosition:after duration:P0Y0M7DT0h0m0s (+7 days)

For a dataset that is ongoing (that is, new data are continuously produced) but for which only the latest file is available (that is, data is only ever available for a rolling window of time), the TemporalExtent should reflect the period covered by the available data, in this case, the period covered by the latest file.

For instance, where only the latest file is ever available, and the latest file is a forecast for the next 7 days, it would be encoded as follows:

```
<gmd:temporalElement>
   <gmd:EX _ TemporalExtent>
      <gmd:extent>
         <gml:TimePeriod>
            <gml:description>Next 7 days only</gml:description>
            <gml:beginPosition indeterminatePosition="now"/>
            <gml:endPosition indeterminatePosition="after"/>
            <gml:duration>P7D</gml:duration>
         </gml:TimePeriod>
      </gmd:extent>
   </gmd:EX _ TemporalExtent>
</gmd:temporalElement>
```

5.8.1.6 *Geographical information*

Geographical information	
Template value:	(ADD-GEOSPATIAL-INFORMATION*C), ADD-BBOX-VALUE-WEST*M-MW, ADD-BBOX-VALUE-EAST*M-MW, ADD-BBOX-VALUE-SOUTH*M-MW, ADD-BBOX-VALUE-NORTH*M-MW
Information:	Geographical coverage of the product, as a bounding box latitude and longitude
Necessity:	Conditional. It is mandatory for WCMP 1.3, if the data is geographical
Category:	Product information
XPath:	*/gmd:MD_Metadata/gmd:identificationInfo/*/gmd:extent/*/gmd:geographicElement/gmd:EX_GeographicBoundingBox/*/*/text() [having 4 elements]*

The geographical area covered by the product is described as a bounding box with latitude and longitude in decimal degrees.

The following example shows the XML for bounding box information of a dataset:

```
<gmd:geographicElement>
   <gmd:EX _ GeographicBoundingBox id="boundingGeographicBoundingBox">
      <gmd:westBoundLongitude>
         <gco:Decimal>-180</gco:Decimal>
      </gmd:westBoundLongitude>
      <gmd:eastBoundLongitude>
         <gco:Decimal>180</gco:Decimal>
      </gmd:eastBoundLongitude>
      <gmd:southBoundLatitude>
         <gco:Decimal>-90</gco:Decimal>
      </gmd:southBoundLatitude>
      <gmd:northBoundLatitude>
         <gco:Decimal>90</gco:Decimal>
      </gmd:northBoundLatitude>
   </gmd:EX _ GeographicBoundingBox>
</gmd:geographicElement>
```

Bounding boxes that cross the 180 degree meridian can be differentiated from bounding boxes that do not, using the following rules:

- In a dataset that does not cross the 180 degree meridian, the westernmost longitude shall always be less than the easternmost longitude;

- Conversely, if a bounding box crosses the 180 degree meridian, the westernmost longitude shall be greater than the easternmost longitude.

Other constraints on geographical bounding boxes:

- Geographical points shall be designated with the northernmost and southernmost latitudes equal, and with the westernmost and easternmost longitudes equal;

- Except for a geographical point, the total longitudinal span shall be greater than zero and less than or equal to 360 degrees;

- The northernmost latitude shall always be greater than or equal to the southernmost latitude;

- Longitude and latitude shall be recorded in a coordinate reference system that has the same axes, units and prime meridian as WGS84.

5.8.1.7 ***Geographic identifier***

Geographic identifier	
Template value:	(ADD-GEOGRAPHIC-IDENTIFIER INFORMATION*O), ADD-GEOGRAPHIC-IDENTIFIER-THESAURUS-NAME*O, ADD-GEOGRAPHIC-IDENTIFIER-CODE*C-MW
Information:	Geographic identifier indicating the zone covered on earth by the product
Necessity:	Optional
Category:	Product information
XPath:	*/gmd:MD_Metadata/gmd:identificationInfo/*/gmd:extent/*/gmd:geographicElement/*/ gmd:geographicIdentifier/gmd:MD_Identifier/code/*/text()*

The optional geographic identifier indicates the area covered by the product. It can be used when the identifier is a well-known name (within a targeted user community), a codified acronym for an area (such as a region), or a feature (such as a water storage or coastline section). If the geographicIdentifier block is used, a code must be provided.

The geographicIdentifier can be expressed in two ways:

(a) With just the geographicIdentifier code and a link to the related codelist (authority):

```
<gmd:extent>
   <gmd:EX _ Extent id="geographicExtent">
      <gmd:geographicElement>
         <gmd:EX _ GeographicDescription id="SouthAustralia _ _ allGensRegister">
            <gmd:geographicIdentifier>
               <gmd:MD _ Identifier>
                  <gmd:code>
                     <gco:CharacterString>
                           South Australia (SA)
                            (http://find.ga.gov.au/FIND/profileinfo/anzlic-allgens.xml#SA)
                     </gco:CharacterString>
                  </gmd:code>
               </gmd:MD _ Identifier>
            </gmd:geographicIdentifier>
         </gmd:EX _ GeographicDescription>
      </gmd:geographicElement>
   </gmd:EX _ Extent>
</gmd:extent>
```

(b) With the geographicIdentifier code, as well as a link to the related codelist, using a CI_Citation group:

```
<gmd:extent>
   <gmd:EX _ Extent id="geographicExtent">
     <gmd:geographicElement>
       <gmd:EX _ GeographicDescription id="SouthAustralia _ _ allGensRegister">
          <gmd:geographicIdentifier>
             <gmd:MD _ Identifier>
                <gmd:authority>
                   <gmd:CI _ Citation>
                      <gmd:title>
                         <gco:CharacterString>
                         ANZLIC Geographic Extent Name Register
                         (http://find.ga.gov.au/FIND/profileinfo/anzlic-allgens.xml)
                         </gco:CharacterString>
                      </gmd:title>
                      <gmd:alternateTitle>
                         <gco:CharacterString>
                         ANZLIC AllGens / subcategory: anzlic-sla _ 2001edition
                         </gco:CharacterString>
                      </gmd:alternateTitle>
                      <gmd:date>
                         <gmd:CI _ Date>
                            <gmd:date>
                               <gco:Date>2011-10-25</gco:Date>
                            </gmd:date>
                            <gmd:dateType>
                               <gmd:CI _ DateTypeCode
codeList="http://www.isotc211.org/2005/resources/Codelist/gmxCodelists.xml#CI
_ DateTypeCode" codeListValue="revision">revision</gmd:CI _ DateTypeCode>
```

```
                            </gmd:dateType>
                         </gmd:CI _ Date>
                      </gmd:date>
                   </gmd:CI _ Citation>
                </gmd:authority>
                <gmd:code>
                   <gco:CharacterString>South Australia (SA)
                          (http://find.ga.gov.au/FIND/profileinfo/anzlic-allgens.xml#SA)
                   </gco:CharacterString>
                </gmd:code>
             </gmd:MD _ Identifier>
          </gmd:geographicIdentifier>
       </gmd:EX _ GeographicDescription>
    </gmd:geographicElement>
  </gmd:EX _ Extent>
</gmd:extent>
```

Station identifiers for GTS bulletins

In WIS metadata records, references to stations for a GTS bulletin should point to WIGOS station identifiers (available through the Observing Systems Capability Analysis and Review tool (OSCAR)/Surface) and should be provided as keywords (see section 5.8.1.8.3).

5.8.1.8 ***Descriptive keywords***

Descriptive keywords are additional "controlled" terms which further classify (thus increasing searching accuracy for) the products. The following general rules apply for keywords in a WCMP record:

- Terms from the same keyword thesaurus/codelist and of the same KeywordTypeCode shall be grouped into a single instance of the <gmd:descriptiveKeywords> class;
- All WCMP metadata records shall have at least one WMO_CategoryCode keyword, and the related KeywordTypeCode will be "theme";
- All WCMP records for GTS data must contain a keyword from the WMO_DistributionScopeCode codelist and must be accompanied by the KeywordTypeCode "dataCentre";
- A WCMP metadata record describing data for global exchange via the WIS shall indicate the scope of distribution using the keyword "GlobalExchange" of type "dataCentre";
- Where data concern WMO stations, the related WIGOS station identifiers should be recorded as keywords(see 5.8.1.8.3);
- Any data parameter term added as a keyword should be accompanied by the KeywordTypeCode "dataParam".

5.8.1.8.1 WMO_CategoryCode keyword

WMO_CategoryCode keyword	
Template value:	WCMP-WMO-CATEGORY-CODE*M
Information:	One or more WMO_CategoryCode keywords for classifying the product
Necessity:	Mandatory for WCMP 1.3
Category:	Product information

WMO_CategoryCode keyword	
XPath:	*/gmd:MD_Metadata/gmd:identificationInfo/*/gmd:descriptiveKeywords/*/gmd:keyword/*/text()* */gmd:MD_Metadata/gmd:identificationInfo/*/gmd:descriptiveKeywords/*/gmd:type/*/@codeListValue="theme"* */gmd:MD_Metadata/gmd:identificationInfo/*/gmd:descriptiveKeywords/*/gmd:thesaurusName/*/gmd:title/*/text()="WMO_CategoryCode"*

Any WCMP metadata record shall have at least one WMO_CategoryCode keyword, and the related KeywordTypeCode will be "theme".

The WMO_CategoryCode list of terms is occasionally revised. For the latest list of terms, see: http://wis.wmo.int/2012/codelists/WMOCodeLists.xml#WMO_CategoryCode.

At the time of writing, the WMO_CategoryCode list of terms includes:

WMO_CategoryCode	*Term*
WMO_CategoryCode_weatherObservations	weatherObservations
WMO_CategoryCode_weatherForecasts	weatherForecasts
WMO_CategoryCode_meteorology	Meteorology
WMO_CategoryCode_hydrology	Hydrology
WMO_CategoryCode_climatology	Climatology
WMO_CategoryCode_landMeteorologyClimate	landMeteorologyClimate
WMO_CategoryCode_synopticMeteorology	synopticMeteorology
WMO_CategoryCode_marineMeteorology	marineMeteorology
WMO_CategoryCode_agriculturalMeteorology	agriculturalMeteorology
WMO_CategoryCode_aerology	Aerology
WMO_CategoryCode_marineAerology	marineAerology
WMO_CategoryCode_oceanography	Oceanography
WMO_CategoryCode_landHydrology	landHydrology
WMO_CategoryCode_rocketSounding	rocketSounding
WMO_CategoryCode_pollution	Pollution
WMO_CategoryCode_waterPollution	waterPollution
WMO_CategoryCode_landWaterPollution	landWaterPollution
WMO_CategoryCode_seaPollution	seaPollution
WMO_CategoryCode_landPollution	landPollution
WMO_CategoryCode_airPollution	airPollution
WMO_CategoryCode_glaciology	Glaciology
WMO_CategoryCode_actinometry	Actinometry
WMO_CategoryCode_satelliteObservation	satelliteObservation
WMO_CategoryCode_airplaneObservation	airplaneObservation
WMO_CategoryCode_observationPlatform	observationPlatform
WMO_CategoryCode_spaceWeather	spaceWeather
WMO_CategoryCode_atmosphericComposition	atmosphericComposition
WMO_CategoryCode_radiation	radiation

The example below, for a satellite product, uses the terms "satelliteObservation" and "meteorology" as keywords from the WMO_CategoryCode thesaurus/codelist:

```
<gmd:descriptiveKeywords>
  <gmd:MD _ Keywords>
    <gmd:keyword>
      <gco:CharacterString>satelliteObservation</gco:CharacterString>
    </gmd:keyword>
    <gmd:keyword>
      <gco:CharacterString>meteorology</gco:CharacterString>
    </gmd:keyword>
    <gmd:type>
    <MD _ KeywordTypeCode xmlns="http://www.isotc211.org/2005/gmd" codeListValue="theme"
codeList="http://standards.iso.org/ittf/PubliclyAvailableStandards/ISO _ 19139 _ Schemas/
resources/Codelist/gmxCodelists.xml#MD _ KeywordTypeCode">Theme</MD _ KeywordTypeCode>
    </gmd:type>
    <gmd:thesaurusName>
    <gmd:CI _ Citation>
          <gmd:title>
            <gco:CharacterString>WMO _ CategoryCode</gco:CharacterString>
          </gmd:title>
          <gmd:date>
            <gmd:CI _ Date>
               <gmd:date>
                  <gco:Date>2016-04-01</gco:Date>
               </gmd:date>
                <gmd:dateType>
                  <gmd:CI _ DateTypeCode codeListValue="publication" codeList="http://
standards.iso.org/ittf/PubliclyAvailableStandards/ISO _ 19139 _ Schemas/resources/Codelist/
gmxCodelists.xml#CI _ DateTypeCode"/>
               </gmd:dateType>
           </gmd:CI _ Date>
          </gmd:date>
        </gmd:CI _ Citation>
    </gmd:thesaurusName>
  </gmd:MD _ Keywords>
</gmd:descriptiveKeywords>
```

5.8.1.8.2 WMO_DistributionScopeCode keywords

WMO_DistributionScopeCode keywords	
Template value:	ADD-DISTRIBUTION-SCOPE*C
Information:	Scope of distribution of data within the WIS
Necessity:	Conditional. Mandatory for WCMP 1.3 for GTS data
Category:	Product information
XPath:	*/gmd:MD_Metadata/gmd:identificationInfo/*/gmd:descriptiveKeywords/*/gmd:keyword/*/text()* */gmd:MD_Metadata/gmd:identificationInfo/*/gmd:descriptiveKeywords/*/gmd:type/*/@codeListValue="dataCentre"* */gmd:MD_Metadata/gmd:identificationInfo/*/gmd:descriptiveKeywords/*/gmd:thesaurusName/*/gmd:title/*/text()="WMO_DistributionScopeCode"*

Any WCMP record for GTS data must contain a WMO_DistributionScopeCode keyword. The scope of distribution for data within WIS shall be expressed with a term from the WMO_DistributionScopeCode vocabulary, using the KeywordTypeCode “datacentre”. The keyword will be one of the following terms from the WMO_DistributionScopeCode vocabulary (a metadata record may not contain more than one of these keywords):

- GlobalExchange
- RegionalExchange
- OriginatingCentre.

The requirements for a WIS Discovery Metadata record describing products for global exchange via the WIS are more stringent. Such a record shall contain, in the “resourceConstraints” section, the keyword “GlobalExchange” from the WMO_DistributionScopeCode thesaurus (codelist), with KeywordTypeCode "dataCentre"; it must also include a term from both the WMO_DataLicenseCode and WMO_GTSProductCategoryCode thesauri (see section 5.8.1.10 for details).

The GTS is the part of the WIS concerned with rapid, near-real-time information exchange. The Global Information System Centres are required to retain at least 24h of information exchanged globally using the GTS.

A keyword from the WMO_DistributionScopeCode codelist is used to indicate whether the product described by a metadata record is or is not delivered via the GTS and GISCs, and, within the GTS, whether it is exchanged globally or regionally:

- Metadata marked "GlobalExchange" or "RegionalExchange" describe product delivered via the GTS. Products are transmitted from an originating NC or DCPC to the principal GISC, distributed to all (or some) GISCs, then placed on the GISC caches;

- Metadata marked "RegionalExchange" describe products that, while transmitted on the GTS, might be simply exchanged between two WMO Members (by bilateral agreement). Some examples are regional warnings or voluminous NWP products;

- The metadata marked "OriginatingCentre" indicate non-GTS products and include, for instance, products delivered to users from a DCPC.

Below is an example for globally exchanged GTS products:

```
<gmd:descriptiveKeywords>
    <gmd:MD _ Keywords>
        <gmd:keyword>
            <gco:CharacterString>GlobalExchange</gco:CharacterString>
        </gmd:keyword>
        <gmd:type>
            <gmd:MD _ KeywordTypeCode codeList="http://wis.wmo.int/2012/codelists/
WMOCodeLists.xml#MD _ KeywordTypeCode" codeListValue="dataCentre">dataCentre</gmd:MD
_ KeywordTypeCode>
        </gmd:type>
        <gmd:thesaurusName>
            <gmd:CI _ Citation>
                <gmd:title>
                    <gco:CharacterString>WMO _ DistributionScopeCode [http://wis.wmo.int/
2012/codelists/WMOCodeLists.xml]</gco:CharacterString>
                </gmd:title>
                <gmd:date>
                    <gmd:CI _ Date>
                        <gmd:date>
                            <gco:Date>2012-06-27</gco:Date>
                        </gmd:date>
                        <gmd:dateType>
                            <gmd:CI _ DateTypeCode codeList="http://standards.iso.org/ittf/
PubliclyAvailableStandards/ISO _ 19139 _ Schemas/resources/codelist/gmxCodelists.xml#CI
_ DateTypeCode" codeListValue="revision">revision</gmd:CI _ DateTypeCode>
                        </gmd:dateType>
                    </gmd:CI _ Date>
                </gmd:date>
            </gmd:CI _ Citation>
        </gmd:thesaurusName>
    </gmd:MD _ Keywords>
</gmd:descriptiveKeywords>
```

5.8.1.8.3 WIGOS Station Identifier keywords

WIGOS Station Identifier keywords	
Template value:	ADD-WIGOS-STATION-IDENTIFIER-CODE*O; ADD-WIGOS-STN-ID-CODE-AUTHORITY*O
Information:	Where a product includes data from stations that have been assigned a WIGOS station identifier, include this as a keyword.
Necessity:	Optional for WCMP 1.3
Category:	Product information
XPath:	*/gmd:MD_Metadata/gmd:identificationInfo/*/gmd:descriptiveKeywords/*/gmd:keyword/*/text()* */gmd:MD_Metadata/gmd:identificationInfo/*/gmd:descriptiveKeywords/*/gmd:type/*/@codeListValue="place"* */gmd:MD_Metadata/gmd:identificationInfo/*/gmd:descriptiveKeywords/*/gmd:thesaurusName/*/ gmd:title/*/text()="WMO WIGOS Station Identifiers"*

Whereas metadata records previously included WMO station numbers as keywords, the WIGOS Station Identifier should now be used. The related KeywordTypeCode should be “place”.

Below is an example including WIGOS station identifiers as keywords:

```
<gmd:descriptiveKeywords>
   <gmd:MD _ Keywords>
       <gmd:keyword>
         <gco:CharacterString>
          0-20000-0-94287; CAIRNS AERO [http://data.wmo.int/wigosid=0-20000-0-94287]
         </gco:CharacterString>
       </gmd:keyword>
       <gmd:keyword>
         <gco:CharacterString>
          0-20000-0-94374; ROCKHAMPTON AERO [http://data.wmo.int/wigosid=0-20000-0-94374]
         </gco:CharacterString>
       </gmd:keyword>
       <gmd:keyword>
         <gco:CharacterString>
          0-20000-0-94294; TOWNSVILLE AERO [http://data.wmo.int/wigosid=0-20000-0-94294]
         </gco:CharacterString>
       </gmd:keyword>
       <gmd:type>
          <gmd:MD _ KeywordTypeCode codeList="http://standards.iso.org/ittf/
PubliclyAvailableStandards/ISO _ 19139 _ Schemas/resources/codelist/gmxCodelists.xml#MD
_ KeywordTypeCode"  codeListValue="place"</gmd:MD _ KeywordTypeCode>
       </gmd:type>
       <gmd:thesaurusName>
          <gmd:CI _ Citation>
             <gmd:title>
                  <gco:CharacterString>WMO WIGOS Station Identifiers</gco:CharacterString>
             </gmd:title>
              <gmd:date>
                 <gmd:CI _ Date>
                    <gmd:date>
                       <gco:Date>2016-06-25</gco:Date>
                    </gmd:date>
                 <gmd:dateType>
                     <gmd:CI _ DateTypeCode codeList="http://www.isotc211.org/2005/
resources/Codelist/gmxCodelists.xml#CI _ DateTypeCode" codeListValue="revision">revision</
gmd:CI _ DateTypeCode>
                 </gmd:dateType>
              </gmd:CI _ Date>
```

```
           </gmd:date>
       </gmd:CI _ Citation>
    </gmd:thesaurusName>
  </gmd:MD _ Keywords>
</gmd:descriptiveKeywords>
```

5.8.1.8.4 Data parameters

Data parameter keywords	
Template value:	ADD-DATA-PARAMETER*O
Information:	Data parameter keywords for classifying the product
Necessity:	Optional for WCMP 1.3
Category:	Product information
XPath:	*/gmd:MD_Metadata/gmd:identificationInfo/*/gmd:descriptiveKeywords/*/gmd:keyword/*/text()* */gmd:MD_Metadata/gmd:identificationInfo/*/gmd:descriptiveKeywords/*/gmd:type/*/@codeListValue="dataParam"*

Where feasible, a list of the data parameters may be added as keywords. These should be added under a separate “descriptiveKeywords” block and should use the KeywordTypeCode “dataParam”.

Below is an example of a data parameter as a keyword:

```
<gmd:descriptiveKeywords>
   <gmd:MD _ Keywords>
      <gmd:keyword>
         <gco:CharacterString>Dewpoint temperature</gco:CharacterString>
      </gmd:keyword>
       <gmd:type>
          <gmd:MD _ KeywordTypeCode codeList="http://wis.wmo.int/2012/codelists/
WMOCodeLists#MD _ KeywordTypeCode" codeListValue="dataParam">dataParam</ gmd:MD
_ KeywordTypeCode>
       </gmd:type>
       <gmd:thesaurusName>
          <gmd:CI _ Citation>
             <gmd:title>
                <gco:CharacterString>WMO Grib2 parameter list http://codes.wmo.int/grib2/
codeflag/4.2/ </gco:CharacterString>
             </gmd:title>
              <gmd:date>
                 <gmd:CI _ Date>
                    <gmd:date>
                       <gco:Date>2016-06-25</gco:Date>
                    </gmd:date>
                 <gmd:dateType>
                    <gmd:CI _ DateTypeCode codeList="http://www.isotc211.org/2005/
resources/Codelist/gmxCodelists.xml#CI _ DateTypeCode" codeListValue="revision">revision</
gmd:CI _ DateTypeCode>
                 </gmd:dateType>
              </gmd:CI _ Date>
           </gmd:date>
       </gmd:CI _ Citation>
    </gmd:thesaurusName>
  </gmd:MD _ Keywords>
</gmd:descriptiveKeywords>
```

5.8.1.9 *Product sample visualization URL*

Product sample visualization URL	
Template value:	ADD-PRODUCT-IMAGERY-URL*O
Information:	URL to a sample data visualization
Necessity:	Optional for WCMP 1.3, but used by WIS portal to display products
Category:	Product information
XPath:	*/gmd:MD_Metadata/gmd:identificationInfo/*/gmd:graphicOverview/*/gmd:fileName/*/text()*

The addition of a link to the product visualization is suggested, when possible. The display of related linked images can make the product more attractive for end users.

Below is an example based on EUMETSAT Seviri Level 1.5:

```
<gmd:graphicOverview>
   <gmd:MD _ BrowseGraphic>
      <gmd:fileName>
         <gco:CharacterString>http://navigator.eumetsat.int:80/smartEditor/preview/msg
-level-1-5.jpg</gco:CharacterString>
      </gmd:fileName>
      <gmd:fileDescription>
         <gco:CharacterString>preview</gco:CharacterString>
      </gmd:fileDescription>
      <gmd:fileType>
         <gco:CharacterString>jpg</gco:CharacterString>
      </gmd:fileType>
   </gmd:MD _ BrowseGraphic>
</gmd:graphicOverview>
```

5.8.1.10 *Data policy information*

Data policy information	
Template value:	ADD-DATA-POLICY-CODE*C
Information:	Data usage and access limitations
Necessity:	Mandatory for WCMP 1.3, for data intended for global exchange on the GTS. Otherwise, highly recommended, since the absence of a policy can result in users assuming that there are no limitations on data use. To avoid uncertainty, where there are no limitations, use the data policy “NoLimitation”.
Category:	Product information
XPath:	*/gmd:MD_Metadata/gmd:identificationInfo/*/gmd:resourceConstraints/gmd:MD_LegalConstraints/*↘ {complex content}, including ↘*/gmd:otherConstraints/*/text()=WMO_DataLicenseCode* and ↘*/gmd:otherConstraints/*/text()=WMO_GTSProductCategoryCode*

The data policy category is used to specify the conditions under which the data products can be accessed and used. Completing the data policy section of a WCMP metadata record is dependent on the type of product, the data policy and the ways in which the product is being distributed. For those reasons, and to minimize the complexity of this section, three representative examples are discussed:

- Non-GTS product, with a policy of no constraints on use or distribution;
- Non-GTS product, with a policy applicable in the WMO context;
- GTS product intended for global exchange.

For more comprehensive information, please refer to the documentation on WCMP contained in the *Manual on WIS*.

When adding the data policy information, two different parts of the metadata record have to be filled:

- resourceConstraints, which contains the data policy information;

- Scope of distribution, using one of the following terms: “GlobalExchange”, “RegionalExchange” or “OriginatingCentre” (to be inserted as a keyword, as explained in Section 5.8.1.8.2).

Each of the three examples below shows the resourceConstraints part of the information that is to be added to the metadata record.

Within the “resourceConstraints” section, the DataLicenseCode term is added into an “otherConstraints” field and an explanation of the data policy is typically given in an additional “otherConstraints” field:

```
/gmd:MD _ Metadata/gmd:identificationInfo/*/gmd:resourceConstraints/gmd:MD
_ LegalConstraints/gmd:otherConstraints/*/text()
```

Allowable terms from the DataLicenseCode codelist include: “WMOAdditional”, “WMOEssential”, “WMOOther” or “NoLimitation”. All of these terms are defined at http://wis.wmo.int/2012/codelists/WMOCodeLists.xml#WMO_DataLicenseCode.

Example 1: Non-GTS product with a policy of no constraints on use or distribution

Publicly available datasets are those for which there are no limitations on distribution or use.

The “useLimitation” field in the “resourceConstraints” block should contain “No conditions apply”, and an “otherConstraints” field should contain the phrase “NoLimitation”.

```
<!-- Example of publicly available, unrestricted data -->
<gmd:resourceConstraints>
  <gmd:MD _ LegalConstraints>
    <!--  add useLimitation with ..No conditions apply..  -->
    <gmd:useLimitation>
      <gco:CharacterString>No conditions apply</gco:CharacterString>
    </gmd:useLimitation>
    <gmd:useConstraints>
      <!--  Restriction code have to point to WMOCodeLists.xml -->
<gmd:MD _ RestrictionCode codeList="http://standards.iso.org/ittf/
PubliclyAvailableStandards/ISO _ 19139 _ Schemas/resources/Codelist/gmxCodelists.xml#MD
_ RestrictionCode"
         codeListValue="otherRestrictions">otherRestrictions</gmd:MD _ RestrictionCode>
    </gmd:useConstraints>
    <!--  otherConstraints with ..NoLimitation..  -->
    <gmd:otherConstraints>
      <gco:CharacterString>NoLimitation</gco:CharacterString>
    </gmd:otherConstraints>
  </gmd:MD _ LegalConstraints>
</gmd:resourceConstraints>
```

In addition, the scope of distribution should ideally be stated as a keyword, and for non-GTS products it should be “OriginatingCentre”.

```
<!-- Scope of distribution for non GTS products: OriginatingCentre -->
<gmd:descriptiveKeywords>
  <gmd:MD _ Keywords>
    <gmd:keyword>
      <!--  keyword OriginatingCentre applies for DCPC Data -->
      <gco:CharacterString>OriginatingCentre</gco:CharacterString>
    </gmd:keyword>
    <gmd:type>
      <gmd:MD _ KeywordTypeCode codeList="http://wis.wmo.int/2012/codelists/WMOCodeLists
.xml#MD _ DistributionScopeCode"
           codeListValue="dataCentre">dataCentre</gmd:MD _ KeywordTypeCode>
    </gmd:type>
    <gmd:thesaurusName>
      <gmd:CI _ Citation>
        <gmd:title>
          <gco:CharacterString>WMO _ DistributionScopeCode, WMOCodelists
dictionary Version 1.3 [http://wis.wmo.int/2012/codelists/WMOCodeLists.xml#WMO
_ DistributionScopeCode]</gco:CharacterString>
        </gmd:title>
    .. .. .. etc    (see Section 5.8.1.8.2 for full details)
```

Example 2: Non-GTS product with a policy applicable in the WMO context

This example describes a product that is not distributed on the GTS and has a single data policy applicable in the WMO context. Note that policies that are applicable in the WMO context, and therefore flagged in an “otherConstraints” field with the term “WMOOther”, will be presented by the GISCs to users when they discover the data. Global Information System Centres have no obligation to show the other data policies.

A term from the WMO_DataLicenseCode codelist (available at http://wis.wmo.int/2012/codelists/WMOCodeLists.xml#WMO_DataLicenseCode) should be added to an “otherConstraints” field.

Note: The data policy term “WMOOther” can also be used for data that is delivered via the GTS.

```
<gmd:resourceConstraints>
  <gmd:MD _ LegalConstraints>
    <!--   Add useLimitation to indicate the limitations of usage for the data  -->
      <gmd:useLimitation>
        <gco:CharacterString>Disclaimer - While every effort has been made to ensure
that these data are accurate and reliable within the limits of the current state of
the art, OrganisationX cannot assume liability for any damages caused by any errors
or omissions in the data, nor as a result of the failure of the data to function on a
particular system. OrganisationX makes no warranty, expressed or implied, nor does the
fact of distribution constitute such a warranty.
        </gco:CharacterString>
      </gmd:useLimitation>
      <gmd:accessConstraints>
<gmd:MD _ RestrictionCode codeList="http://standards.iso.org/ittf/
PubliclyAvailableStandards/ISO _ 19139 _ Schemas/resources/Codelist/gmxCodelists.xml#MD
_ RestrictionCode" codeListValue="copyright">copyright</gmd:MD _ RestrictionCode>
      </gmd:accessConstraints>
      <gmd:accessConstraints>
         <gmd:MD _ RestrictionCode codeList="http://standards.iso.org/ittf/
PubliclyAvailableStandards/ISO _ 19139 _ Schemas/resources/Codelist/gmxCodelists.xml
#MD _ RestrictionCode" codeListValue="otherRestrictions">otherRestrictions</gmd:MD
_ RestrictionCode>
```

```
      </gmd:accessConstraints>
      <gmd:useConstraints>
        <gmd:MD _ RestrictionCode 
codeList="http://standards.iso.org/ittf/PubliclyAvailableStandards/ISO
_ 19139 _ Schemas/resources/Codelist/gmxCodelists.xml#MD _ RestrictionCode" 
codeListValue="copyright">copyright</gmd:MD _ RestrictionCode>
      </gmd:useConstraints>
      <gmd:useConstraints>
         <gmd:MD _ RestrictionCode 
codeList="http://standards.iso.org/ittf/PubliclyAvailableStandards/ISO
_ 19139 _ Schemas/resources/Codelist/gmxCodelists.xml#MD _ RestrictionCode" 
codeListValue="otherRestrictions">otherRestrictions</gmd:MD _ RestrictionCode>
      </gmd:useConstraints>
      <!--  Add WMOOther, to signal that the policy is applicable in the WMO Context -->
      <gmd:otherConstraints>
         <gco:CharacterString>WMOOther 
Ordnance Survey Open Data License [https://www.ordnancesurvey.co.uk/docs/licences/os
-opendata-licence.pdf]
         </gco:CharacterString>
      </gmd:otherConstraints>
   </gmd:MD _ LegalConstraints>
</gmd:resourceConstraints>
```

The scope of distribution should, ideally, be added as a keyword using the term "OriginatingCentre".

Please refer to the encoding of scope of distribution, provided under Example 1 above or in section 5.8.1.8.2.

Example 3: GTS data intended for global exchange

This example describes data distributed via the GTS and available from the cache at a GISC. For data delivered via the GTS, the data policy term to be added to the "otherConstraints" field can only be "WMOAdditional" or "WMOEssential" – both of these terms are defined at http://wis.wmo.int/2012/codelists/WMOCodeLists.xml#WMO_DataLicenseCode.

In the example below, the code used is "WMOEssential".

WMO policies for data and products (licence conditions) are defined by Resolution 40 (Cg-XII), Resolution 25 (Cg-XIII) and Resolution 60 (Cg-17). Data and products exchanged on a free and unrestricted basis are marked as "WMOEssential"; data classed as "WMOAdditional" have restrictions on commercial activities. Operational meteorological information for aviation is not included in these resolutions but is controlled by the International Civil Aviation Organization (ICAO); this information is an example of "WMOOther" data.

Only one term from the WMO_DataLicenseCode codelist may be used within a metadata record. As well as assigning one of these terms, it is expected, where the term used is "WMOOther" or "WMOAdditional", that further clarification of the licence constraints will also be provided (either directly in the metadata record or else via a URL).

For data circulating on the GTS, "WMOAdditional" is used to qualify products under the WMOAdditional data policy; "WMOEssential" is used for products made available under the WMOEssential data policy; and "WMOOther" can be used (where applicable) for other products, regardless of whether the data is being delivered via the GTS, GISC or otherwise.

Where data is for global exchange on the GTS (which is signified by the WMO_DistributionScopeCode keyword), both a WMO_DataLicenseCode and a WMO_GTSProductCategoryCode term must be provided, under "resourceConstraints". The terms from the WMO_GTSProductCategoryCode codelist to be used are: "GTSPriority1", "GTSPriority2", "GTSPriority3" and "GTSPriority4".

Below is the “resourceConstraints” element for a WMOEssential GTS product intended for global exchange:

```
<!--   Data intended for WMOEssential data intended for Global exchange -->
<gmd:resourceConstraints>
   <gmd:MD _ LegalConstraints>
      <gmd:useLimitation>
        <gco:CharacterString>Data is near realtime, and is not quality controlled. 
License conditions apply, as indicated below</gco:CharacterString>
      </gmd:useLimitation>
      <!--   MD _ RestrictionCode to be "otherRestrictions" -->
      <gmd:accessConstraints>
<gmd:MD _ RestrictionCode codeList="http://standards.iso.org/ittf/
PubliclyAvailableStandards/ISO _ 19139 _ Schemas/resources/Codelist/gmxCodelists.xml#MD
_ RestrictionCode" codeListValue="copyright">copyright</gmd:MD _ RestrictionCode>
      </gmd:accessConstraints>
      <gmd:accessConstraints>
         <gmd:MD _ RestrictionCode codeList="http://standards.iso.org/ittf/
PubliclyAvailableStandards/ISO _ 19139 _ Schemas/resources/Codelist/gmxCodelists.xml
#MD _ RestrictionCode" codeListValue="otherRestrictions">otherRestrictions</gmd:MD
_ RestrictionCode>
      </gmd:accessConstraints>
      <gmd:useConstraints>
        <gmd:MD _ RestrictionCode
codeList="http://standards.iso.org/ittf/PubliclyAvailableStandards/ISO
_ 19139 _ Schemas/resources/Codelist/gmxCodelists.xml#MD _ RestrictionCode"
codeListValue="copyright">copyright</gmd:MD _ RestrictionCode>
      </gmd:useConstraints>
      <gmd:useConstraints>
         <gmd:MD _ RestrictionCode
codeList="http://standards.iso.org/ittf/PubliclyAvailableStandards/ISO
_ 19139 _ Schemas/resources/Codelist/gmxCodelists.xml#MD _ RestrictionCode"
codeListValue="otherRestrictions">otherRestrictions</gmd:MD _ RestrictionCode>
      </gmd:useConstraints>
      <!-- Add WMO Data policy and GTSPriority -->
      <gmd:otherConstraints>
         <gco:CharacterString>WMOEssential A definition of "WMOEssential" is available 
at: http://wis.wmo.int/2012/codelists/WMOCodeLists.xml#WMO _ DataLicenseCode </gco:
CharacterString>
      </gmd:otherConstraints>
      <gmd:otherConstraints>
         <gco:CharacterString>GTSPriority2</gco:CharacterString>
      </gmd:otherConstraints>
   </gmd:MD _ LegalConstraints>
</gmd:resourceConstraints>
```

In addition, the scope of distribution of data marked as “GlobalExchange” has to be added as a keyword (with KeywordTypeCode “dataCentre”).

```
<!-- keyword for stating the scope of distribution: Global Exchange   -->
<gmd:descriptiveKeywords>
  <gmd:MD _ Keywords>
    <gmd:keyword>
      <gco:CharacterString>GlobalExchange</gco:CharacterString>
    </gmd:keyword>
    <gmd:type>
      <gmd:MD _ KeywordTypeCode codeList="http://wis.wmo.int/2012/codelists/WMOCodeLists
.xml#MD _ DistributionScopeCode"
           codeListValue="dataCentre">dataCentre</gmd:MD _ KeywordTypeCode>
    </gmd:type>
  .. .. .. etc   (see section 5.8.1.8.2 for full example)
```

5.8.1.11 *Distribution information*

Distribution information	
Template value:	ADD-URL-TO-DATA-ACCESS-SERVICE*HR-MW, ADD-DISTRIBUTOR-SHORTNAME*HR (e.g.:EUM), ADD-DISTRIBUTOR-EMAIL-ADDRESS*HR, ADD-FORMAT-NAME*O-MW, ADD-FORMAT-VERSION*O-MW
Information:	Resource format, distributor information and resource transfer options (URLs)
Necessity:	Highly recommended for WCMP 1.3
Category:	Product information
XPath:	*/gmd:MD_Metadata/gmd:distributionInfo/*/gmd:distributionFormat/*/gmd:formatDistributor/*/* {complex content}, including ↘*distributorContact/gmd:CI_ResponsibleParty/* and ↘*distributorTransferOptions/*/gmd:online/*

Below is an example of a GRIB product made available via an FTP server (for readability, distributor details are not included in this snippet, but can be found in the template record):

```
<gmd:distributionInfo>
    <gmd:MD _ Distribution>
        <gmd:distributionFormat>
            <gmd:MD _ Format>
                <gmd:name>
                    <gco:CharacterString>GRIB</gco:CharacterString>
                </gmd:name>
                <gmd:version>
                    <gco:CharacterString>FM 92 GRIB Edition 2</gco:CharacterString>
                </gmd:version>
                <gmd:specification>
                    <gco:CharacterString>http://www.wmo.int/pages/prog/www/WMOCodes.html</
gco:CharacterString>
                </gmd:specification>
            </gmd:MD _ Format>
        </gmd:distributionFormat>
        <gmd:transferOptions>
            <gmd:MD _ DigitalTransferOptions>
                <gmd:onLine>
                    <gmd:CI _ OnlineResource>
                        <gmd:linkage>
                            <gmd:URL>ftp://data-portal.ecmwf.int/</gmd:URL>
                        </gmd:linkage>
                        <gmd:protocol>
```

```
                            <gco:CharacterString>WWW:DOWNLOAD-1.0-ftp--download</gco:
CharacterString>
                        </gmd:protocol>
                        <gmd:name>
                            <gco:CharacterString>ECMWF DCPC FTP Server</gco:
CharacterString>
                        </gmd:name>
                        <gmd:description>
                            <gco:CharacterString>WMO Information System download service 
through ECMWF DCPC</gco:CharacterString>
                        </gmd:description>
                        <gmd:function>
                            <gmd:CI _ OnLineFunctionCode codeList="http://standards
.iso.org/ittf/PubliclyAvailableStandards/ISO _ 19139 _ Schemas/resources/Codelist/
gmxCodelists.xml#CI _ OnLineFunctionCode" codeListValue="download">download</gmd:CI
_ OnLineFunctionCode>
                        </gmd:function>
                    </gmd:CI _ OnlineResource>
                </gmd:onLine>
            </gmd:MD _ DigitalTransferOptions>
        </gmd:transferOptions>
    </gmd:MD _ Distribution>
</gmd:distributionInfo>
```

5.8.1.12 *Party to be recognized as the originator of the information*

Cited party information	
Template value:	ADD-CITED-RESPONSIBLE-PARTY-ORGANISATION*O-MW
Information:	Party that should be cited as the originator (that is, data author) of the resource.
Necessity:	Optional for WCMP 1.3
Category:	Product information
XPath:	*/gmd:MD_Metadata/gmd:distributionInfo/*/gmd:citation/*/gmd:citedResponsibleParty/ gmd:CI_ResponsibleParty/* {complex content}

When the data owners wish to be cited in references to their data, they can stipulate this in the “citedResponsibleParty” block, using the role “originator”.

Below is an example:

```
<gmd:identificationInfo>
<gmd:MD _ DataIdentification>
   <gmd:citation>
      <gmd:CI _ Citation>
         …. .. .. ..
         <gmd:citedResponsibleParty>
            <gmd:CI _ ResponsibleParty>
                <gmd:organisationName>
                    <gco:CharacterString>EUMETSAT</gco:CharacterString>
                </gmd:organisationName>
                <gmd:role>
                    <gmd:CI _ RoleCode      codeList="http://standards.iso.org/ittf/
PubliclyAvailableStandards/ISO _ 19139 _ Schemas/resources/Codelist/gmxCodelists.xml#MD
_ ScopeCode" codeListValue="pointOfContact">originator</gmd:CI _ RoleCode>
                </gmd:role>
            </gmd:CI _ ResponsibleParty>
         </gmd:citedResponsibleParty>
         <gmd:otherCitationDetails>
             <gco:CharacterString>Add other citing instructions here</gco:
CharacterString>
```

```
         </gmd:otherCitationDetails>
           ..  ..  ..  ..
       </gmd:CI _ Citation>
    </gmd:citation>
     ..  ..  ..  ..
  </gmd:MD _ DataIdentification>
</gmd:identificationInfo>
```

Further details on how the item should be cited can be added to the “otherCitationDetails” block.

5.8.1.13 *Frequency of resource updates*

Resource update frequency information	
Template value:	ADD-PRODUCT-UPDATE-FREQ-PERIOD*O, ADD-PRODUCT-UPDATE-FREQ-CODE*O-MW
Information:	Frequency of resource update
Necessity:	Optional for WCMP 1.3
Category:	Product information
XPath:	*/gmd:MD_Metadata/gmd:identificationInfo/*/gmd:resourceMaintenance/*/gmd: maintenanceAndUpdateFrequency/*

If the block on resource maintenance and update frequency is used, the MD_MaintenanceFrequencyCode is mandatory.

The example below shows a product that is available every 6 hours starting at 03 UTC.

```
<gmd:resourceMaintenance>
   <gmd:MD _ MaintenanceInformation>
      <gmd:maintenanceAndUpdateFrequency>
         <gmd:MD _ MaintenanceFrequencyCode codeListValue="irregular" codeList="http://
standards.iso.org/ittf/PubliclyAvailableStandards/ISO _ 19139 _ Schemas/resources/codelist/
gmxCodelists.xml#MD _ MaintenanceFrequencyCode"/>
      </gmd:maintenanceAndUpdateFrequency>
      <gmd:userDefinedMaintenanceFrequency>
         <gts:TM _ PeriodDuration>PT6H</gts:TM _ PeriodDuration>
      </gmd:userDefinedMaintenanceFrequency>
      <gmd:maintenanceNote>
         <gco:CharacterString>ADD-PRODUCT-UPDATE-FREQ-NOTE (e.g. Instances of bulletin
SIKB20NGTT are available every 6 hours starting at 03 UTC)</gco:CharacterString>
      </gmd:maintenanceNote>
   </gmd:MD _ MaintenanceInformation>
</gmd:resourceMaintenance>
```

5.8.2 **Mandatory WIS technical information**

In addition to the mandatory elements included in section 5.8.1 above, the following information is required:

5.8.2.1 *Metadata record unique identifier*

Metadata record unique identifier	
Template value:	ADD-WCMP-IDENTIFIER*M
Information:	Unique identifier (UID) for individual WIS discovery metadata records
Necessity:	Mandatory for WCMP 1.3
Category:	WIS technical information
XPath:	*/gmd:MD_Metadata/gmd:fileIdentifier/*/text()*

The WCMP UID (fileIdentifier) has to be globally unique, that is, no two WIS metadata records can have the same WCMP UID.

In the absence of any system, defined by the organization creating a metadata record, that ensures uniqueness of the WCMP UID, this should be structured as follows:

```
urn:x-wmo:md:DataProviderInternetDomainName::ProductUID
```

where:

“:” is used as a separator;

urn:x-wmo:md: is mandatory;

DataProviderInternetDomainName:: designates the citation authority, based on the reversed Internet domain name of the data provider (for example, int.eumetsat, gov.noaa); please note the recommended use of two colons “::”. For products exchanged on the GTS, the required form is “int.wmo.wis::”.

ProductUID is a unique identifier whose structure is defined by the organization responsible for the metadata record.

Examples:

UID for northern hemisphere satellite cloud information chart from Japan:

```
urn:x-wmo:md:jp.go.jma.wis.dcpc-sat::WAID
```

UID for an outgoing long-wave radiation product from the FY-2D satellite:

```
urn:x-wmo:md:cn.gov.cma::NSMC.FY2D.OLR _ MLT _ OTG.BAWX
```

Unique identifier for GTS products

Additional rules apply to metadata records describing products distributed through the GTS. The file identifier for bulletin metadata has the following structure:

```
urn:x-wmo:md:int.wmo.wis::{uid}
```

where {uid} is a unique identifier derived from the GTS bulletin or file name.

Further background information on constructing a file identifier for products distributed through the GTS is available in the WMO Core Metadata Profile version 1.3, Part 1, section 9.2.

An example of file identifier for a Deutscher Wetterdienst Numerical Weather Prediction Model is:

```
urn:x-wmo:md:int.wmo.wis::HTXC85EDZW
```

An example of file identifier for Meteo France Numerical Weather Prediction Model is:

```
urn:x-wmo:md:int.wmo.wis::FR-meteofrance-toulouse,GRIB,ARPEGE-75N10N-60W65E _ C _ LFPW
```

5.8.2.2 *Metadata modification – DateStamp*

Metadata modification – DateStamp	
Template value:	ADD-METADATA-LAST-MODIFICATION-DATE*M
Information:	Date when the metadata record was last modified
Necessity:	Mandatory for WCMP 1.3
Category:	WIS technical information
XPath:	*/gmd:MD_Metadata/gmd:dateStamp*

This shows when the metadata record was last modified and has the following date pattern: YYYY-MM-DDThh:mm:ss, for example 2015-12-29T11:45:55.

5.8.2.3 *Product creation date*

Creation date	
Template value:	ADD-PRODUCT-CREATION-DATE*M
Information:	Creation date of the product
Necessity:	Mandatory for WCMP 1.3
Category:	WIS technical information
XPath:	*/gmd:MD_Metadata/gmd:identificationInfo/*/gmd:citation/*/gmd:date/*/* *↘/gmd:date/*/text() and* *↘/gmd:dateType/*/@codeListValue="creation"*

This shows when the product was created and has the following date pattern: YYYY-MM-DD or YYYY-MM-DDThh:mm:ss. See also section 5.8.1.5 for details of the date/time format.

Example:

```
<gmd:date>
   <gmd:CI _ Date>
      <gmd:date>
         <gco:Date>2015-03-23</gco:Date>
      </gmd:date>
      <gmd:dateType>
         <gmd:CI _ DateTypeCode codeList="http://standards.iso.org/ittf/
PubliclyAvailableStandards/ISO _ 19139 _ Schemas/resources/Codelist/gmxCodelists.xml#CI
_ DateTypeCode" codeListValue="creation"/>
      </gmd:dateType>
   </gmd:CI _ Date>
<gmd:date>
```

5.9 TECHNICAL DOCUMENT

More details on the WCMP metadata can be found at http://wis.wmo.int/MD_Index.

ANNEX. CRITERIA FOR CREATING A METADATA RECORD THAT REPRESENTS A COLLECTION OF PRODUCTS

This annex defines criteria and other elements to consider when creating a metadata record that represents a collection of products.

To understand the notion of collection, it is important to distinguish between a dataset and a temporal subset of a dataset. Meteorological data is often transient (for example, observations, forecasts and NWP products) and continuously updated. A dataset is typically seen as an aggregate of temporal instances or subsets (the collection) and, as explained below, metadata for a dataset is not typically set at the instance level. This is so even when a new instance or subset of a dataset is produced daily, and when only the latest day of data is ever available (in that case, the temporalExtent of the dataset is "latest 24 hours only").

The criteria to be considered when creating the collection metadata record include:

(a) Size of dataset instances:

An important consideration, in terms of dataset granularity, is how the dataset instances will be made available to end users; for instance, push or pull services, with filter capabilities or not.

Numerical model output could be seen as a four- and even five-dimensional dataset (latitude, longitude, height, time, reference time). It is possible to set granularity at this level, but the amount of data would be huge, and it would not be possible to exchange the whole dataset using "push" mode. Such large scale granularity of data is ideally provided via download (or publish-subscribe) services with subsetting capabilities (for instance, Web Coverage Service (WCS) or direct download INSPIRE services).

When the data provider is not able to implement such services, and when only predefined datasets or time windows are made available (for example, datasets for global exchange on the WIS) the granularity may have to be finer. For example, the French high-resolution model, AROME, is split into two daily subsets:

– Dataset 1: AROME 0°01 FRANCE – 00h–23h

– Dataset 2: AROME 0°01 FRANCE – 24h–45h

where Dataset 1 covers hourly steps H to H+23h and Dataset 2 covers hourly steps H+24 to H+45.

The granularity of the subsets is chosen according to the size of the instances to be exchanged, and the size of the granules (500 Mb, 1Gb, etc.) should be compatible with the bandwidth available for data exchange.

Note that it is also possible to define an aggregate of two subsets, for instance:

– Dataset 0: AROME 0°01 FRANCE

where Dataset 0 is an aggregate of Dataset 1 and Dataset 2;

(b) Content consistency:

It is recommended, if possible, not to blend multiple data categories or topics in the same dataset, which would result in a heterogeneous aggregate. For example, an aggregate of satellite observations and weather forecasts would typically not make sense (unless they had been combined for a particular purpose); whereas an aggregate of lake pollution and river pollution data makes sense, especially if the data processing has been similar and the data license is the same.

More generally, dataset heterogeneity in terms of content can result in very vague descriptions in the metadata, which will in turn affect data discoverability on the WIS;

(c) Update frequency and other temporal characteristics:

The refresh rate of data also has to be taken into account, in terms of dataset granularity, because this will have an impact on catalogues.

Setting the dataset/metadata granularity at the temporal instance level instead of time series level would require the generation (automatically) of a lot of metadata records and the update of catalogues in near real time. It would also make it difficult to synchronize metadata records among the GISCs, especially through harvesting processes. Such a large number of metadata records would also make it difficult for users to find the information they were seeking. For instance, a "French WMO Resolution 40 Essential SYNOP" dataset could be seen as a temporal series and, provided that the entire dataset continues to be available, the discovery metadata should be provided at this level not at temporal instance level (for example, "French WMO Resolution 40 Essential SYNOP 2016-04-07T12:00:00Z").

It is also recommended not to blend data of different refresh rates in the same dataset, because it will not be possible to specify the update frequency in discovery metadata records;

(d) Data policy and distribution scope:

A dataset shall be homogeneous in terms of data policy, including WMO distribution policy, which is described through WMO_DistributionScopeCode, WMO_DataLicenseCode, WMO_GTSProductCategoryCode and MD_RestrictionCode codelists. The *Manual on WIS*, Appendix C, Part C1, section 9.3 states: "The presence of more than one WMO data-policy statement in a single metadata record yields an ambiguous state; a WIS discovery metadata record describing data for global exchange shall declare only a single WMO data policy.";

(e) Spatial extent:

Except for global datasets, a coarse granularity is likely to affect the discoverability of data on the basis of a spatial criterion, especially if the areas where data are available are disjoint. For example, synoptic observations from the French Overseas Departments of Guyana, Martinique, Reunion and Guadeloupe are dispatched in different datasets.

Field hierarchy and cardinality

Below is a nested list of fields likely to be used in a WCMP record, together with their cardinality.

Cardinality is denoted by [x..y]. Where it is preceded by ISO, the cardinality in the WCMP will be the same. Where it is different, the cardinality for both ISO and WCMP will be appended to the element name.

As noted in paragraph 5.7.10, many optional subsections of a WCMP record contain elements that are mandatory only if that subsection is used. See, for example, the identifier, authority and title segments, as shown in lines 53–57 in the hierarchical list of fields below, where identifier is optional [0..n] and, even if it is used, authority is also optional [0..n]; however, if authority is used, then title is mandatory [1..1].

The cardinality notation [x..y] indicates the minimum and maximum allowable times that the element may be used within that part of the hierarchy or tree.

For instance, the notation:

> [0..n] means that the element is optional, but can also be used any number of times;
>
> [1..2] means that it is mandatory (there must be at least one) and may be used a maximum of two times.

```
1     MD _ Metadata _ . _ .ISO[1..1]
2     _ .fileIdentifier _ .char _ . _ . WMO[1..1] , ISO[0..1]
3     _ .language _ .char _ . _ .ISO[0..1]
4     _ .characterSet _ .CODE:MD _ CharacterSetCode _ . _ .ISO[0..1]
5     _ .parentIdentifier _ .char _ . _ .ISO[0..1]
6     _ .hierarchyLevel _ .char _ . _ .ISO[0..n]
7     _ .hierarchyLevelName _ .char _ . _ .ISO[0..n]
8
9     _ .contact _ . _ .ISO[1..n]
10    _ . _ .CI _ ResponsibleParty
    see lines 66-99, for all fields available for CI _ ResponsibleParty
11    _ . _ . _ .individualName _ .char _ . _ .ISO[0..1]
12    _ . _ . _ .organisationName _ .char _ . _ .ISO[0..1]
13    _ . _ . _ .contactInfo _ . _ .ISO[0..1]
14    _ . _ . _ . _ . CI _ Contact _ . _ .
15    _ . _ . _ . _ . _ .address _ . _ .ISO[0..1]
16    _ . _ . _ . _ . _ . _ .CI _ Address _ . _ .
17    _ . _ . _ . _ . _ . _ . _ .electronicMailAddress _ .char _ . _ .ISO[0..n]
18    _ . _ . _ .role _ .CODE:CI _ RoleCode _ . _ .ISO[1..1]
19
20    _ .dateStamp _ .DATETIME _ . _ .ISO[1..1]
21      _ .metadataStandardName _ .char _ . _ .ISO[0..1]
22    _ .metadataStandardVersion _ .char _ . _ .ISO[0..1]
23      _ .dataSetURI _ .char _ . _ .ISO[0..1]
24       ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
25    _ .spatialRepresentationInfo _ . _ .ISO[0..n]
26    _ . _ .MD _ GridSpatialRepresentation
27    _ . _ . _ .numberOfDimensions _ .integer _ . _ .ISO[1..1]
28    _ . _ . _ .axisDimensionProperties _ . _ .ISO[1..1]
29    _ . _ . _ . _ .MD _ Dimension _ . _ .
30    _ . _ . _ . _ . _ .dimensionName _ .CODE:MD _ DimensionNameTypeCode _ . _ .ISO[1..1]
31    _ . _ . _ . _ . _ .dimensionSize _ .integer _ . _ .ISO[1..1]
32    _ . _ . _ . _ . _ .resolution _ .SCALE _ . _ .ISO[0..1]
33    _ . _ . _ . _ . _ .dimensionName _ .CODE:MD _ DimensionNameTypeCode _ . _ .ISO[1..1]
34    _ . _ . _ . _ . _ .dimensionSize _ .integer _ . _ .ISO[1..1]
35    _ . _ . _ . _ . _ .resolution _ .SCALE _ . _ .ISO[0..1]
36    _ . _ . _ .cellGeometry _ .CODE:MD _ CellGeometryCode _ . _ .ISO[1..1]
37    _ . _ . _ .transformationParameterAvailability _ .Boolean _ . _ .ISO[1..1]
38       ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
39
40    _ .identificationInfo _ . _ .ISO[1..n]
41    _ . _ .MD _ DataIdentification _ .
42
43    _ . _ . _ .citation _ . _ .ISO[1..1]
44    _ . _ . _ . _ .CI _ Citation _ . _ .
45    _ . _ . _ . _ . _ .title _ .char _ . _ .ISO[1..1]
46    _ . _ . _ . _ . _ .alternateTitle _ .char _ . _ .ISO[0..n]
47    _ . _ . _ . _ . _ .DATE _ . _ .ISO[1..n]
48    _ . _ . _ . _ . _ . _ .CI _ Date _ .
49    _ . _ . _ . _ . _ . _ . _ .DATE _ .DATETIME _ . _ .ISO[1..1]
50    _ . _ . _ . _ . _ . _ . _ .dateType _ .CODE:CI _ DateTypeCode _ . _ .ISO[1..1]
51    _ . _ . _ . _ . _ .edition _ .char _ . _ .ISO[0..1]
```

```
52
53    _ . _ . _ . _ . _ .identifier _ . _ .ISO[0..n]
54    _ . _ . _ . _ . _ . _ .MD _ Identifier _ . _ .
55    _ . _ . _ . _ . _ . _ . _ .authority _ . _ .ISO[0..1]
56    _ . _ . _ . _ . _ . _ . _ . _ .CI _ Citation _ . _ .
   see lines 43-111, for all fields available for CI _ Citation
57    _ . _ . _ . _ . _ . _ . _ . _ . _ .title _ .char _ . _ .ISO[1..1]
58    _ . _ . _ . _ . _ . _ . _ . _ . _ .alternateTitle _ .char _ . _ .ISO[0..n]
59    _ . _ . _ . _ . _ . _ . _ . _ . _ .DATE _ . _ .ISO[1..n]
60    _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .CI _ Date _ .
61    _ . _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .DATE _ .DATE _ . _ .ISO[1..1]
62    _ . _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .dateType _ .CODE:CI _ DateTypeCode _ . _ .ISO[1..1]
63    _ . _ . _ . _ . _ . _ . _ .code _ .char _ . _ .ISO[1..1]
64
65    _ . _ . _ . _ . _ .citedResponsibleParty _ . _ .ISO[0..n]
66    _ . _ . _ . _ . _ . _ .CI _ ResponsibleParty _ . _ .
67    _ . _ . _ . _ . _ . _ . _ .individualName _ .char _ . _ .ISO[0..1] *C
68    _ . _ . _ . _ . _ . _ . _ .organisationName _ .char _ . _ .ISO[0..1] *C
69    _ . _ . _ . _ . _ . _ . _ .positionName _ .char _ . _ .ISO[0..1] *C
70
71    _ . _ . _ . _ . _ . _ . _ .contactInfo _ . _ .ISO[0..1]
72    _ . _ . _ . _ . _ . _ . _ . _ .CI _ Contact _ . _ .
73
74    _ . _ . _ . _ . _ . _ . _ . _ . _ .phone _ . _ .ISO[0..1]
75    _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .CI _ Telephone _ . _ .
76    _ . _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .voice _ .char _ . _ .ISO[0..n]
77    _ . _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .facsimile _ .char _ . _ .ISO[0..n]
78
79    _ . _ . _ . _ . _ . _ . _ . _ . _ .address _ . _ .ISO[0..1]
80    _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .CI _ Address _ . _ .
81    _ . _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .deliveryPoint _ .char _ . _ .ISO[0..n]
82    _ . _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .city _ .char _ . _ .ISO[0..1]
83    _ . _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .administrativeArea _ .char _ . _ .ISO[0..1]
84    _ . _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .postalCode _ .char _ . _ .ISO[0..1]
85    _ . _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .country _ .char _ . _ .ISO[0..1]
86    _ . _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .electronicMailAddress _ .char _ . _ .ISO[0..n]
87
88    _ . _ . _ . _ . _ . _ . _ . _ . _ .onlineResource _ . _ .ISO[0..1]
89    _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .CI _ OnlineResource _ . _ .
90    _ . _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .linkage _ .URL _ . _ .ISO[1..1]
91    _ . _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .protocol _ .char _ . _ .ISO[0..1]
92    _ . _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .applicationProfile _ .char _ . _ .ISO[0..1]
93    _ . _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .name _ .char _ . _ .ISO[0..1]
94    _ . _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .description _ .char _ . _ .ISO[0..1]
95    _ . _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .function _ .CODE:CI _ OnLineFunctionCode _ . _
      .ISO[0..1]
96
97    _ . _ . _ . _ . _ . _ . _ . _ . _ .hoursOfService _ .char _ . _ .ISO[0..1]
98    _ . _ . _ . _ . _ . _ . _ . _ . _ .contactInstructions _ .char _ . _ .ISO[0..1]
99    _ . _ . _ . _ . _ . _ . _ .role _ .CODE:CI _ RoleCode _ [1..1].
100
101   _ . _ . _ . _ . _ .presentationForm _ .CODE:CI _ PresentationFormCode _ . _ .ISO[0..n]
102
103   _ . _ . _ . _ . _ .series _ . _ .ISO[0..1]
104   _ . _ . _ . _ . _ . _ .CI _ Series _ .
105   _ . _ . _ . _ . _ . _ . _ .name _ .char _ . _ .ISO[0..1]
106   _ . _ . _ . _ . _ . _ . _ .issueIdentification _ .char _ . _ .ISO[0..1]
107   _ . _ . _ . _ . _ . _ . _ .page _ .char _ . _ .ISO[0..1]
108   _ . _ . _ . _ . _ .otherCitationDetails _ .char _ . _ .ISO[0..1]
109   _ . _ . _ . _ . _ .collectiveTitle _ .char _ . _ .ISO[0..1]
```

```
110   _ . _ . _ . _ . _ .ISBN _ .char _ . _ .ISO[0..1]
111   _ . _ . _ . _ . _ .ISSN _ .char _ . _ .ISO[0..1]
112
113
114   _ . _ . _ .abstract _ .char _ . _ .ISO[1..1]
115   _ . _ . _ .purpose _ .char _ . _ .ISO[0..1]
116   _ . _ . _ .credit _ .char _ . _ .ISO[0..n]
117   _ . _ . _ .status _ .CODE:MD _ ProgressCode _ . _ .ISO[0..n]
118
119   _ . _ . _ .pointOfContact _ . _ .ISO[0..n]
120   _ . _ . _ . _ .CI _ ResponsibleParty _ . _ .
121   _ . _ . _ . _ . _ .individualName _ .char _ . _ .ISO[0..1]
122   _ . _ . _ . _ . _ .organisationName _ .char _ . _ .ISO[0..1]
123   _ . _ . _ . _ . _ .positionName _ .char _ . _ .ISO[0..1]
124   _ . _ . _ . _ . _ .contactInfo _ . _ .ISO[0..1]
125   _ . _ . _ . _ . _ . _ .CI _ Contact _ . _ .
126   _ . _ . _ . _ . _ . _ . _ .phone _ . _ .ISO[0..1]
127   _ . _ . _ . _ . _ . _ . _ . _ .CI _ Telephone _ . _ .
128   _ . _ . _ . _ . _ . _ . _ . _ . _ .voice _ .char _ . _ .ISO[0..1]
129   _ . _ . _ . _ . _ . _ . _ . _ . _ .facsimile _ .char _ . _ .ISO[0..1]
130   _ . _ . _ . _ . _ . _ . _ .address _ . _ .ISO[0..1]
131   _ . _ . _ . _ . _ . _ . _ . _ .CI _ Address _ . _ .
132   _ . _ . _ . _ . _ . _ . _ . _ . _ .deliveryPoint _ .char _ . _ .ISO[0..1]
133   _ . _ . _ . _ . _ . _ . _ . _ . _ .electronicMailAddress _ .char _ . _ .ISO[0..1]
134   _ . _ . _ . _ . _ .role _ .CODE:CI _ RoleCode _ . _ .ISO[1..1]
135
136   _ . _ . _ .resourceMaintenance _ . _ .ISO[0..n]
137   _ . _ . _ . _ .MD _ MaintenanceInformation _ .
138   _ . _ . _ . _ . _ .maintenanceAndUpdateFrequency _ .
          CODE: MD _ MaintenanceFrequencyCode _ . _ .ISO[1..1]
139   _ . _ . _ . _ . _ .userDefinedMaintenanceFrequency _ .TM _ PeriodDuration _ . _ .ISO[0..1]
140   _ . _ . _ . _ . _ .updateScopeDescription _ . _ .ISO[0..n]
141   _ . _ . _ . _ . _ . _ .MD _ ScopeDescription _ .
142   _ . _ . _ . _ . _ . _ . _ .dataset _ .char _ . _ .ISO[1..1]
143   _ . _ . _ . _ . _ .maintenanceNote _ .char _ . _ .ISO[0..n]
144
145   _ . _ . _ .graphicOverview _ . _ .ISO[0..n]
146   _ . _ . _ . _ .MD _ BrowseGraphic _ .
147   _ . _ . _ . _ . _ .fileName _ .char _ . _ .ISO[1..1]
148   _ . _ . _ . _ . _ .fileDescription _ .char _ . _ .ISO[0..1]
149   _ . _ . _ . _ . _ .fileType _ .char _ . _ .ISO[0..1]
150
151   _ . _ . _ .descriptiveKeywords _ . _ WMO[1..n]    .ISO[0..n]
152   _ . _ . _ . _ .MD _ Keywords _ .
153   _ . _ . _ . _ . _ .keyword _ .char _ . _ .ISO[1..n]
154   _ . _ . _ . _ . _ .type _ .CODE:MD _ KeywordTypeCode _ . _ .ISO[0..1]
155   _ . _ . _ . _ . _ .thesaurusName _ . _ .ISO[0..1]
156   _ . _ . _ . _ . _ . _ .CI _ Citation _ . _ .
    see lines 43-111, for all fields available for CI _ Citation
157   _ . _ . _ . _ . _ . _ . _ .title _ .char _ . _ .ISO[1..1]
158   _ . _ . _ . _ . _ . _ . _ .DATE _ . _ .ISO[1..1]
159   _ . _ . _ . _ . _ . _ . _ . _ .CI _ Date _ . _ .
160   _ . _ . _ . _ . _ . _ . _ . _ . _ .DATE _ .DATE _ . _ .ISO[1..1]
161   _ . _ . _ . _ . _ . _ . _ . _ . _ .dateType _ .CODE:CI _ DateTypeCode _ . _ .ISO[1..1]
162
163   _ . _ . _ .resourceSpecificUsage _ . _ .ISO[0..n]
164   _ . _ . _ . _ .MD _ Usage _ .
165   _ . _ . _ . _ . _ .specificUsage _ .char _ . _ .ISO[1..1]
166   _ . _ . _ . _ . _ .userDeterminedLimitations _ .char _ . _ .ISO[0..n]
167   _ . _ . _ . _ . _ .userContactInfo _ . _ .ISO[1..n]
```

```
168   _ . _ . _ . _ . _ . _ .CI _ ResponsibleParty _ . _ .
      see lines 66-99, for all fields available for CI _ ResponsibleParty
169   _ . _ . _ . _ . _ . _ . _ .individualName _ .char _ . _ .ISO[0..1]
170   _ . _ . _ . _ . _ . _ . _ .organisationName _ .char _ . _ .ISO[0..1]
171   _ . _ . _ . _ . _ . _ . _ .role _ .CODE:CI _ RoleCode _ . _ .ISO[1..1]
172
173   _ . _ . _ .resourceConstraints _ . _ .ISO[0..n]
174   _ . _ . _ . _ .MD _ Constraints _ . ISO[0..n]
175   _ . _ . _ . _ . _ .useLimitation _ . _ .ISO[0..n]
176   _ . _ . _ . _ .MD _ LegalConstraints _ . ISO[0..n]
177   _ . _ . _ . _ . _ .useLimitation _ .char _ . _ .ISO[0..n]
178   _ . _ . _ . _ . _ .accessConstraints _ .CODE:MD _ RestrictionCode _ . _ .ISO[0..n]
179   _ . _ . _ . _ . _ .accessConstraints _ .CODE:MD _ RestrictionCode _ . _ .ISO[0..n]
180   _ . _ . _ . _ . _ .useConstraints _ .CODE:MD _ RestrictionCode _ . _ .ISO[0..n]
181   _ . _ . _ . _ . _ .useConstraints _ .CODE:MD _ RestrictionCode _ . _ .ISO[0..n]
182   _ . _ . _ . _ . _ .otherConstraints _ .char _ . _ .ISO[0..n]
183   _ . _ . _ . _ . _ .otherConstraints _ .char _ . _ .ISO[0..n]
184   _ . _ . _ . _ .MD _ SecurityConstraints _ . ISO[0..n]
185   _ . _ . _ . _ . _ .useLimitation _ .char _ . _ .ISO[0..n]
186   _ . _ . _ . _ . _ .classification _ .CODE:MD _ ClassificationCode _ . _ .ISO[1..1]
187   _ . _ . _ . _ . _ .userNote _ .char _ . _ .ISO[0..1]
188   _ . _ . _ . _ . _ .classificationSystem _ .char _ . _ .ISO[0..1]
189   _ . _ . _ . _ . _ .handlingDescription _ .char _ . _ .ISO[0..1]
190
191   _ . _ . _ .aggregationInfo _ . _ .ISO[0..n]
192   _ . _ . _ . _ .MD _ AggregateInformation _ .
193
194   _ . _ . _ . _ . _ .aggregateDataSetName _ . _ .ISO[0..1]
195   _ . _ . _ . _ . _ . _ .CI _ Citation _ . _ .
      see lines 43-111, for all fields availablefor CI _ Citation
196   _ . _ . _ . _ . _ . _ . _ .title _ .char _ . _ .ISO[1..1]
197   _ . _ . _ . _ . _ . _ . _ .DATE _ . _ .ISO[1..1]
198   _ . _ . _ . _ . _ . _ . _ . _ .CI _ Date _ . _ .
199   _ . _ . _ . _ . _ . _ . _ . _ . _ .DATE _ . DATE _ . _ .ISO[1..1]
200   _ . _ . _ . _ . _ . _ . _ . _ . _ .dateType _ .CODE:CI _ DateTypeCode _ . _ .ISO[1..1]
201
202   _ . _ . _ . _ . _ .aggregateDataSetIdentifier _ . _ .ISO[0..1]
203   _ . _ . _ . _ . _ . _ .MD _ Identifier _ .
204   _ . _ . _ . _ . _ . _ . _ .authority _ . _ .ISO[0..1]
205   _ . _ . _ . _ . _ . _ . _ . _ .CI _ Citation _ . _ .
      see lines 43-111, for all fields available for CI _ Citation
206   _ . _ . _ . _ . _ . _ . _ . _ . _ .title _ .char _ . _ .ISO[1..1]
207   _ . _ . _ . _ . _ . _ . _ . _ . _ .DATE _ . _ .ISO[1..1]
208   _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .CI _ Date _ . _ .
209   _ . _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .DATE _ . DATE _ . _ .ISO[1..1]
210   _ . _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .dateType _ .CODE:CI _ DateTypeCode _ . _ .ISO[1..1]
211   _ . _ . _ . _ . _ . _ . _ .code _ .char _ . _ .ISO[1..1]
212
213   _ . _ . _ . _ . _ .associationType _ .CODE:DS _ AssociationTypeCode _ . _ .ISO[1..1]
214   _ . _ . _ . _ . _ .initiativeType _ .CODE:DS _ InitiativeTypeCode _ . _ .ISO[0..1]
215
216   _ . _ . _ .spatialRepresentationType
217   _ . _ . _ . _ .MD _ SpatialRepresentationTypeCode
                              CODE: MD _ SpatialRepresentationTypeCode   ISO[0..n]
218
219   _ . _ . _ .spatialResolution _ . _ .ISO[0..n]
220   _ . _ . _ . _ .MD _ Resolution _ . _ .ISO[ ..]
221   _ . _ . _ . _ . _ .equivalentScale _ . _ .ISO[1..1]
```

```
_ . _ . _ . _ . _ . _ .MD _ RepresentativeFraction _ .
_ . _ . _ . _ . _ . _ . _ .denominator _ .integer _ . _ .ISO[1..1]

_ . _ . _ .language _ .char _ . _ .ISO[1..n]
_ . _ . _ .characterSet _ .CODE:MD _ CharacterSetCode _ . _ .ISO[0..n]
_ . _ . _ .topicCategory _ .CODE:MD _ TopicCategoryCode _ . _ .WMO[1..n]   ISO[0..n]
_ . _ . _ .environmentDescription _ .char _ . _ .ISO[0..1]

_ . _ . _ .extent _ . _ .ISO[0..n]
_ . _ . _ . _ .EX _ Extent _ .
_ . _ . _ . _ . _ .description _ .char _ . _ .ISO[0..1]
_ . _ . _ . _ . _ .geographicElement _ . _ . .ISO[0..n] (Mandatory, if data is geospatial)
_ . _ . _ . _ . _ . _ . EX _ GeographicBoundingBox _
_ . _ . _ . _ . _ . _ . _ .westBoundLongitude _ .DECIMAL _ . _ .ISO[1..1]
_ . _ . _ . _ . _ . _ . _ .eastBoundLongitude _ . DECIMAL _ . _ .ISO[1..1]
_ . _ . _ . _ . _ . _ . _ .southBoundLatitude _ . DECIMAL _ . _ .ISO[1..1]
_ . _ . _ . _ . _ . _ . _ .northBoundLatitude _ . DECIMAL _ . _ .ISO[1..1]


_ . _ . _ . _ . _ .geographicElement _ . ISO[0..n]
_ . _ . _ . _ . _ . _ .EX _ GeographicDescription _ .
_ . _ . _ . _ . _ . _ . _ .extentTypeCode _ . _ .Boolean _ . _ .ISO[0..1]
_ . _ . _ . _ . _ . _ . _ .geographicIdentifier _ . _ .ISO[1..1]
_ . _ . _ . _ . _ . _ . _ . _ .MD _ Identifier _ .
_ . _ . _ . _ . _ . _ . _ . _ . _ .code _ .char _ . _ .ISO[1..1]


_ . _ . _ . _ . _ .temporalElement _ . _ .ISO[0..n]
_ . _ . _ . _ . _ . _ .EX _ TemporalExtent _ .
_ . _ . _ . _ . _ . _ . _ .extent _ . _ .ISO[1..1]

_ . _ . _ .supplementalInformation _ .char _ . _ .ISO[0..1]
    ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

_ .referenceSystemInfo _ . _ .ISO[0..n]
_ . _ .MD _ ReferenceSystem _ .
_ . _ . _ .referenceSystemIdentifier _ . _ .ISO[0..1]
_ . _ . _ . _ .RS _ Identifier _ .
_ . _ . _ . _ . _ .authority _ . _ .ISO[0..1]
_ . _ . _ . _ . _ .code _ .char _ . _ .ISO[1..1]
_ . _ . _ . _ . _ .codeSpace _ .char _ . _ .ISO[0..1]
_ . _ . _ . _ . _ .version _ .char _ . _ .ISO[0..1]
    ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

_ .contentInfo _ . _ .ISO[0..n]
_ . _ .MD _ CoverageDescription _ .
_ . _ . _ .attributeDescription _ . _ .ISO[1..1]
_ . _ . _ . _ .RecordType _ . _ .
_ . _ . _ .contentType _ .CODE:MD _ CoverageContentTypeCode _ . _ .ISO[1..1]
    ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

_ .distributionInfo _ . _ .ISO[0..1]
_ . _ .MD _ Distribution _ .
_ . _ . _ .distributionFormat _ . _ .ISO[0..n]
_ . _ . _ . _ .MD _ Format _ .
_ . _ . _ . _ . _ .name _ .char _ . _ .ISO[1..1]
_ . _ . _ . _ . _ .version _ .char _ . _ .ISO[1..1]
_ . _ . _ . _ . _ .amendmentNumber _ .char _ . _ .ISO[0..1]
_ . _ . _ . _ . _ .specification _ .char _ . _ .ISO[0..1]
_ . _ . _ . _ . _ .fileDecompressionTechnique _ .char _ . _ .ISO[0..1]
```

```
283  _ . _ . _ . _ . _ .formatDistributor _ . _ .ISO[0..n]
284  _ . _ . _ . _ . _ . _ .MD _ Distributor _ .
285  _ . _ . _ . _ . _ . _ . _ .distributorContact _ . _ .ISO[1..1]
286  _ . _ . _ . _ . _ . _ . _ . _ .CI _ ResponsibleParty _ .
     see lines 66-99, for all fields available for CI _ ResponsibleParty
287  _ . _ . _ . _ . _ . _ . _ . _ . _ .individualName _ .char _ . _ .ISO[0..1]
288  _ . _ . _ . _ . _ . _ . _ . _ . _ .organisationName _ .char _ . _ .ISO[0..1]
289  _ . _ . _ . _ . _ . _ . _ . _ . _ .role _ .CODE:CI _ RoleCode _ . _ .ISO[1..1]
290  _ . _ . _ . _ . _ . _ . _ .distributorTransferOptions _ . _ .ISO[0..n]
291  _ . _ . _ . _ . _ . _ . _ . _ .MD _ DigitalTransferOptions _ .
292  _ . _ . _ . _ . _ . _ . _ . _ . _ .unitsOfDistribution _ .char _ . _ .ISO[0..1]
293  _ . _ . _ . _ . _ . _ . _ . _ . _ .transferSize _ .Real _ . _ .ISO[0..1]
294
295  _ . _ . _ . _ . _ . _ . _ . _ . _ .onLine _ . _ .ISO[0..n]
296  _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .CI _ OnlineResource _ .
297  _ . _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .linkage _ .URL _ . _ .ISO[1..1]
298  _ . _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .protocol _ .char _ . _ .ISO[0..1]
299  _ . _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .name _ .char _ . _ .ISO[0..1]
300  _ . _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .description _ .char _ . _ .ISO[0..1]
301  _ . _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .function _ .CODE: CI _ OnLineFunctionCode _ . _
     .ISO[0..1]
302     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
303
304  _ .dataQualityInfo _ . _ .ISO[0..n]
305  _ . _ .DQ _ DataQuality _ .
306  _ . _ . _ .scope _ . _ .ISO[1..1]
307  _ . _ . _ . _ .DQ _ Scope _ .
308  _ . _ . _ . _ . _ .level _ .CODE:MD _ ScopeCode _ . _ .ISO[1..1]
309  _ . _ . _ . _ . _ .extent _ .
310  _ . _ . _ . _ . _ .levelDescription _ . _ .ISO[0..n]
311  _ . _ . _ . _ . _ . _ .MD _ ScopeDescription _ .
312  _ . _ . _ . _ . _ . _ . _ .dataset _ .char _ . _ .ISO[1..1]
313  _ . _ . _ .lineage _ . _ .ISO[0..1]
314  _ . _ . _ . _ .LI _ Lineage _ .
315  _ . _ . _ . _ . _ .statement _ .char _ . _ .ISO[0..1]
316
317  _ . _ . _ . _ . _ .processStep _ . _ .ISO[0..n]
318  _ . _ . _ . _ . _ . _ .LI _ ProcessStep _ .
319  _ . _ . _ . _ . _ . _ . _ .description _ .char _ . _ .ISO[1..1]
320  _ . _ . _ . _ . _ . _ . _ .rationale _ .char _ . _ .ISO[0..1]
321  _ . _ . _ . _ . _ . _ . _ .source _ . _ .ISO[0..n]
322  _ . _ . _ . _ . _ . _ . _ . _ .LI _ Source _ .
323  _ . _ . _ . _ . _ . _ . _ . _ . _ .description _ .char _ . _ .ISO[0..1]
324  _ . _ . _ . _ . _ . _ . _ . _ . _ .sourceCitation _ . _ .ISO[0..1]
325  _ . _ . _ . _ . _ . _ . _ . _ . _ . _ .CI _ Citation _ . _ .
326
327  _ . _ . _ . _ . _ .source _ . _ .ISO[0..n]
328  _ . _ . _ . _ . _ . _ .LI _ Source _ .
329  _ . _ . _ . _ . _ . _ . _ .description _ .char _ . _ .ISO[0..1]
330     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
331
332  _ .metadataConstraints _ . _ .ISO[0..n]
333  _ . _ .MD _ Constraints _ .
334  _ . _ . _ .useLimitation _ .char _ . _ .ISO[0..n]
335  _ . _ .MD _ LegalConstraints _ .
336  _ . _ . _ .useLimitation _ .char _ . _ .ISO[0..n]
337  _ . _ . _ .accessConstraints _ .CODE: MD _ RestrictionCode _ . _ .ISO[0..n]
338  _ . _ . _ .useConstraints _ .CODE: MD _ RestrictionCode
339  _ . _ . _ .otherConstraints _ .char _ . _ .ISO[0..n]
340     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

```
341
342   _ .applicationSchemaInfo _ . _ .ISO[0..n]
343   _ . _ .MD _ ApplicationSchemaInformation _ .
344   _ . _ . _ .name _ . _ .ISO[1..1]
345   _ . _ . _ . _ .CI _ Citation _ . _ .
    see lines 43-111, for all fields available for CI _ Citation
346   _ . _ . _ .schemaLanguage _ .char _ .
347   _ . _ . _ .constraintLanguage _ .char _ . _ .ISO[1..1]
348      ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
349
350   _ .metadataMaintenance _ .
351   _ . _ .MD _ MaintenanceInformation _ . _ .ISO[0..1]
352   _ . _ . _ .maintenanceAndUpdateFrequency _ . CODE:MD _ MaintenanceFrequencyCode _ . _
      .ISO[1..1]
353   _ . _ . _ .dateOfNextUpdate _ .DATE _ . _ .ISO[1..1]
354   _ . _ . _ .userDefinedMaintenanceFrequency _ .PERIODDURATION _ . _ .ISO[0..1]
355   _ . _ . _ .updateScope _ .CODE:MD _ ScopeCode _ . _ .ISO[0..1]
356   _ . _ . _ .updateScopeDescription _ . _ .ISO[0..n]
357   _ . _ . _ . _ .MD _ ScopeDescription _ . _ .ISO[0..n]
358   _ . _ . _ . _ . _ .dataset _ .char _ .
359   _ . _ . _ .maintenanceNote _ .char _ . _ .ISO[1..1]
360      ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

PART VI. INFORMATION MANAGEMENT

Guidance on management of information about climate reports and climate observing stations is available in *Climate Data Management System Specifications* (WMO-No. 1131), which is an attachment to this Guide.

PART VII. OPERATIONAL GUIDANCE

7.1 GENERAL

The *Manual on WIS* defines practices and procedures based on specific standards, defined in Part IV of the Manual, which are to be used by centres contributing to WIS. This part of the Guide contains information on the agreed operational practices that are considered to be stable and slow to change. Other guidance on agreed or recommended practices for WIS centres may be found at http://wis.wmo.int/WIS_Operations.

7.2 GISC SUPPORT TO NCS AND DCPCS

A GISC is expected to provide the following support to the centres (NCs and DCPCs) in its area of responsibility.

7.2.1 Operation coordination

7.2.1.1 Each GISC should organize regular meetings with the WIS National and WIS Centre Focal Points for those centres belonging to its Area Meteorological Data Communication Network (AMDCN), in order to coordinate the implementation, operation and improvement of the AMDCN and to ensure it meets WIS requirements.

7.2.1.2 Each GISC should maintain business continuity plans and handover arrangements to ensure continued service to the NCs and DCPCs in its area of responsibility, especially for the collection and distribution of data and products.

7.2.2 Technical support

7.2.2.1 Each GISC should provide technical consultation on implementing and improving WIS functionality, such as search and management of metadata, to the centres in its area of responsibility.

7.2.2.2 Each GISC should support the centres in its area of responsibility in creating and maintaining WIS discovery metadata, in adopting recommended data formats as well as in monitoring activities.

7.2.3 Capacity-building support

Each GISC should develop and provide training courses with reference to the WIS competencies and the WMO Information System Training and Learning Guide (Appendix A) to meet the capacity-development requirements of the centres in its area of responsibility.

7.3 GISC BACKUP PROCEDURES

The *Manual on WIS*, Part III, 3.5.9.2, requires GISCs to maintain arrangements with one or more backup GISCs that include, as a minimum, the collection and dissemination of information for its AMDCN to be taken up by another GISC in case of an incapacitating system failure.

Note: Responsibilities of the backup GISC are limited to the centres designated in the backup agreement with the GISC.

7.3.1 Backup services

7.3.1.1 Data collection and distribution must continue without interruption to and from centres in the area of the GISC being backed up. Where a centre's routine receipt of data is through subscription (e.g. GTS push), the backup GISC must have a current list of data to be sent to each centre or provide a place for the centres to come and get the data (e.g. GISC Cache).

7.3.1.2 Centres may be unable to change their GTS subscriptions during a period of back up operation, and any changes to subscriptions might not be maintained when normal operations resume.

7.3.1.3 Changes to metadata will not be possible during a backup period.

7.3.1.4 Any ad hoc changes made during a backup period may need to be redone after return to normal operations.

7.3.2 User information

7.3.2.1 If there is a need to exchange user information between GISCs in support of backup, proper security measures should be taken based on the agreement between the two GISCs. However, the centres concerned should ensure that the backup GISC has sufficient information for sending and collecting data from the centres being supported during a backup period.

7.3.2.2 Ad hoc changes to subscriptions, including additions or deletions of subscribers, should be avoided while in backup mode. Any ad hoc changes made during a backup period may need to be redone after return to normal operations.

7.3.3 Networks

Global Information System Centres need to ensure network connectivity to centres in the AMDCN of the GISC they are backing up. This may be through dedicated links, such as GTS, or over the Internet. Such connectivity should be in line with the *Guide to Information Technology Security* (WMO-No. 1115) and the *Guide to Virtual Private Networks (VPN) via the Internet between GTS centres* (WMO-No. 1116), as applicable.

7.4 PROCEDURES FOR CHANGING THE PRINCIPAL GISC

7.4.1 The principal GISC for each centre is listed in the *Manual on WIS*, Appendix B. The recommended procedure for NCs and DCPCs changing their principal GISC is provided in the annex to this paragraph (Appendix D).

7.4.2 Once notified that the new principal GISC is ready, the centre shall start using the WIS services of the new principal GISC, in particular the service of uploading and managing the WIS discovery metadata for its data and products.

7.5 GUIDELINES FOR MIGRATING WIS DISCOVERY METADATA RECORDS FROM ONE GISC TO ANOTHER

7.5.1 A corollary of the recommendations for the exchange of metadata, contained in the *Manual on WIS*, Part IV, 4.10, is that any NC or DCPC can upload its metadata records only to its principal GISC. Not applying this rule will lead to unnecessary duplication of WIS discovery metadata. The annex to this paragraph (Appendix D) describes the procedures that should be followed in the event of a centre changing its principal GISC.

7.5.2 The principles defined in the annex to paragraph 7.5.1 can also apply to a GISC providing temporary backup metadata management services to a centre’s principal GISC.

7.6 PROCEDURE FOR ROLLING REVIEW OF WIS CENTRES

7.6.1 The *Manual on WIS*, Part II, 2.2.4 and 2.3.4, define how Members hosting GISCs and DCPCs are required to demonstrate to CBS their ability to provide WIS services in compliance with GISC or DCPC functions and responsibilities.

7.6.2 The Commission for Basic Systems recognizes that for WIS to remain fully functional regular reviews of each NC, DCPC and GISC are required, ensuring their ongoing compliance with the *Manual on WIS*. Recommended practices for this rolling review are provided in the annex to this paragraph (Appendix D).

7.7 PROCURE FOR GISCS TO MANAGE THE EXCHANGE OF INFORMATION IN WIS BASED ON THE VALUE OF WMO_DISTRIBUTIONSCOPECODE IN THE METADATA RECORDING DESCRIBING THE INFORMATION TO BE EXCHANGED

7.7.1 WMO_DistributionScopeCode is used for indicating the distribution scope of the data published for exchange within WIS. The scope is defined as follows (see *Manual on the WMO Information System (*WMO-No. 1060), Appendix C , Part C2, Table 17):

(a) GlobalExchange: Data are published for global exchange via WIS. Data shall be incorporated into the GISC cache;

(b) RegionalExchange: Data are published for regional exchange via a GISC;

(c) OriginatingCentre: Data are published for exchange directly via the originating centre.

7.7.2 The value of WMO_DistributionScopeCode is set by the information provider as the only entity permitted to modify its WIS discovery metadata record.

7.7.2.1 Members are encouraged to use the value “GlobalExchange” for most of the information intended for near-real-time exchange.

7.7.2.2 Providers of large information streams, such as high-resolution imagery, high-resolution numerical weather prediction files or radar data, should consider using either the value “RegionalExchange” or the value “OriginatingCentre” in order to limit the impacton telecommunications circuits of distributing large volumes of data in near-real-time to a broad spectrum of users.

7.7.3 The principal GISC of the information provider should, at the time of initial entry of the metadata record into the WIS metadata catalogue, monitor the volume and frequency of the information as they have an impact on the requirements for telecommunications bandwidth for exchange and on the size of the cache in GISC. If either this estimate, or the information exchanges observed by at least one GISC, is considered to be exceptional or to place excessive load on the WIS infrastructure, the principal GISC should discuss with the information provider whether it is necessary to exchange all the information routinely.

7.7.4 If the information provider is confident that the transfer is appropriate, the principal GISC should check with other GISCs that they accept near-real-time exchange of this new information.

7.7.5 If the information provider and the GISCs are unable to reach consensus on the exchange of the information, the matter should be referred to the constituent body working group that has been designated to resolve issues concerning WIS. The working group should report its conclusions to the constituent body responsible for the WIS.

Note: In 2018, the Commission for Basic Systems was responsible for WIS and it had designated the Inter-Commission Task Team on the WMO Information System as the working group responsible for resolving WIS-related issues.

7.8 MANAGING OPERATIONAL OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

Correct and reliable operation of Information and Communications Technology (ICT) is critical to many services provided by Members. Guidance on recommended practices in managing operations of ICT is provided in Appendix E to this Guide.

7.9 WIS IT SECURITY INCIDENT RESPONSE PROCESS

The WIS IT security incident response process is defined in Appendix F.

PART VIII. MONITORING OF WIS

8.1 Monitoring of WIS is intended to improve the exchange of information by WMO Programmes and to ensure that the functions of WIS centres minimize the cost of operating WIS. It is also essential for planning and scaling WIS components in order to meet changing user needs. It complements monitoring of quality of the information being exchanged, which is the responsibility of the Programmes sponsoring the information within WIS.

8.2 Management of WIS needs three types of monitoring to answer four different questions:

(a) How do we exchange information?

(b) How much information do we exchange?

(c) How well do we meet the expected standards for information exchange?

(d) How does the performance of a WIS component affect the performance and cost effectiveness of WIS?

8.3 WIS network monitoring seeks to address the first question: How do we exchange information and is the method used cost effective? It concentrates on determining the ability of the information and communication technology (ICT) systems underlying WIS to meet their performance targets. System managers of WIS centres will use this type of monitoring to identify problems in real time in addition to using analyses of the monitoring to report performance against Service Level Agreements. This will also identify weaknesses in WIS communication systems and detect changes in usage patterns for planning purposes.

8.4 WIS quantitative monitoring seeks to address the second question: How much information do we exchange and is it exchanged as required? This type of monitoring compares the information available at WIS centres with the information that should be available. Managers of WMO Programmes will use this type of monitoring to verify that the information they need is being transferred by the WIS, and system managers of WIS centres will use the information to identify issues with data flows due to the way WIS is being used rather than to underlying ICT infrastructure problems that are identified by WIS network monitoring.

8.5 WIS qualitative monitoring seeks to address the third question: Do we meet the expected standards for information exchange? It also addresses the fourth question about the effectiveness of WIS, on the basis of users' subjective assessments, in particular users' satisfaction with the services and performance of WIS. This monitoring is primarily concerned with the quality of representation of the information being exchanged. Managers of WMO Programmes will use this type of monitoring to determine whether the processes used to create and discover the information are producing outputs that are of the expected standard. Details of WIS qualitative monitoring differ between information types and WMO Programmes, and its principles and practices are described in the Manuals and Guides and in technical documents of the WMO Programmes responsible for the information content. WMO Programmes are also responsible for monitoring the quality of the data and information being exchanged; this is not included in the WIS qualitative monitoring.

8.6 Information to support the network and quantitative monitoring of WIS shall be exchanged using files in JSON format as specified at https://wis.wmo.int/WIS-Monitor-JSON. The files are used to create a summary overview of the status of WIS known as the "WIS Common Dashboard". All GISCs shall provide the files.

8.7 GISCs shall collaboratively deliver the “GISC Watch” operational monitoring of WIS as described in the Annex to this paragraph in Appendix D.

APPENDIX A. WMO INFORMATION SYSTEM TRAINING AND LEARNING GUIDE

1. INTRODUCTION

1.1 This guide is designed to assist trainers in the development and running of training courses for WIS personnel and to show learners what is expected of them. As this is a guide, it is not mandatory to follow its directions precisely. There may be more appropriate ways to teach or learn something. However, it is essential that the learning outcomes are met.

1.2 This guide is not a syllabus. A syllabus is essentially a list of topics without indications of learning outcomes or how the learning is to be demonstrated. With a competency-based approach, the focus is on learners acquiring and demonstrating the required competencies.

1.3 This guide covers the whole gamut of competencies required of people working with WIS. It is important to note that these are the competencies required in a large WIS centre where they would normally be shared across a number of staff. Although different WIS centres may require the same competencies, the components, complexity and depth of each may vary. Furthermore, an individual competency or component may not be required at a particular centre (if the corresponding task is not performed there) or by all individuals within the centre.

1.4 Thus, the training should be tailored to each individual's needs. These learning needs will depend on what is required of staff to perform their work and what competencies and skills they already possess (recognition of prior competence). Training should fill these gaps, not cover all of the possible content.

1.5 It is possible that not all of the competencies are required in a small centre. In any case, each individual working with WIS has to show competence in performing the tasks required of them. Where staff already possess the necessary skills and are able to demonstrate competence against the assessment criteria they will be exempt from the corresponding sections of the training course.

2. IN AND OUT OF SCOPE

Staff are expected to have standard professional skills and capabilities. The emphasis here is on WIS specific skills. Training in generic skills such as using information and communication technology (ICT) systems and standard applications, networking, carrying out maintenance, using databases and managing projects would normally be outsourced or be part of a person's training prior to working in the centre. The same applies to team work and generic management skills.

3. ASSESSMENT

3.1 It is essential to ensure that learning is transferred from the learning environment to operations. Assessment should thus simulate the operational conditions as closely as practicable. The emphasis is on what people are able to do, under the conditions in which they are required to do it, and with the tools they would normally use, rather than on what they know.

3.2 Examples of suitable assessment types include:

(a) Demonstrated performance;

(b) Portfolio of examples of work they have done;

(c) Recognition of prior competence;

(d) Evaluation of supervisor certifying their competencies, based on evidence of prior performance or work under supervision.

3.3 As competencies need to be maintained on an ongoing basis, continuing assessment may be required. This would normally be on a periodic basis at a frequency appropriate for the particular competency.

3.4 Competency-based assessment means that staff are deemed capable of performing the job, not that they receive a pass mark of say 60%.

4. TYPES OF TRAINING

4.1 This document is not meant to prescribe how training should be performed but to offer some suggestions. Any mode of training is acceptable, as long as it is effective and the outcomes can be assessed against the required competencies; hence it will depend on the competency to be assessed, the size of the WIS centre, available resources and other factors.

4.2 Forms of training include:

(a) Working under supervision (on the job);

(b) Mentoring;

(c) Self-directed study;

(d) Internal or external courses (online or classroom), especially for generic skills;

(e) Scenario-based activities, including use cases;

(f) Role plays, especially for external interactions.

5. KEY LEARNING RESOURCES

The key publications, along with their references, explaining the operation of WIS are:

(a) *Manual on the WMO Information System* (WMO-No. 1060);

(b) *Guide to the WMO Information System* (WMO-No. 1061).

6. UPDATING OF THE GUIDE

As the training for WIS evolves it is expected that this guide will evolve with it. Suggestions about ways to improve this document and ideas about how the training can be conducted are always welcome and should be sent to: wis-help@wmo.int.

7. COMPETENCIES

Seven competencies across four basic functional areas have been identified as follows:

Infrastructure

1. Manage the physical infrastructure

2. Manage the operational applications

Data

3. Manage the data flow

4. Manage data discovery

External interactions

5. Manage interaction among WIS centres

6. Manage external user interactions

Overall service

7. Manage the operational service

COMPETENCY 1: MANAGE THE PHYSICAL INFRASTRUCTURE

Competency description

Prepare, plan, design, procure, implement and operate the physical infrastructure, networks and applications required to support the WIS centre.

Many of the skills required here are generic ICT skills and will have already been acquired as part of prior education and training or will be provided by hardware and system suppliers.

Performance components

Management of information technology operations

1a. Maintain the system in optimal operational condition by setting and meeting service levels, including:

- Configuration;
- Preventative and corrective maintenance and servicing;
- Equipment replacement or upgrade;
- Networking and processing capacity;
- System monitoring and reporting procedures, and corrective actions;

1b. Provide contingency planning and operation backup and restoration;

Management of facilities

1c. Manage physical site security;

1d. Manage physical site environmental control.

Knowledge and skill requirements

- General ICT skills;
- Operation, configuration and maintenance of equipment and applications;
- Recognized information technology service management frameworks;
- Current technologies and emerging trends;
- Service level agreements.

Learning outcomes

Staff will be able to:

- Maintain the system in optimal operational condition;
- Plan for upgrades and operation backup and restoration;
- Maintain site security and environmental control.

Staff will learn:

- WIS specific systems;
- WIS site security policies;
- Service level agreements for the centre.

Learning activities

To learn how to perform the required tasks staff may:

- Attend training sessions run by providers of systems and other tools or by other training providers;
- Respond to typical monitoring reports;
- Apply WIS site security measures and respond to typical incidents;
- Apply WIS site environmental control measures and respond to typical incidents.

Assessment

Staff must be able to:

- Configure and maintain system components;
- Respond to monitoring reports;

- Apply WIS site security measures and respond to typical incidents;
- Apply WIS site environmental control measures and respond to typical incidents.

Key learning resources

- Manufacturers' handbooks and guides;
- Documentation of centre's facilities;
- WIS/GTS manuals and guides;
- Tools to monitor system security;
- WIS security policies;
- WIS environmental control policies.

COMPETENCY 2: MANAGE THE OPERATIONAL APPLICATIONS

Competency description

Prepare, plan, design, procure, implement and operate the applications required to support the WIS functions.

Many of the skills required here are generic ICT skills and will have already been acquired as part of prior education and training or will be provided by suppliers of applications.

Performance components

2a. Meet service levels by maintaining applications in optimal operational condition through:

- Configuration of applications;
- Monitoring and responding to applications' behaviour;
- Preventative and corrective maintenance;
- Replacement or upgrade of applications;

2b. Provide contingency planning and application backup and restoration;

2c. Ensure data integrity and completeness in the event of system failure;

2d. Ensure system security.

Knowledge and skill requirements

- General ICT skills;
- Operation, configuration and maintenance of applications;
- Recognized information technology service management frameworks;

- Current technologies and emerging trends;
- WIS functions and requirements;
- WIS security policies.

Learning outcomes

Staff will be able to:

- Operate, configure and maintain applications;
- Monitor applications and take corrective action;
- Apply and test WIS security protocols.

Staff will learn:

- WIS applications specific to the centre;
- WIS system security policies and procedures.

Learning activities

To learn how to perform the required tasks staff may:

- Attend training sessions run by providers of systems and other tools or by other training providers;
- Initiate monitoring and reporting procedures and respond to typical monitoring reports;
- Apply WIS site security measures and respond to typical incidents.

Assessment

Staff must be able to:

- Configure and maintain system components;
- Respond to monitoring reports;
- Apply site security measures and respond to typical incidents.

Key learning resources

- Documentation of centre's applications;
- WIS/GTS manuals and guides;
- Tools to monitor system security;
- WIS security policies.

COMPETENCY 3: MANAGE THE DATA FLOW

Competency description

Manage the collection, processing and distribution of data and products through scheduled and on-demand services.

Performance components

3a. Ensure collection and distribution of data and products as per data policy;

3b. Publish data and products;

3c. Subscribe to data and products;

3d. Encode, decode, validate and package data and products;

3e. Create, update and maintain data flow catalogues;

3f. Manage connectivity between centres;

3g. Control the data flow to meet service levels.

Knowledge and skill requirements

- System and network monitoring and viewing tools;
- Data formats and protocols;
- Licensing and data policies;
- Message and file switching systems.

Learning outcomes

Staff will be able to:

- Transfer data and products between their centre, other WIS centres and external users;
- Request data and respond to data requests using ad hoc and routine delivery mechanisms;
- Maintain quality standards (service levels) by monitoring, and responding to, traffic flow, missing data and products, errors and service messages;
- Apply relevant data policies to data and products;
- Identify appropriate formats for data and product exchange;
- Write and read data in WIS formats using their centre’s tools.

Staff will learn:

- Data representations used in WIS and when to apply them;
- WMO data policies and how they apply to data in WIS;

- The structure of the WIS and GTS and how to use reference documents to identify and interpret the routing plans and protocols they will need to use;
- The interfaces of their centre's WIS applications, the information they use to modify their behaviour, and the tools available to control the operation of the applications to achieve service levels;
- How to use a WIS centre interface to find and request data for delivery by ad hoc request and by subscription;
- How WIS handles backup and how GTS handles alternative routings to maintain continuity of data flows.

Learning activities

To learn how to perform the required tasks staff may:

- Connect to a WIS centre to search for information, select a dataset and download a copy from the cache;
- Using a WIS centre interface, create, modify and delete a subscription for routine delivery of a dataset;
- Use the software tools of their centre's WIS application to exchange information between computers;
- Assess data flows by analysing monitoring reports from their applications;
- Investigate how data policy (including WMO Resolutions 40 (Cg-XII) and 25 (Cg-XIII)) is applied to data published by their centre;
- Use tools provided at their centre to view information in different formats and convert data between these formats.

Assessment

Staff must be able to:

- Go to a WIS centre, find data, download them immediately, subscribe for regular delivery and cancel the subscription;
- Use a GTS switch to move data between training computers and control the flow.

Key learning resources

Data policies

- Resolution 40 (Cg-XII) – WMO policy and practice for the exchange of meteorological and related data and products including guidelines on the relationships in commercial meteorological activities;
- Resolution 25 (Cg-XIII) – Exchange of hydrological data and products;
- Resolution 60 (Cg-17) – WMO policy for the international exchange of climate data and products to support the implementation of the Global Framework for Climate Services;
- The centre's data policies.

GTS data exchange

Manual on the Global Telecommunication System (WMO-No. 386), Attachments II-5, II-6, II-7, II-15 and II-16.

Data representations

- *Manual on Codes* (WMO-No. 306), Volume I.1; Volume I.2 and Volume I.3;
- Guidance on migration to table driven code forms available at http://www.wmo.int/pages/prog/www/WMOCodes.html;
- Tools used at the centre to read, write, convert, validate and display information in Table Driven Code Forms;
- Sample data for reading and writing in Table Driven Code Forms.

WIS discovery, access and retrieval

- *Manual on the WMO Information System* (WMO-No. 1060), Part I, 1.7 and Appendix D (WIS-TechSpec-2, -10, -11 and -12);
- *Guide to the WMO Information System* (WMO-No. 1061);
- User account at a GISC and PC with Internet connection.

Managing GTS data exchange

- *Manual on the Global Telecommunication System* (WMO-No. 386);
- *Weather Reporting* (WMO-No. 9), Volume C1;
- Global Telecommunication System routing tables;
- Training environment on message and file switch;
- World Weather Watch quantity monitoring statistics.

Security of data exchange

- *Guide to Virtual Private Networks (VPN) via the Internet between GTS centres* (WMO-No. 1116);
- *Guide to Information Technology Security* (WMO-No. 1115).

Network management

- Network management tool and associated documentation;
- System error reports and event viewing tools.

COMPETENCY 4: MANAGE DATA DISCOVERY

Competency description

Create and maintain discovery metadata records describing services and information, and upload them to the WIS Discovery Metadata Catalogue.

Each datum and product record held within WIS must have metadata associated with it so that it can be found and understood. These metadata records are held in a catalogue for discovery, access and retrieval (DAR).

Performance components

4a. Create and maintain discovery metadata records describing products and services;

4b. Add, replace or delete metadata records within the catalogue;

4c. Ensure that all information and service offerings from a WIS centre have complete, valid and meaningful discovery metadata records uploaded to the catalogue.

Knowledge and skill requirements

- Knowledge of WMO and ISO documentation sufficient to create complete and valid metadata;
- Metadata entry and management tools;
- Policies;
- Discovery metadata concepts and formats;
- Written English.

Learning outcomes

Staff will be able to:

- Use standard WIS tools to create discovery metadata from descriptions supplied by users;
- Add, replace or delete metadata records within the catalogue.

Staff will learn:

- The role of metadata in discovery, access and retrieval of data and products;
- Approved metadata formats;
- How to identify content that is mandatory, acceptable or inapplicable;
- Use of metadata creation tools;
- How to access and modify a catalogue;
- How data flow within, to and from their centre;
- About the tools that allow users to input descriptions.

Learning activities

To learn how to perform the required tasks staff may:

- Create metadata records based on sample descriptions for a range of data and products typical of their WIS centre;
- Insert such records into a catalogue, replace them with records that have been changed and delete them.

Assessment

Staff must be able to demonstrate:

- Successful creation of metadata records for typical products;
- Competence in publishing and deleting metadata catalogue records.

Key learning resources

- *Manual on the WMO Information System* (WMO-No. 1060), Part IV, 4.10, and Appendix D (WIS-TechSpec-9), and Part V and Appendix C;
- WIS metadata guidance;
- Metadata entry and management tools;
- Samples of how to complete typical metadata records;
- Metadata policies and WIS metadata guidelines;
- ISO 19100 series: ISO standards on geographic information.

COMPETENCY 5: MANAGE INTERACTION AMONG WIS CENTRES

Competency description

Manage relationships and compliance between the participants' centre and other WIS centres.

Performance components

5a. Exchange information with other centres on operational matters;

5b. Facilitate registration of new WIS centres;

5c. Facilitate registration of new data and products by other WIS centres;

5d. Create and respond to WIS service messages, including GTS.

Knowledge and skill requirements

- Knowledge of current exchanges and requirements for notification of operational changes;

- Procedures and practices for registration of other centres and their data and products;
- Service level agreements;
- Written English.

Learning outcomes

Staff will be able to:

- Facilitate registration of new WIS centres and their data and products;
- Keep other WIS centres informed of the status of services, incidents and requests;
- Monitor and respond to service level reports;
- Manage subscriptions.

Staff will learn:

- About current exchanges and requirements for notification of operational changes;
- What type of data, products and services are available at their centre;
- Procedures and practices for registration of other centres and their data and products;
- Procedures and practices for notifying other centres about operational changes and service availability.

Learning activities

To learn how to perform the required tasks staff may carry out the above activities with the help of software, tools and guidance as used in their operational environment, either in a classroom or under supervision on the job.

Assessment

Staff must be able to:

- Respond to a request for registration of a new centre and its data and products;
- Prepare notifications of typical operational scenarios;
- Respond to typical notifications from other WIS centres.

Key learning resources

- *Manual on the Global Telecommunication System* (WMO-No. 386);
- *Manual on the WMO Information System* (WMO-No. 1060), Part II; Part IV, 4.5, 4.7, 4.8, 4.9 and 4.14, and Appendix D (WIS-TechSpec- 4, - 6, - 7, - 8 and - 13);
- *Guide to the WMO Information System* (WMO-No. 1061);
- *Weather Reporting* (WMO-No. 9), Volume C1;

- *Exchanging Meteorological Data: Guidelines on Relationships in Commercial Meteorological Activities – WMO Policy and Practice* (WMO No. 837).

Local resources

- Service level agreements (as used by the participants' centre);
- Frequently Asked Questions (FAQ) documents (for the user);
- WIS software user guides;
- Guidelines for services available at WIS centre;
- Data policy and associated guidance material;
- First-line support procedures and guides;
- User database (for contact information);
- Case tracking and customer management;
- WIS user management;
- WIS subscription management;
- Monitoring dashboard for WIS components.

COMPETENCY 6: MANAGE EXTERNAL USER INTERACTIONS

Competency description

Ensure that users, including other centres, data providers and subscribers, can publish and access data and products through WIS.

Performance components

6a. Register data providers and subscribers and maintain a service agreement;

6b. Set and register access criteria;

6c. Provide systems and support for users to publish and access data and products;

6d. Manage user relations to ensure a high satisfaction level.

Knowledge and skill requirements

- Data policies;
- External WIS interface;
- WIS registration and monitoring tools and policies;
- User support documentation and help files;

- Written English.

Learning outcomes

Staff will be able to:

- Register new WIS users and providers, setting roles, access authorizations and levels;
- Create and amend WIS user subscriptions;
- Use WIS tools to assist users and providers in resolving problems;
- Create and respond to WIS service messages, including GTS;
- Undertake first-line investigation and diagnosis;
- Manage incidents and requests: log them, categorize and prioritize them, escalate as appropriate and close them when the user is satisfied;
- Keep users informed of the status of services, incidents and requests;
- Gather information and report on user and provider satisfaction;
- Assist users in uploading and accessing data;
- Identify potential problems in services and implement improvements.

Staff will learn:

- What type of data, products and services are available at their centre;
- How WIS applications, including discovery, access and retrieval (DAR) should be used;
- How to apply data policies;
- How to interact effectively with users and providers.

Learning activities

To learn how to perform the required tasks staff may:

- Register users (data providers and subscribers) and set access authorizations and levels using the same software, tools and guidance as in their operational environment;
- Role play user interactions.

Assessment

Staff must be able to:

- Register typical data providers and users;
- Ensure that users are able to upload and access data;
- Respond to typical incidents.

Key learning resources

- *Manual on the Global Telecommunication System* (WMO-No. 386);

- *Manual on the WMO Information System* (WMO-No. 1060), Part II; Part IV, 4.5, 4.7, 4.8, 4.9 and 4.14, and Appendix D (WIS-TechSpec-4, -6, -7, -8 and -13);

- *Guide to the WMO Information System* (WMO-No. 1061);

- *Weather Reporting* (WMO-No. 9), Volume C1;

- *Exchanging Meteorological Data: Guidelines on Relationships in Commercial Meteorological Activities – WMO Policy and Practice* (WMO-No. 837).

Local resources

- Service level agreements (as used by their centre);

- FAQ documents (for the user);

- WIS software user guides;

- Guidelines for services available at WIS centre;

- Data policy and associated guidance material;

- First-line support procedures and guides;

- User database (for contact information);

- Case tracking and customer management;

- WIS user management;

- WIS subscription management;

- Monitoring dashboard for WIS components.

COMPETENCY 7: MANAGE THE OPERATIONAL SERVICE

Competency description

Ensure the quality and continuity of the service.

This is essentially a management role ensuring that the WIS system operates as required, now and in the future. Some of the skills required are generic management skills, rather than WIS specific, and would be taught or learnt elsewhere.

Performance components

7a. Coordinate all WIS functions and activities of the centre;

7b. Ensure and demonstrate compliance with regulations and policies;

7c. Monitor and meet quality and service performance standards;

7d. Ensure service continuity through risk management and planning and implementation of service contingency, backup and restoration. Ensure data continuity in the event of system failure;

7e. Plan and coordinate the delivery of new functionalities.

Knowledge and skill requirements

- General management skills;
- Overview of local and external WIS operations and associated service agreements;
- WIS regulations and policies;
- Functional specifications;
- Written English.

Learning outcomes

Staff will be able to:

- Ensure that the WIS centre meets quality and service performance standards;
- Identify the challenges and issues to be addressed;
- Foster compliance with WIS framework.

Staff will learn:

- Functions and responsibilities of the WIS centre;
- WIS quality and service performance standards;
- Methods to manage quality, risk and operational service;
- How to monitor quality and service performance standards;
- How to analyse, demonstrate and report quality and service performance at the WIS centre;
- How to maintain troubleshooting, backup and restoration procedures;
- How to plan and coordinate the delivery of new functionalities and improvements;
- How to integrate new technologies and developments;
- How to update the regulatory documents;
- How to maintain service agreements;
- How to plan monitoring resources;
- How to align budget restrictions with human resources demands.

Learning activities

To learn how to perform the required tasks staff may:

- Monitor quality and service performance standards;
- Analyse quality and service performance in the WIS centre;
- Demonstrate and report quality and service performance;
- Maintain troubleshooting, backup and restoration procedures;
- Plan and coordinate the delivery of new functionalities;
- Keep timely records, as required.

Assessment

Staff must be able to:

- Demonstrate successful WIS service;
- Plan replacement and upgrade of equipment and applications to meet new functionalities and requirements.

Key learning resources

- *Technical Regulations* (WMO-No. 49), Volume I;
- Resolution 40 (Cg-XII) – WMO policy and practice for the exchange of meteorological and related data and products including guidelines on the relationships in commercial meteorological activities;
- Resolution 25 (Cg-XIII) – Exchange of hydrological data and products;
- Resolution 60 (Cg-17) – WMO policy for the international exchange of climate data and products to support the implementation of the Global Framework for Climate Services;
- *Manual on the Global Telecommunication System* (WMO-No. 386);
- *Manual on the WMO Information System* (WMO-No. 1060), Part IV, 4.16, WIS-TechSpec-15;
- *Guide to the WMO Information System* (WMO-No. 1061);
- WIS demonstration procedures and guidelines;
- Monitoring reports;
- Audit reports.

APPENDIX B. WIS TECHNICAL SPECIFICATIONS – USE CASES

General

1. This appendix provides the use cases for major WIS functions relating to the WIS Technical Specifications as described in the *Manual on the WMO Information System* (WMO-No. 1060), Part IV. Use cases are designed to help system developers understand how the system is supposed to operate, given certain preconditions and reactions to decisions during processing.

2. The content of most of the use cases given in this appendix follows closely the work of the SIMDAT project led by the European Centre for Medium-Range Weather Forecasting. The form of the use cases follows the general guidance of the Unified Modelling Language (UML). It also uses a specific template derived from an example published by Karl E. Wiegers (with permission granted to use, modify and distribute the template).

3. Table 2 provides a key to the elements of the Use Case template as used herein.

Table 2. Key to elements in the Use Case template

Use Case goal	A brief description of the reason for and outcome of the Use Case, or a high-level description of the sequence of actions and the outcome of executing the Use Case.
Actors	An actor is a person or other entity, external to the system under consideration, that interacts with the system: the person or entity that will be initiating the Use Case or will participate in completing it. Different actors often correspond to different users or roles, selected from the customer community that will use the product.
Trigger	An event that initiates the Use Case such as an external business event, a system event or the first step in the normal flow.
Preconditions	Activities that must take place, or any conditions that must be true, before the Use Case can be started.
Post-conditions	The state of the system once the Use Case has been completed.
Normal flow	Detailed description of the user actions and system responses during execution of the Use Case under normal, expected conditions. This dialogue sequence will ultimately lead to the accomplishment of the goal stated in the Use Case name and description.
Alternative flows	Other, legitimate usage scenarios that can take place within the Use Case under consideration.
Exceptions	Anticipated error conditions that could occur during execution of the Use Case, and how the system is to respond to those conditions; the Use Case execution fails for some reason.
Includes	Other Use Cases that are included ("called") by the Use Case being described (this is to avoid repeating the text of those use cases that are subsets of several other use cases with common functionality).
Notes and issues	Additional comments about the Use Case and any remaining open issues that must be resolved. It is useful to identify who will resolve each such issue and by what date.

Note: The DAR Metadata Catalogue holds WIS Discovery Metadata records.

Use Case B.1 – Providing metadata for data or products

Use Case goal	Metadata for any data or products provided by the DCPC or GISC are entered or updated in the DAR Metadata Catalogue of the DCPC or GISC.
Actors	Metadata originator (NC or DCPC) and metadata catalogue publisher (DCPC or GISC)

Preconditions	(1) The metadata originator is authorized to update the DAR Metadata Catalogue for the associated file(s); (2) The metadata originator has the necessary information and the ability to update the DAR Metadata Catalogue for the associated file(s); (3) The metadata catalogue publisher supports facilities for authorized metadata originators to update the metadata for the associated file(s).
Post-conditions	The DAR Metadata Catalogue has changes made by the metadata originator.
Normal flow	The authorized metadata originator uses a facility supported by the metadata catalogue publisher to update the DAR Metadata Catalogue for the associated file. Typically, two kinds of maintenance facilities are supported:(a) a file upload facility for "batch" updating (adding, replacing or deleting metadata records treated as separate files); and (b) an online form for changing metadata records treated as entries in the DAR Metadata Catalogue (adding, changing or deleting elements in a record as well as whole records). The metadata catalogue publisher maintains the updated DAR Metadata Catalogue as a searchable resource offered to all authorized searchers (see Use Case B.6). The metadata catalogue publisher also shares the metadata as part of the logically centralized but physically distributed catalogue across WIS centres.
Notes and issues	This set of actions is a simple extrapolation from existing GTS practice, adding the particular standard format for WIS metadata.
Last updated	30 June 2014
Last updated by	WMO Secretariat

Use Case B.2 – Uploading data or products to DCPC or GISC

Use Case goal	Data or products are sent as files to a DCPC or GISC.
Actors	Data sender (NC or DCPC) and data receiver (DCPC or GISC)
Preconditions	(1) Appropriate metadata to be associated with the file is already available in the DAR Metadata Catalogue of the DCPC or GISC (if not, see Use Case B.3); (2) The data sender is authorized to send the files to the data receiver; (3) The data receiver supports a method for uploading the files, which the data sender is able to use.
Post-conditions	The data or products uploaded by the data sender are received and stored by the data receiver.
Normal flow	The data sender uses his authorized access to send the files using an appropriate transmission method supported by the data receiver. Typically, the transmission is accomplished using GTS or a file transfer method available over the Internet. A file naming convention or other agreed mechanism is used to make an association between the file and its metadata.
Notes and issues	This set of actions builds on existing GTS practice, supplemented with other file transfer mechanisms such as the Internet.
Last updated	30 June 2014
Last updated by	WMO Secretariat

Use Case B.3 – Controlling metadata association to data or products

Use Case goal	To confirm that metadata for a datum or product file at the DCPC or GISC already exists in the DAR Metadata Catalogue before the data or products are available.
Actors	Data sender (NC or DCPC) and data receiver (DCPC or GISC)
Preconditions	(1) Datum or product has been sent as a file from a data sender (Use Case B.1); (2) DAR Metadata Catalogue includes all updates (Use Case B.2).
Post-conditions	An error is reported when there is no confirmation that a given file is associated correctly with its metadata in the DAR Metadata Catalogue.

Normal flow	On receipt of a file containing a datum or product, the data receiver checks the current DAR Metadata Catalogue to confirm that the file has an associated metadata record. If such a record is not found within two minutes of receipt of the file, an error message is sent to the data sender.
Notes and issues	This control action addresses the situation wherein data arrives before its associated metadata. Rather than rejecting the file immediately, a grace period of two minutes is allowed before the data file is regarded as erroneous.
Last updated	30 June 2014
Last updated by	WMO Secretariat

Use Case B.4 – Managing cache of data across GISCs

Use Case goal	GISCs manage a logically centralized collection containing at least a 24-hour cache of data and products agreed by WMO for routine global exchange.
Actors	Data administrators at each of the GISCs
Preconditions	(1) At each GISC, the cache of data and products received from NCs and DCPCs in its area of responsibility is up to date; (2) Transmission and control mechanisms across GISCs are available; (3) All data administrators are authenticated and authorized as needed.
Post-conditions	The cache of data and products is accessible as a logically centralized collection that includes current data and products at each GISC.
Normal flow	A data administrator monitors the transmission methods and control mechanisms that enable a logically centralized view of the physically distributed cache of data and products. Depending on the methods in place, a data administrator takes various corrective actions whenever the cache is not available as required.
Notes and issues	At this point in WIS system design, it has not been decided how the GISCs will accomplish centralization of the cache.
Last updated	30 June 2014
Last updated by	WMO Secretariat

Use Case B.5 – Maintaining identification and role information for WIS users

Use Case goal	Internal and external users of WIS can be identified for their authentication, and their role information is maintained as needed so that they can be authorized to perform specific functions.
Actors	Internal and external users of WIS and people in charge of authentication and authorization at WIS centres.
Preconditions	(1) Administrators have agreed authentication policies delineating the credentials required to establish identity of a WIS user; (2) Administrators have agreed authorization policies delineating which roles are authorized to perform each WIS action; (3) Administrators have mechanisms to create and maintain the identification information needed for authentication of users of WIS; (4) Administrators have mechanisms to create and maintain the role information needed for authorization of authenticated users of WIS.
Post-conditions	WIS centres collectively have the ability to authenticate each user of WIS and authorize them to perform all of the functions appropriate to their role, and only those functions.
Normal flow	Identification and role information about candidate or current users of WIS is to be recorded through facilities controlled by WIS centres. Typically, two kinds of facilities should be supported: (a) a file upload facility for "batch" updating (adding, replacing or deleting the identification and role records as separate files); and (b). an online form for changing identification and role records (adding, changing or deleting elements in a record as well as whole records). Administrators of authentication and authorization at WIS centres share the updated identification and role information as a resource available as needed across WIS centres.

Notes and issues	At this point in WIS system design, it has not yet been decided which mechanisms will be used for handling identification and role information as needed across WIS centres.
Last updated	30 June 2014
Last updated by	WMO Secretariat

Use Case B.6 – Discovering data or products

Use Case goal	A user of WIS finds available WMO data or products that he wants to receive.
Actors	Data searcher
Preconditions	(1) The DAR Metadata Catalogue is accessible for browsing or searching; (2) The GISC infrastructure provides a unified catalogue view to the user (i.e. the catalogue is logically centralized although physically distributed).
Post-conditions	The data searcher has the information needed to select relevant data or products.
Normal flow	The data searcher discovers available WMO data and products by browsing the DAR Metadata Catalogue or by searching it using discovery concepts such as subject keywords, geographic extent and temporal range. As a result of browsing or searching, the data searcher gets a relevance-ordered list of data and products including data or product metadata such as data origin, data type, generation date, availability and use constraints.
Notes and issues	At this point in WIS system design, multiple methods can be envisioned for logically centralizing the physically distributed DAR Metadata Catalogue.
Last updated	30 June 2014
Last updated by	WMO Secretariat

Use Case B.7 – Ad hoc request for data or products ("pull")

Use Case goal	A user of WIS requests WMO data or products on an ad hoc basis.
Actors	User of WIS centres
Preconditions	(1) The desired data or products have been identified by the user of WIS; (2) The user of WIS has been authenticated and authorized to retrieve the desired data or products from the WIS centre; (3) Delivery uses one of the supported mechanisms for the transmission of the desired data or products, within the published service level commitment of the WIS centre.
Post-conditions	Data or products are readied for delivery to the user of WIS according to the service level commitment of the WIS centre.
Normal flow	Once the user has identified the desired data or products, he/she requests delivery on a one-time basis (Use Case B.8 covers the alternate choice, recurring delivery). The WIS centre authenticates the user and checks authorization for delivery of the products according to the user's role. The WIS centre then sets up delivery through any of a broad range of online and offline options (delivery options are described in Use Case B.9).
Last updated	30 June 2014
Last updated by	WMO Secretariat

Use Case B.8 – Subscribing to data or products ("push")

Use Case goal	A user of WIS can subscribe to receive data or products on a recurring basis.
Actors	User of WIS centre

Preconditions	(1) The desired data or products have been identified by the user of WIS; (2) The user of WIS has been authenticated and authorized to retrieve the desired data or products from the WIS centre; (3) Delivery is achievable through one of the supported mechanisms for the transmission of the desired data or products, within the published service level commitment of the WIS centre.
Post-conditions	Data or products are readied for delivery to the user of WIS according to the service level commitment of the WIS centre.
Normal flow	Once the user has identified the desired data or products, he/she requests a subscription to receive the data or products on a recurring basis (Use Case B.7 covers the alternate choice, one-time delivery). The WIS centre authenticates the user and checks authorization for delivery of the product according to the user's role. The WIS centre then sets up delivery through any of a broad range of online and offline options (described in Use Case B.9). As necessary, the WIS centre updates the dissemination metadata associated with the subscription (Use Case B.10).
Last updated	30 June 2014
Last updated by	WMO Secretariat

Use Case B.9 – Downloading data or products from a WIS centre

Use Case goal	A user of WIS receives from a WIS centre, on an ad hoc or subscription basis, data or products transmitted as files.
Actors	User of WIS and WIS centre
Preconditions	(1) Data or products are ready for delivery to the authenticated and authorized user, as requested through one of the supported transmission mechanisms, according to the service level commitment of the WIS centre; (2) For subscription delivery, the WIS centre has access to subscription information in the Dissemination Metadata Catalogue (see Use Case B.10).
Post-conditions	Selected data or products are received by the user of WIS.
Normal flow	The WIS centre sends files containing the requested data or products, using an appropriate transmission method, as indicated in the associated subscription information accessible through the Dissemination Metadata Catalogue. Typically, the transmission is accomplished using GTS or a file transfer method available over the Internet, such as HTTP, OpenDap, FTP, SFTP, GFTP and e-mail). In any case, transmission must be efficient and reliable (checksum and error recovery mechanisms are required as a minimum).
Last updated	30 June 2014
Last updated by	WMO Secretariat

Use Case B.10 – Providing dissemination metadata

Use Case goal	Metadata concerning delivery specifics of subscription(s) to data and products from a DCPC or GISC are created or updated in the Dissemination Metadata Catalogue.
Actors	The subscription registrar (NC or DCPC) and dissemination catalogue publisher (DCPC or GISC)
Preconditions	(1) The subscription registrar is authorized to update the Dissemination Metadata Catalogue for the given subscription(s); (2) The subscription registrar has the necessary information and the ability to update the Dissemination Metadata Catalogue for the given subscription(s); (3) The dissemination catalogue publisher supports facilities for authorized subscription registrars to update the metadata for the given subscription(s).
Post-conditions	The Dissemination Metadata Catalogue has changes made by the subscription registrar.

Normal flow	The authorized subscription registrar uses a facility supported by the Dissemination Metadata Catalogue publisher to update the Dissemination Metadata Catalogue for the given subscription(s). Typically, two kinds of maintenance facility are supported:(a) a file upload facility for "batch" updating (adding, replacing or deleting metadata records treated as separate files); and (b). an online form for changing metadata records treated as entries in the Dissemination Metadata Catalogue (adding, changing or deleting elements in a record as well as whole records). The Dissemination Metadata Catalogue publisher maintains the updated Dissemination Metadata Catalogue as a reference resource accessible as part of a logically centralized but physically distributed catalogue across WIS centres.
Notes and issues	At this point in WIS system design, it has yet to be decided how each Dissemination Metadata Catalogue publisher will communicate changes to each physically distributed part of the logically centralized Dissemination Metadata Catalogue.
Last updated	30 June 2014
Last updated by	WMO Secretariat

Use Case B.11 – Reporting quality of service across WIS centres

Use Case goal	Managers of WIS centres receive performance reports of operations against agreed quality of service indicators.
Actors	WIS centre managers
Preconditions	(1) Measurable quality of service indicators are agreed; (2) Schedule of reporting and specifics of reporting formats are agreed.
Post-conditions	WIS centre managers have the performance information needed to manage WIS operations across the range of GISC, DCPC and NC services.
Normal flow	Following a mutually agreed schedule, all WIS centre managers send performance reports of operations against agreed quality of service indicators.
Notes and issues	It can be anticipated that WIS will eventually have agreements that address quality of service requirements. These should include data and network security as well as performance and reliability. CBS is investigating monitoring processes and reviewing established procedures for the World Weather Watch.
Last updated	30 June 2014
Last updated by	WMO Secretariat

APPENDIX C. WIS DEMONSTRATION TEST CASES

General

1. This appendix provides the test cases for major WIS functions relating to the WIS technical specifications (TechSpecs) as described in the *Manual on the WMO Information System* (WMO-No. 1060), Part IV. The WIS demonstration test cases differ from the Use Cases in that they are designed to check whether a process is correct, by looking at the particular input, and whether the result is as expected.

2. The guidelines for DCPCs and GISCs on how to demonstrate their compliance with the requirements established by CBS are available online at http://www-db.wmo.int/WIS/centres/guidance.doc.

3. Guidance for NCs on how to work with their principal GISC to demonstrate their compliance is included in regional WIS implementation plans available at http://wis.wmo.int/R-WISIP.

4. In order to be WIS compliant, all centres should be able to complete the demonstration test cases that are applicable to the services they provide. Demonstration test cases are based on the WIS Technical Specifications defined in the *Manual on the WMO Information System* (WMO-No. 1060), Part IV and Appendix D, and on the Use Cases detailed in this Guide, Appendix B.

5. There are six test cases for GISCs, labelled WIS-TC1 to WIS-TC6. All, except for WIS-TC4, are also relevant to DCPCs where they are applicable. The six test cases are described in Part 1 of this appendix.

6. There are three test cases for NCs, labelled NC-TC1 to NC-TC3, which are described in Part 2 of this appendix.

Part 1 – WIS demonstration test cases for GISCs and DCPCs

<table>
<tr><th colspan="4">Test case name: WIS Demonstration Test Case 1</th></tr>
<tr><td colspan="4">Uploading of metadata for data and products to DAR catalogue</td></tr>
<tr><td>Test case ID</td><td colspan="3">WIS-TC1</td></tr>
<tr><td>Component</td><td colspan="3">Metadata management</td></tr>
<tr><td colspan="4">Purpose of test</td></tr>
<tr><td colspan="4">To validate the functions of adding, updating and deleting metadata records provided by other WIS centres

All metadata records must be checked against the relevant schemas (i.e. a record should be rejected if it does not fit the corresponding schema).

NOTE 1: The term “upload” refers to the movement of metadata records between the WIS centre that provides the metadata and the WIS centre that manages the DAR catalogue. Uploading can actually be implemented as a “pull” initiated from the DAR catalogue site or as a “push” initiated by the metadata provider.
NOTE 2: Those functionalities can be implemented through:
• A web interface allowing registered users to manage their metadata interactively;
• A machine-to-machine interface allowing automated batch processing of metadata.

It is necessary that GISCs implement both methods.</td></tr>
<tr><td colspan="4">Relevant technical specifications</td></tr>
<tr><td colspan="4">• WIS-TechSpec-1: Uploading of metadata for data and products
• WIS-TechSpec-8: DAR Metadata (WIS Discovery Metadata) Catalogue search and retrieval</td></tr>
<tr><td colspan="4">Preconditions</td></tr>
<tr><td colspan="4">1. There is a network connection (dedicated and/or public) with other WIS centre(s);
2. A file upload facility for collecting metadata from other WIS centre(s) is available;
3. A fully functional DAR catalogue is available;
4. There is a registered user/process that is authorized to manage the metadata of a given WIS centre;
5. There is a web interface with the DAR catalogue that allows searches (see WIS-TC6).</td></tr>
<tr><td colspan="4">Test steps</td></tr>
<tr><td></td><td><i>Description</i></td><td><i>Expected results</i></td><td><i>Actual results</i></td></tr>
<tr><td>1</td><td>An authorized user/process adds a valid metadata record to the DAR catalogue.</td><td>The metadata record is found when browsing/searching the DAR catalogue.</td><td></td></tr>
<tr><td>2</td><td>An authorized user/process modifies a record in the DAR catalogue.</td><td>The modification is immediately visible when browsing/searching the DAR catalogue.</td><td></td></tr>
<tr><td>3</td><td>An authorized user/process deletes a record from the DAR catalogue.</td><td>The deleted record is not found when browsing/searching the DAR catalogue.</td><td></td></tr>
<tr><td>4</td><td>An authorized user/process attempts to upload an invalid metadata record.</td><td>The user/process is informed that the metadata record is invalid. The addition/update operation is aborted. The DAR catalogue is unchanged.</td><td></td></tr>
</table>

5	An authorized user/process attempts to upload a record with a unique identifier which is already in the DAR catalogue. NOTE: It is essential to ensure that an update is an edit, not an accidental duplication.	The DAR catalogue does not contain records with duplicate identifiers. Either: 1. The new metadata record replaces the old one, which disappears from the catalogue. The new metadata record is found when browsing/searching the catalogue; or: 2. The user/process is notified of the fact that the record is a duplicate. The addition/update operation is aborted. The DAR catalogue is unchanged.	
6	Access control – No unauthorized addition (1): An unauthorized user/process tries to add a metadata record to the DAR catalogue.	A non-authorized user/process is not allowed to add a metadata record to the DAR catalogue.	
7	Access control – No unauthorized addition (2): A WIS centre user/process tries to add to the DAR catalogue a metadata record representing data from another WIS centre.	A user/process is not able to add a metadata record representing data from another WIS centre to the DAR catalogue.	
8	Access control – No unauthorized modification (1): An unauthorized user/process tries to modify a metadata record in the DAR catalogue.	A non-authorized user/process is not able to modify a metadata record in the DAR catalogue.	
9	Access control – No unauthorized modification (2): A WIS centre user/process tries to modify a metadata record belonging to another WIS centre, which is held in the DAR catalogue.	A user/process is not able to modify a metadata record belonging to another WIS centre, which is held in the DAR catalogue.	
10	Access control – No unauthorized deletion (1): An unauthorized user/process tries to delete a metadata record from the DAR catalogue.	A non-authorized user/process is not able to delete a metadata record from the DAR catalogue.	
11	Access control – No unauthorized deletion (2): A WIS centre user/process tries to delete from the DAR catalogue a metadata record belonging to another WIS centre, which the user/process is not authorized to edit.	A user/process is not able to delete from the DAR catalogue a metadata record that belongs to another WIS centre.	

Centre		Organization		Country	
Test Date					

<table>
<tr><td colspan="9">Test case name: WIS Demonstration Test Case 2</td></tr>
<tr><td colspan="9">Synchronizing DAR catalogues among GISC nodes</td></tr>
<tr><td colspan="2">Test case ID</td><td colspan="7">WIS-TC2</td></tr>
<tr><td colspan="2">Component</td><td colspan="7">Metadata management</td></tr>
<tr><td colspan="9">Purpose of test</td></tr>
<tr><td colspan="9">(a) To validate the synchronization of DAR Metadata Catalogues among GISC nodes via a synchronization protocol, so that GISCs will have a global view of metadata;
(b) To test GISC to GISC synchronization (between separate centres);
(c) To assess the timeliness (accuracy) of synchronization.
This test should complement the mechanism for adding, changing and deleting metadata tested in WIS-TC1.</td></tr>
<tr><td colspan="9">Relevant technical specifications</td></tr>
<tr><td colspan="9">• WIS-TechSpec-1: Uploading of metadata for data and products
• WIS-TechSpec-8: DAR Metadata (WIS Discovery Metadata) Catalogue search and retrieval
• WIS-TechSpec-9: Consolidated view of distributed DAR Metadata (WIS Discovery Metadata) Catalogues</td></tr>
<tr><td colspan="9">Preconditions</td></tr>
<tr><td colspan="9">1. A network connection (dedicated and/or public) with the other GISC(s) exists;
2. A DAR catalogue already populated is available at each GISC participating in the test;
3. A facility for synchronizing metadata with the other GISC(s) is available.</td></tr>
<tr><td colspan="9">Test steps</td></tr>
<tr><td></td><td colspan="3"><i>Description</i></td><td colspan="3"><i>Expected results</i></td><td colspan="2"><i>Actual results</i></td></tr>
<tr><td>1</td><td colspan="3">Synchronize the DAR metadata catalogue.</td><td colspan="3">Identical content of the DAR Metadata Catalogues of the GISCs participating in the test: identical number of records, list of unique identifier and a random selection of records.</td><td colspan="2"></td></tr>
<tr><td>2</td><td colspan="3">Add new metadata record at GISC 1.</td><td colspan="3">The uploaded metadata record is added to the DAR Metadata Catalogue of the other GISC(s) participating in the test.</td><td colspan="2"></td></tr>
<tr><td>3</td><td colspan="3">Update metadata record at GISC 1.</td><td colspan="3">The updated metadata record is added to the DAR Metadata Catalogue of the other GISC(s) participating in the test.</td><td colspan="2"></td></tr>
<tr><td>4</td><td colspan="3">Delete from GISC 1 one of its metadata file records.</td><td colspan="3">The concerned metadata record is deleted from the DAR Metadata Catalogue of the other GISC(s) participating in the test.</td><td colspan="2"></td></tr>
<tr><td>5</td><td colspan="3">Delete from GISC 1 the metadata file record that doesn’t belong to it.</td><td colspan="3">The concerned metadata record is uploaded to the DAR Metadata Catalogue of GISC1 from the DAR Metadata Catalogue of the other GISC(s) participating in the test.</td><td colspan="2"></td></tr>
<tr><td colspan="9">Repeat steps 2–5 making the changes specified at each GISC in turn and check that each change is propagated to the other GISCs.</td></tr>
<tr><td colspan="2">Centre</td><td></td><td colspan="2">Organization</td><td></td><td colspan="2">Country</td><td></td></tr>
<tr><td colspan="2">Test date</td><td colspan="7"></td></tr>
</table>

<table>
<tr><td colspan="9">Test case name: WIS Demonstration Test Case 3</td></tr>
<tr><td colspan="9">Uploading and downloading of data between WIS centres</td></tr>
<tr><td colspan="2">Test case ID</td><td colspan="7">WIS-TC3</td></tr>
<tr><td colspan="2">Component</td><td colspan="7">Data upload and download</td></tr>
<tr><td colspan="9">Purpose of test</td></tr>
<tr><td colspan="9">To validate the upload and download of data and products and the metadata associated with them</td></tr>
<tr><td colspan="9">Relevant technical specifications</td></tr>
<tr><td colspan="9">• WIS-TechSpec-2: Uploading of data and products
• WIS-TechSpec-10: Downloading files via dedicated networks
• WIS-TechSpec-11: Downloading files via non-dedicated networks
• WIS-TechSpec-12: Downloading files via other methods</td></tr>
<tr><td colspan="9">Preconditions</td></tr>
<tr><td colspan="9">1. A network connection (dedicated and/or public) with other WIS centres exists;
2. File upload and download facilities such as FTP, e-mail and HTTP are available;
3. Data for upload or download are available;
4. DAR facilities are available at GISCs.</td></tr>
<tr><td colspan="9">Test steps</td></tr>
<tr><td></td><td colspan="3"><em>Description</em></td><td colspan="3"><em>Expected results</em></td><td colspan="2"><em>Actual results</em></td></tr>
<tr><td>1</td><td colspan="3">(a) Upload a file that is associated with a metadata record in the DAR catalogue of one GISC to another GISC;
(b) Use DAR facilities to search the metadata then retrieve the file.</td><td colspan="3">(a) The uploaded file has been delivered to the GISC and matches the corresponding metadata;
(b) The file can be downloaded.</td><td colspan="2"></td></tr>
<tr><td>2</td><td colspan="3">For GISCs only:
(a) Upload a file which is not associated with a metadata record in the DAR catalogue of one GISC to another GISC;
(b) Later, upload the metadata record associated with the file to the other GISC;
(c) Use DAR facilities to search the metadata and retrieve the file.</td><td colspan="3">(a) The uploaded file has been delivered to the GISC;
(b) The DAR catalogue is updated with the new record. The file received earlier is associated with the metadata;
(c) The file can be downloaded.</td><td colspan="2"></td></tr>
<tr><td colspan="2">Centre</td><td></td><td colspan="2">Organization</td><td></td><td colspan="2">Country</td><td></td></tr>
<tr><td colspan="2">Test date</td><td colspan="7"></td></tr>
</table>

<table>
<tr><td colspan="6">Test case name: WIS Demonstration Test Case 4</td></tr>
<tr><td colspan="6">Centralization of globally distributed data (applies only to GISCs)</td></tr>
<tr><td colspan="2">Test case ID</td><td colspan="4">WIS-TC4</td></tr>
<tr><td colspan="2">Component</td><td colspan="4">24-hour cache at GISC</td></tr>
<tr><td colspan="6">Purpose of test</td></tr>
<tr><td colspan="6">To validate the completeness of the 24-hour cache:
• Finding a current datum or product originating from another centre via the GISC DAR search mechanism, and retrieving that item from the GISC cache;
• Providing a document describing how the GISC will ensure that it holds a complete cache for 24 hours, including performance metrics.</td></tr>
<tr><td colspan="6">Relevant technical specifications</td></tr>
<tr><td colspan="6">• WIS-TechSpecs-3: Centralization of globally distributed data
• WIS-TechSpecs-8: DAR Metadata (WIS Discovery Metadata) Catalogue search and retrieval</td></tr>
<tr><td colspan="6">Preconditions</td></tr>
<tr><td colspan="6">1. A network connection (dedicated and/or public) exists;
2. A DAR catalogue already populated with metadata of the 24-hour data for global exchange is available;
3. DAR facilities are available through a portal;
4. A cache with at least the last 24 hours of data for global exchange is available.</td></tr>
<tr><td colspan="6">Test steps</td></tr>
<tr><td></td><td><i>Description</i></td><td colspan="2"><i>Expected results</i></td><td colspan="2"><i>Actual results</i></td></tr>
<tr><td>1</td><td>Search catalogue for data/products from other centres and programs in other areas, and retrieve selected data or products.</td><td colspan="2">The selected data/products can be retrieved from the GISC.</td><td colspan="2"></td></tr>
<tr><td>2</td><td>Search catalogue for data/products that are 6 hours old and retrieve selected data or products.</td><td colspan="2">The selected data/products can be retrieved from the GISC.</td><td colspan="2"></td></tr>
<tr><td>3</td><td>Search catalogue for data/products that are 12 hours old and retrieve selected data or products.</td><td colspan="2">The selected data/products can be retrieved from the GISC.</td><td colspan="2"></td></tr>
<tr><td>4</td><td>Search catalogue for data/products that are 18 hours old and retrieve selected data or products.</td><td colspan="2">The selected data/products can be retrieved from the GISC.</td><td colspan="2"></td></tr>
<tr><td>5</td><td>Search catalogue for data/products that are 24 hours old and retrieve selected data or products.</td><td colspan="2">The selected data/products can be retrieved from the GISC.</td><td colspan="2"></td></tr>
<tr><td>Centre</td><td></td><td>Organization</td><td></td><td>Country</td><td></td></tr>
<tr><td colspan="2">Test date</td><td colspan="4"></td></tr>
</table>

Test case name: WIS Demonstration Test Case 5			
Maintenance of user roles, authorization and authentication			
Test case ID	WIS-TC5		
Component	Management of users and access		
Purpose of test			
To create and run a variety of user types			
Relevant technical specifications			
• WIS-TechSpec-4: Maintenance of user identification and role information • WIS-TechSpec-6: Authentication of a user • WIS-TechSpec-7: Authorization of a user role • WIS-TechSpec-13: Maintenance of dissemination metadata			
Preconditions			
1. A WIS centre is entitled to provide access to users (i.e. it has received the approval of the Permanent Representative of the user's country); 2. The user interface is via the Internet (i.e. web page).			
Test steps			
	Description	*Expected results*	*Actual results*
1	Provide access for an external user to search metadata.	Temporary users can search metadata, but can neither access data from the GISC or cache, nor subscribe to data.	
	The user: (a) goes to search the web page; (b) searches for metadata; (c) tries to access data.	The user: (a) has access to the search page; (b) user finds metadata; (c) is referred to the authorization page at data source and cannot access data without an authorized user role.	
2	Create accounts with access to WIS metadata and data for authorized users of a WMO centre.	Two accounts have been created: one with access to metadata only, the other with the ability to access the centre subscription service or ad hoc request from the cache.	

	The user: (a) goes to the registered user web page; (b) is required to login or create an account; (c) registers the account and selects the role of valid "WMO member" with authority to access WIS data (for example, from WMO NC); (d) enters login details; (e) makes metadata search; (f) tries to access WMO globally available data from the centre; (g) tries to access additional data at centre for which he/she has no authorization; (h) tries to access data or products at another site; (i) subscribes to data for future delivery from centre; (j) returns to another session and reuses login to search or subscribe; (k) edits subscription details; (l) cancels a subscription; (m) logs out or leaves centre's site and tries to return to a bookmarked page at a later date to access data.	The user: (a) has access to the login page; (b) if new, has to create an account; (c) is able to create an account as a "WMO member". He/she receives a user login (for instance, a code via email or an encrypted symbol); (d) has logged in as a "WMO member", can search and download data from cache and has access to subscription services; (e) finds metadata; (f) accesses data from the centre; (g) is informed that she/he is not authorized to access these data and is referred to the access page where she/he can request a change of user role or can login again as another user; (h) is referred to the authorization page at the other site; (i) receives scheduled data via agreed method at agreed time; (j) maintains access with the same access rights; (k) has subscription details that are updated and reflected in subsequent deliveries; (l) has subscription details that are updated and receives no further deliveries; (m) is directed to the registered user login page.	
3	The user checks status of account and subscriptions.	The user can view his account and subscription details, including past, current and future transactions.	

Centre		Organization		Country	
Test date					

<table>
<tr><th colspan="4">Test case name: WIS Demonstration Test Case 6</th></tr>
<tr><td colspan="4">DAR Metadata (WIS Discovery Metadata) Catalogue search and retrieval</td></tr>
<tr><td colspan="2">Test case ID</td><td colspan="2">WIS-TC6</td></tr>
<tr><td colspan="2">Component</td><td colspan="2">DAR Metadata Catalogue</td></tr>
<tr><td colspan="4">Purpose of test</td></tr>
<tr><td colspan="4">To assess the functionality of the DAR Metadata Catalogue</td></tr>
<tr><td colspan="4">Relevant technical specifications</td></tr>
<tr><td colspan="4">WIS-TechSpec-8: DAR Metadata (WIS Discovery Metadata) Catalogue search and retrieval</td></tr>
<tr><td colspan="4">Preconditions</td></tr>
<tr><td colspan="4">1. The DAR catalogue is loaded with a representative number of WMO core metadata records for a variety of data and products; in particular, the records should represent several time ranges (climate and real-time), several geographical extents (from point to global coverage) and several disciplines (meteorology, hydrology, etc.), when applicable, for the functions of the candidate centre (GISC, DCPC, etc.);
2. A web-based user interface is made available on the open Internet to provide access to the DAR catalogue;
3. There exists a registered user that is allowed to retrieve some data and/or products;
4. The number of records returned may be subject to size limits of the system (e.g. 1000 record limit).</td></tr>
<tr><td colspan="4">Test steps</td></tr>
<tr><td></td><td><i>Description</i></td><td><i>Expected results</i></td><td><i>Actual results</i></td></tr>
<tr><td>1</td><td>Browsing</td><td>Any record in the DAR catalogue is reachable by browsing.</td><td></td></tr>
<tr><td>2</td><td>Free-text search: The user inputs one or more words in a web form and submits the request.</td><td>All records containing the required words are retrieved. If the user is allowed to select a Boolean operation between the results, the outcome should reflect this condition.</td><td></td></tr>
<tr><td>3</td><td>Geographic search: The user inputs a rectangular geographical area (using a form or a map).</td><td>Retrieval of all records that are contained in the area or that overlap with the area, depending on the implementation (the user should be aware of the matching algorithm used). The system handles the poles and the date line properly.</td><td></td></tr>
<tr><td>4</td><td>Time search: The user inputs either a time interval or a point in time in a web form.</td><td>Retrieval of all records representing a time interval or point in time that are contained in or overlap with the requested interval or point in time, depending on the implementation (the user should be aware of the matching algorithm used).</td><td></td></tr>
<tr><td>5</td><td>A combination of the above searches: A user can select a combination of any two or all of the above simultaneously.</td><td>Records that match all the selected criteria are retrieved.</td><td></td></tr>
<tr><td>6</td><td>Invalid search</td><td>The user receives a clear error message.</td><td></td></tr>
<tr><td>7</td><td>Search/Retrieval via URL (SRU) in accordance with ISO 23950 SRU protocol</td><td>The above searches will produce the same results when the SRU protocol is used.</td><td></td></tr>
</table>

8	Visualization of metadata	The user is able to select a metadata record when browsing or from a search result list. The record is rendered in a human readable form.	
9	Selection and retrieval of data: The user tries to select and retrieve specific data.	The user is able to select data and products either when browsing or from a search result list or when visualizing a meta record. The user is presented with a means to select instances that are associated with the chosen record. The system provides a retrieval/referral mechanism that will allow the user to receive the data, noting that the data may be available from another site.	

Centre		Organization		Country	
Test date					

Part 2 – WIS Demonstration Test Cases for NCs

<table>
<tr><td colspan="4">Test Case name: NC Demonstration Test Case 1</td></tr>
<tr><td colspan="4">Uploading of discovery metadata for data and products to the DAR catalogue</td></tr>
<tr><td>Test case ID</td><td colspan="3">NC-TC1</td></tr>
<tr><td>Component</td><td colspan="3">Metadata management</td></tr>
<tr><td colspan="4">Purpose of test</td></tr>
<tr><td colspan="4">To validate the functions of adding, updating and deleting metadata records provided by an NC to its principal GISC

All metadata records must be checked against the relevant schemas. A record should be deleted if it does not fit its corresponding schema.

NOTE 1: The term "upload" refers to the movement of metadata records between the National Centre that provides the metadata and the WIS centre that manages the DAR catalogue hosted by the principal GISC. Uploading can actually be implemented as a "pull" initiated from the DAR catalogue site, or as a "push" initiated by the metadata provider;
NOTE 2: Those functionalities can be implemented through:
• A web interface allowing registered users to manage their metadata interactively;
• A machine-to-machine interface allowing automated batch processing of metadata.

All GISCs support both methods. NCs may choose one or both methods.</td></tr>
<tr><td colspan="4">Relevant technical specifications</td></tr>
<tr><td colspan="4">• WIS-TechSpec-1: Uploading of metadata for data and products
• WIS-TechSpec-8: DAR Metadata (WIS Discovery Metadata) Catalogue search and retrieval</td></tr>
<tr><td colspan="4">Preconditions</td></tr>
<tr><td colspan="4">1. A network connection (dedicated and/or public) exists between the NC and GISC;
2. The GISC has a file upload facility for collecting metadata from other WIS centres;
3. The GISC has a fully functional DAR catalogue;
4. The GISC has a registered user/process that is authorized to manage metadata of a given WIS centre;
5. The GISC has a web interface with the DAR catalogue that allows searches (see WIS-TC6).</td></tr>
<tr><td colspan="4">Test steps</td></tr>
<tr><td></td><td><i>Description</i></td><td><i>Expected results</i></td><td><i>Actual results</i></td></tr>
<tr><td>1</td><td>An authorized user/process adds a valid metadata record to the DAR catalogue.</td><td>The metadata record is found when browsing/searching the DAR catalogue.</td><td></td></tr>
<tr><td>2</td><td>An authorized user/process modifies a record from the DAR catalogue.</td><td>The modification is immediately visible when browsing/searching the DAR catalogue.</td><td></td></tr>
<tr><td>3</td><td>An authorized user/process deletes a record in the DAR catalogue.</td><td>The deleted record is not found when browsing/searching the DAR catalogue.</td><td></td></tr>
</table>

4	An authorized user/process attempts to upload an invalid metadata record.	The user/process is informed that the metadata record is invalid. The addition/update operation is aborted. The DAR catalogue is unchanged.	
5	An authorized user/process attempts to upload a record with a unique identifier that is already in the DAR catalogue. NOTE: It is essential to ensure that an update is an edit and not an accidental duplication.	The DAR catalogue does not contain records with duplicate identifiers. Either: 1. The new metadata record replaces the old one, which is deleted from the catalogue. The new metadata record is found when browsing/searching the catalogue; or: 2. The user/process is notified that the record is a duplicate. The addition/update operation is aborted. The DAR catalogue is unchanged.	
6	Access control – No unauthorized addition (1): An unauthorized user/process tries to add a metadata record to the DAR catalogue.	A non-authorized user/process is not able to add a metadata record to the DAR catalogue.	
7	Access control – No unauthorized addition (2): A WIS centre user/process tries to add a metadata record representing data from another WIS centre to the DAR catalogue.	A WIS centre user/process is not able to add a metadata record representing data from another WIS centre to the DAR catalogue.	
8	Access control – No unauthorized modification (1): An unauthorized user/process tries to modify a metadata record in the DAR catalogue.	A non-authorized user/process is not able to modify a metadata record in the DAR catalogue.	
9	Access control – No unauthorized modification (2): A WIS centre user/process tries to modify a metadata record belonging to another WIS centre, which is held in the DAR catalogue.	A WIS centre user/process is not able to modify a metadata record belonging to another WIS centre, which is held in the DAR catalogue.	
10	Access control – No unauthorized deletion (1): An unauthorized user/process tries to delete a metadata record from the DAR catalogue.	A non-authorized user/process is not able to delete a metadata record from the DAR catalogue.	
11	Access control – No unauthorized deletion (2): A WIS centre user/process tries to delete from the DAR catalogue a metadata record belonging to another WIS centre, which the user/process is not authorized to edit.	A WIS user/process is not able to delete from the DAR catalogue a metadata record belonging to another WIS centre, which the user/process is not authorized to edit.	

Centre		Organization		Country	
Test Date					

<table>
<tr><td colspan="9">Test case name: NC Demonstration Test Case 2</td></tr>
<tr><td colspan="9">Uploading and downloading of data between WIS centres</td></tr>
<tr><td colspan="2">Test case ID</td><td colspan="7">NC-TC2</td></tr>
<tr><td colspan="2">Component</td><td colspan="7">Uploading and downloading of data</td></tr>
<tr><td colspan="9">Purpose of test</td></tr>
<tr><td colspan="9">To validate the upload and download of data and products and the associated metadata</td></tr>
<tr><td colspan="9">Relevant technical specifications</td></tr>
<tr><td colspan="9">• WIS-TechSpec-2: Uploading of data and products
• WIS-TechSpec-10: Downloading files via dedicated networks
• WIS-TechSpec-11: Downloading files via non-dedicated networks
• WIS-TechSpec-12: Downloading files via other methods</td></tr>
<tr><td colspan="9">Preconditions</td></tr>
<tr><td colspan="9">1. A network connection (dedicated and/or public) exists between an NC and a GISC (including via RTH where relevant);
2. File upload and download facilities such as FTP, e-mail and HTTP are available;
3. Data are available for upload or download;
4. DAR facilities are available at GISC.</td></tr>
<tr><td colspan="9">Test steps</td></tr>
<tr><td></td><td colspan="3"><i>Description</i></td><td colspan="3"><i>Expected results</i></td><td colspan="2"><i>Actual results</i></td></tr>
<tr><td>1</td><td colspan="3">(a) Upload a file that is associated with a metadata record in the DAR catalogue of a GISC to another GISC;
(b) Use DAR facilities to search the metadata and retrieve the file.</td><td colspan="3">(a) The file has been uploaded to the other GISC and matches the corresponding metadata;
(b) The file can be downloaded.</td><td colspan="2"></td></tr>
<tr><td colspan="2">Centre</td><td></td><td colspan="2">Organization</td><td></td><td colspan="2">Country</td><td></td></tr>
<tr><td colspan="2">Test date</td><td colspan="7"></td></tr>
</table>

Test case name: NC Demonstration Test Case 3	
Maintenance of user roles, authorization and authentication	
Test case ID	NC-TC3
Component	Management of users and access
Purpose of test	
To create and run a variety of user types NOTE: A centre may use the GISC user control interface.	
Relevant technical specifications	
• WIS-TechSpec-4: Maintenance of user identification and role information • WIS-TechSpec-6: Authentication of a user • WIS-TechSpec-7: Authorization of a user role • WIS-TechSpec-13: Maintenance of dissemination metadata	
Preconditions	
1. The centre is entitled to provide access to users (i.e. it has received the approval of the Permanent Representative of the user’s country); 2. A process is in place for an NC to authorize its users to use the GISC with appropriate access levels; 3. The user interface is via the Internet (i.e. web page).	
Test steps	

	Description	*Expected results*	*Actual results*
1	Provide access for an external user to search metadata.	A temporary user can search metadata, but can neither access data from the GISC or cache, nor subscribe to data.	
	The user: (a) goes to search the web page; (b) searches for metadata; (c) tries to access data.	The user: (a) has access to the search page; (b) finds metadata; (c) is referred to the authorization page at data source. He/she cannot access data without an authorized user role.	
2	Create accounts with access to WIS metadata and data for a WMO centre authorized user.	Two user accounts have been created: one with access to metadata only, the other with access to the centre subscription service or ad hoc request from the cache.	

	The user: (a) goes to the registered user web page; (b) is required to login or create an account; (c) registers the account and selects the role of valid "WMO member" with authority to access WIS data (for example, from a WMO NC); (d) enters login details; (e) searches for metadata; (f) tries to access WMO globally available data from the centre; (g) tries to access additional data at centre for which he/she has no authorization; (h) tries to access data or products at another site; (i) subscribes to data for future delivery from centre; (j) returns to another session and reuses login to search or subscribe; (k) edits subscription details; (l) cancels a subscription; (m) logs out or leaves the centre's site and tries to return to a bookmarked page at a later date to access data.	The user: (a) has access to the login page; (b) if new, has to create an account; (c) is able to create an account as a "WMO member" and receives a user login (for example, a code via e-mail or an encrypted symbol); (d) is logged in. As a "WMO member", she/he can search and download data from the cache and has access to subscription services; (e) finds metadata; (f) accesses data from the centre; (g) is informed that he/she is not authorized to access the data and is referred to the access page where he/she can request a change of user role or login again as another user; (h) is referred to the authorization page at the other site; (i) receives scheduled data via agreed method at agreed time; (j) maintains access with the same access rights; (k) has subscription details that are updated and reflected in subsequent deliveries; (l) has subscription details that are updated and receives no further deliveries; (m) is directed to the registered user login page.	
3	The user checks the status of his/her account and subscriptions.	The user can view his/her account and subscription details, including past, current and future transactions.	
...			

Centre		Organization		Country	
Test date					

APPENDIX D. ANNEXES TO PARAGRAPHS 7.4.1, 7.5.1, 7.6.2 AND 8.7

Annex to paragraph 7.4.1: Procedure for changing principal GISC

1. The centre (NC/DCPC) wishing to change its principal GISC should consult with its present and proposed principal GISCs and receive the agreement of the latter.

2. The centre should check the communication network connectivity to the chosen GISC and ensure that the bandwidth is sufficient to send and receive all data without undue delays.

3. The centre should send a letter, endorsed by the Permanent Representative of its host country with WMO, to the WMO Secretary-General, with a copy to its current principal GISC. The letter should state the centre's choice of new principal GISC and include endorsement of the arrangement by the new principal GISC. The letter should also ask the Secretary-General to communicate that change to the regional association responsible for the centre and to the GISCs concerned where these are not in the same region as the centre.

4. The WMO Secretariat shall inform CBS of the change, with copy to the original and new principal GISC, and ask the Commission to prepare an update to the *Manual on WIS,* Appendix B.

5. The WMO Secretariat should update the WIS centres database (http://wis.wmo.int/wiscentresdb) and the WMO Country Profile Database (http://www.wmo.int/cpdb).

6. The new principal GISC should coordinate with the associated GISC(s) to make arrangements for the backup service.

7. The new principal GISC should liaise with the previous principal GISC to take over responsibility for the discovery metadata records describing the data and products of the centre that has been transferred (see section 7.5 of this Guide).

8. The new principal GISC should notify all operational GISCs of the change to its area of responsibility.

Annex to paragraph 7.5.1: Guidelines for migrating metadata records from one GISC to another

1. Scenario and use case

Consider the migration of metadata between two GISCs: GISC A and GISC B. GISC B is becoming operational and starting metadata management for National Centre X as its principal GISC. Accordingly, GISC A, which has been providing the WIS Interim Metadata Management Service for National Centre X, is ending this service. Practically, a set of metadata records owned by National Centre X needs to be moved from the Open Archive Initiative (OAI) set provided by GISC A (also referred to as WIS-GISC-A) to that provided by GISC B (WIS-GISC-B).

2. Operational guidelines

2.1 *Giving notice to other GISCs*

GISCs A and B jointly give one-week notice to other operational GISCs that they will transfer the metadata management from GISC A to B, with the list of location indicators (CCCC) in the case of metadata records that are associated with GTS messages. This notification is necessary because other GISCs need to make configuration changes, before they start harvesting new records, so that each CCCC belongs to specific OAI sets.

2.2 *Deleting and adding records at GISCs A and B*

2.2.1 Deleting records from GISC A

This should be done by using the procedure for deleted records described in The Open Archives Initiative Protocol for Metadata Harvesting (OAI-PMH), subsection 2.5.1 (http://wis.wmo.int/oaiprotocol), not by simply deleting records from the database, so that harvesters of other GISCs can harvest the deletion information through the ordinary incremental harvesting.

If GISC A needs to delete these records completely from its database, it must do so only after other GISCs have completed harvesting the deletion.

2.2.2 Adding records to GISC B

This should be done with an accurate date stamp, which allows harvesters of other GISCs to gain the added records through the ordinary incremental harvesting.

2.3 *Track harvesting by other GISCs*

GISCs A and B make sure that other GISCs harvest the change correctly, otherwise they need to ask for manual adjustments.

3. References

The Open Archives Initiative Protocol for Metadata Harvesting, http://wis.wmo.int/oaiprotocol.

Annex to paragraph 7.6.2: Recommended practices for the rolling review of WIS centres

Note: If the structure of CBS changes, all references to Open Area Programme Group (OPAG), Implementation Coordination Team (ICT), Expert Team (ET) or Task Team (TT) are intended to apply to successors of the named bodies.

1. Background

The Commission for Basic Systems is responsible for certification of WIS centres’ compliance with the WIS technical specifications defined in the *Manual on WIS*, Appendix D. The Commission for Basic Systems will maintain, within the structure of its OPAG on Information Systems and Services (OPAG-ISS), or its successor, a team to coordinate audits and certification of WIS centres. For the purpose of this Guide, the team or its equivalent group of experts is referred to as the Expert Team on Centre Audit and Certification (ET-CAC).

Audits and certifications will be carried out in line with the principles established in *Technical Regulations* (WMO-No. 49), Volume I: General Meteorological Standards and Recommended Practices, Part VII.

2. Auditing and certification

Auditors and certifiers shall be or shall become members of ET-CAC. New members must have relevant technical or auditing experience (the nomination form is at http://wis.wmo.int/Expert-Form). They must be members (core or associate) of an OPAG-ISS expert team or have written commitment of the Permanent Representative of their country with WMO allowing them to participate as members of the ET-CAC. New members will be mentored by a nominated existing expert. Note that regional diversity of members of ET-CAC is essential.

Access to ET-CAC workspace and online databases is restricted to ET-CAC and the WMO Secretariat.

2.1 *GISC audits*

The Expert Team on Centre Audit and Certification, on behalf of CBS, is responsible for auditing and certification of GISCs.

A GISC should be audited by two experts, one of whom must have previous experience of auditing GISCs. Auditors should be from a different region than that of the GISC.

Travel and per diem should be at the GISC's expense and arranged through WMO.

2.1.1 Scope of GISC audits

Full audits will cover all aspects of WIS compliance and shall include site visits using practices in line with those of the ISO 9000 series standards.

Interim audits will focus on a particular subset of topics. Actual elements to be focused on will be determined by the Implementation Coordination Team on Information Systems and Services (ICT-ISS) or its delegated expert team in coordination with ICT-ISS members. Centres will be told in advance on which subset of topics the interim audit will focus. Possible areas for review in interim audits include:

(a) GISC to GISC backup;

(b) Security;

(c) Monitoring;

(d) Quality of service provided by the WIS;

(e) WIS core network (e.g. in 2014, this was the Regional Meteorological Data Communication Network – Next generation);

  (i) Connectivity and management;

  (ii) Cacheing of "Globally distributed data" content;

(f) Management of the GISC area of responsibility;

  (i) Capacity development;

  (ii) The AMDCN connecting the GISC to NCs and DCPCs in its area;

    a. Cacheing of "Area of responsibility" content;

  (iii) Participation in WIS coordination and planning mechanisms (e.g. CBS Inter-programme Expert Teams, Expert Teams and Task Teams).

2.2 *DCPC certification*

Data Collection or Production Centres are to be certified by the ET-CAC. Where a DCPC is not using the infrastructure of its principal GISC, and its principal GISC is operational, it can be certified by ET-CAC once the principal GISC has performed the necessary tests. However, if the principal GISC is not operational, the ET-CAC will arrange for a suitable GISC to perform the tests. Where a DCPC uses the infrastructure of its principal GISC, it is certified as a part of the GISC certification process.

The certification of a DCPC requires only one ET-CAC coordinator, who will ask a GISC to undertake tests with the DCPC. It is expected that the centre's principal GISC will undertake those tests.

2.3 *Verification of compliance of NCs*

Compliance of NCs is the responsibility of the Permanent Representative with WMO of the Member accountable for the centre. Verification of compliance of an NC should be done by its principal GISC. The Expert Team on Centre Audit and Certification will monitor the NC compliance process in consultation with NCs and GISCs.

3. The review cycle

The review cycle should start from the date of CBS endorsement. For centres endorsed before 1 January 2012 (the date on which WIS became operational) the cycle will start on 1 January 2012. Audits should take place within the calendar year in which the cycle ends and their timing will need to be coordinated with the experts called upon to undertake them.

The CBS endorsement date should be recorded in the WIS centre database. The date on which the centre became operational should also be recorded if known.

Similarly to an ISO 9001:2008 audit process, the GISC audit will follow the principle of alternating intermediate and full audits aligned with the CBS/EC four-year cycle:

(a) Intermediate audit (interim, four years): a mid-cycle review of performance and compliance to provide, if necessary, opportunities to introduce corrective actions well in advance of a full audit;

(b) Full audit (every second audit, i.e. every eight years): this audit will result in a recommendation for confirmation or cancellation of endorsement.

3.1 *Review of DCPCs*

The DCPC review cycle will be eight years. Reviews will cover all aspects of WIS compliance.

3.2 *Review of NCs*

Review of NC compliance is the responsibility of the Permanent Representative with WMO of the Member responsible for the Centre in liaison with the NC and its principal GISC.

4. Ad hoc audits or reviews

An ad hoc audit or review can be requested by the president of CBS due, for example, to non-conformance causing problems with WIS operations.

5. **Audit or review outcome**

The outcome of the audit or review will be categorized as “endorsed”, “endorsed with qualification” or “not endorsed”. Audit or review recommendations will be provided to the president of CBS and to the Director of WIS.

6. **Format of report**

The Expert Team on Centre Audit and Certification will use a template for final reports, although the content will reflect the areas audited.

7. **Public notification of type of CBS endorsement**

The endorsement of CBS is based on continued successful audit outcomes. Centre endorsements are published only as “CBS endorsed” with no public declaration of whether endorsement was with “qualifications”.

Details of reviews and audits of centres are confidential. Auditors will have access to the previous reports on a centre in order to perform their role.

8. **Review of audits with qualification**

Global Information System Centres that were “endorsed with qualifications” have two years from the date of the audit to demonstrate that they have taken remedial action on the points of qualification.

The Expert Team on Centre Audit and Certification will investigate GISCs that were “endorsed with qualifications” and have not demonstrated that they have taken remedial action within two years of the date of audit. The Expert Team should report to CBS on progress in addressing the aspects that incurred the “qualification”, and can recommend to CBS that it revokes its endorsement.

Annex to paragraph 8.7: GISC Watch Programme

1. Every GISC shall participate in the GISC Watch according to a monthly roster.

2. GISCs shall agree the roster at their coordination meeting (see *Manual on the WMO Information System* (WMO-No. 1060), paragraph 3.5.11).

3. The GISC on duty shall:

(a) Carry out the GISC Watch by using information exchanged in JSON files. The WIS Common Dashboard (WCD) provides a convenient summary to support this activity;

(b) Provide a summary report;

(c) Formally hand over the GISC Watch operation to the next GISC in the roster.

4. The monitoring activities performed by the on-duty GISC shall include at the least the following:

(a) Daily monitoring of the status of services of each GISC, including OAI-PMH, SRU and the HTTP portal. A history of these statuses is required, and providers of the WCD should store and make available the history for one month;

(b) Monitoring the number of metadata records of each GISC, including an assessment of whether the numbers are similar and contain no sudden major changes;

(c) Maintaining entries in an agreed issue tracking system to report incidents and follow up on the action taken. The notification of inclusion of an entry in the issue tracking system should be sent to affected GISCs. Note that the issue tracking system is used to manage and refer issues as needed.

Template and example of GISC Watch Report

ID	*Date*	*GISC*	*Finding*	*Status*	*Reporter*
1	DD/MM/YYYY	GISC A	OAI provider inactive	closed	XXX
2	DD/MM/YYYY	GISC B	Timeout login process	partially open	XXX
3	DD/MM/YYYY	GISC C	Can't reach GISC C	open	XXX
4	……				
5	……				
On-duty GISC		GISC E	Watch period	From: DD/MM/YYYY	To: DD/MM/YYYY

APPENDIX E. ANNEX TO PARAGRAPH 7.8

Overview

This appendix describes the key management activities associated with information and communications systems: ICT service incident management, ICT service continuity management (ITSCM), ICT service monitoring, and ICT service change management.

1. ICT SERVICE INCIDENT MANAGEMENT

1.1 Objective

Incident management is to restore normal service as quickly as possible after an incident and minimize the adverse impact on business operations, ensuring that agreed levels of service quality are maintained.

1.2 Scope

Incident management is not expected to perform root cause analysis to identify why an incident occurred. Rather, the focus is on doing whatever is necessary to restore the service. This often requires the use of a temporary fix or workaround. An important tool in the diagnosis of incidents is the known error database (KEDB), which is maintained by problem management. The KEDB identifies any problems or known errors that have caused incidents in the past and provides information about any workarounds that have been identified.

1.3 Key activities/functions to consider

(a) A service level agreement between the provider and the customer that defines incident priorities, escalation paths and response/resolution time frames;

(b) Incident models or templates that allow incidents to be resolved efficiently;

(c) Categorization of incident types for better data gathering and problem management;

(d) Agreement on incident statuses, categories and priorities;

(e) Establishment of a major incident response process;

(f) Agreement on incident management role assignment.

1.4 Incident management's main function: The service desk

Incident management involves several functions, the most important being the service desk, also known as the help desk. The service desk is the single point of contact for users to report incidents.

A service desk is divided into tiers of support. The first tier is for basic issues, such as password reset and basic computer troubleshooting. Tier-one incidents are most likely to turn into incident models, since the templates to create them are easy and the incidents recur often. For example, a model for a password reset includes the categorization of the incident (category: "Account" and type:"Password Reset", for example), a template for information to be completed by the support staff (such as username and verification requirements) and links to internal or external knowledge base articles that support the incident. Low-priority tier-one incidents do not impact the business in any way and can be worked around by users.

Second-tier support involves issues that need more skill, training or access. Resetting an RSA token, for example, may require tier-two escalation.

1.5 The incident process

Incidents go through a structured workflow that encourages efficiency and best results for both providers and customers. Management of incidents should include the following:

(a) Incident identification;

(b) Incident logging;

(c) Incident categorization;

(d) Incident prioritization;

(e) Incident response:

    (i) Initial diagnosis;

    (ii) Incident escalation;

    (iii) Investigation and diagnosis;

    (iv) Resolution and recovery;

    (v) Incident closure.

2. ICT SERVICE CONTINUITY MANAGEMENT

2.1 Objective

To apply the processes through which plans are implemented and maintained in order to ensure the ongoing operation of IT services and functions before, during and after a disruption or crisis.

2.2 Scope

Business continuity management can apply to any service or function. In the context of this annex, the focus is on IT services and functions.

2.3 Key activities/functions to consider when implementing ICT service continuity management plans

The development of business continuity plans, regardless of domain, typically involves a common set of activities in order to be complete, robust and effective.

(a) Carry out a business impact analysis (BIA): The purpose of the BIA is to identify and prioritize key ICT services and functions. Priority setting should take into account the impact of disruptions on the organization’s finances, operations, reputation, customers, suppliers, environment and staff:

(i) Financial impact may be related to revenue (as in the case of organizations selling products and/or services), costs to continue operations during the disruption, and costs of re-establishing services:

a. Identify the products and services that represent the greatest revenue to the organization;

b. Identify the products/services that incur the greatest costs to support during a disruption;

(ii) Operational impact may be related to how business functions/services are delivered during disruptions, including those caused in downstream areas due to interdependence with the area of primary disruption:

a. Identify functions/services having upstream and downstream interdependence;

b. Identify the functions/services having the highest impact during a disruption;

(iii) Impact on reputation may range from loss of trust/credibility to more significant legal consequences and breaches due to failure to meet service level agreements:

a. Identify functions/services encompassing more sensitive data and information that could result in greater loss of credibility or incur greater potential legal consequences;

b. Identify higher-demand functions/services that may result in far-reaching consequences and a major response in the event of failure;

(iv) Impact on customers and suppliers may be caused by disruption in incoming services/products from suppliers, by customers not being in a position to accept/use them, and by disruptions in downstream customer (external) processes/services due to inability to deliver at normal levels;

(v) Environmental impact may be related to an organization's position in the market (for example, relative to competitors and partners, position of leadership);

(vi) Impact on staff may be caused by increased or reduced staffing levels during disruption and recovery, by the potential need to re-prioritize staff workloads thus impacting other services/functions, and by the associated financial consequences for the staff themselves.

(b) Determine risks and mitigation methods:

Identify risks to ICT services and functions, along with potential mitigation strategies;

(c) Establish recovery options:

Identify, evaluate and select recovery options;

(d) Build business continuity plans:

(i) Document who/what/where/when/why/how for reference when a disruption, incident or crisis occurs:

a. Cover at least all critical business functions;

b. Cover interdependency with external stakeholders;

(e) Test, review and maintain continuity plans:

Periodically test and review plans to ensure they continue to be relevant and provide intended results.

2.4 Ensuring key processes are in place

(a) Continuity strategies:

(i) Determine what continuity strategies exist and which ones are appropriate (and when);

(ii) Some continuity strategies (for example, support agreements with vendors, initiating business operations at an alternate site) incur costs which must be understood and resourced;

(b) Business continuity planning;

(c) Incident management;

(d) Continuity during disruption, incident or crisis;

(e) Recovery/resumption:

(i) Restoration priorities and levels;

(ii) Decision points on when a recovered service is deemed “acceptable”, “back in operation”;

(f) Exercising/testing.

2.5 Building resilience

(a) Set priorities:

Determine relative priorities for restoration - it is not possible to recover everything at once;

(b) Set service levels and use these to plan continuity strategies, etc.:

Establish maximum tolerable period of disruption, recovery time objectives and recovery point objectives (these should be fulfilled by the continuity plan);

(c) Communications:

(i) Ensure that communication tools are available in case of a major crisis (for example, multiple channels such as e-mail and phone);

(ii) Define roles and responsibilities;

(d) People:

(i) Maintain adequate staffing levels;

(ii) Ensure training/cross-training/contracting;

(iii) Define roles and responsibilities in the event of failure;

(iv) Maintain contact lists;

(e) Business locations:

(i) Have primary and alternative work locations;

(ii) Ensure physical security;

(f) Processes/tools:

Maintain documented procedures;

(g) Technology (ICT):

(i) Ensure cyber security;

(ii) Provide public and private infrastructure.

2.6 When to use ICT service continuity management in the WIS context

General centre failure:

- GISC
- DCPC
- NC

2.7 Supporting ICT service continuity management throughout the WIS network

(a) ICT service continuity management plans should exist at all levels of the network (GISC, DCPC, NC). This is not always the case due to varying capabilities and capacity;

(b) Continuity plans are a component of a centre’s overarching quality management system;

(c) WIS could develop a basic ICT service continuity management framework based on the core capabilities/functions of the WIS network. Such a framework would:

(i) Ensure that the core WIS functions are covered;

(ii) Reduce efforts on the part of the centres, without stopping work at the centres;

(iii) Not address situations at each individual centre;

(iv) Require resources to be defined and developed.

3. ICT SERVICE MONITORING

“If you cannot measure it, you cannot improve it.” – Peter Drucker.

3.1 Objective

Monitoring refers to the practice of collecting regular data regarding your ICT infrastructure in order to provide alerts both of unplanned downtime, network intrusion and resource saturation.

The main goal is to guarantee operations.

3.2 Candidates for monitoring

Status of key configuration items, looking for abnormalities or failures (servers, network, computers, etc.):

(a) Security events or network intrusions;

(b) Unauthorized changes to infrastructure or computers;

(c) Performance and tracked data for key performance indicators (KPIs);

(d) Processes to determine theeffectiveness of the key configuration items.

3.3 Types of monitoring

(a) Passive: collecting logs;

(b) Active: ping servers;

(c) Reactive: the monitoring system has reached an execute action threshold;

(d) Proactive: preventive analysis of collected data to anticipate problems.

3.4 Planning

Monitoring should be planned to cover all aspects that contribute to maintaining operations. It must include the definition of KPIs and service-level agreements (SLAs):

(a) Key performance indicators identify and measure the key metrics for operations:

  (i) Efficiency and effectiveness of a service;

  (ii) Service operation status;

  (iii) Metric-based data (cpu, uptime, memory, bandwidth, etc.);

  (iv) Learned or detected trends and bias.

(b) A service-level agreement is a document describing the level of service expected, laying out the metrics (KPIs) by which that service is measured, and the remedies or penalties that can be applied in case KPIs are not met. An SLA:

  (i) Represents the expected state of a service;

  (ii) Describes agreed and guaranteed minimal service performance;

  (iii) Establishes a condition for one or more activities that triggers a consequence.

4. ICT SERVICE CHANGE MANAGEMENT PROCEDURE

4.1 Objective

ICT service change management aims to control the lifecycle of all changes. The primary objective of this process is to enable beneficial changes to be made, with minimum disruption to ICT services.

4.2 Scope

Change management involves any new, modified or withdrawn service for:

(a) Hardware;

(b) Communication equipment and software;

(c) System software;

(d) All documentation and procedures for the running, support and maintenance of live systems.

4.3 Authority proposition

The change management process should have an owner. A group of key individuals, known as the change advisory board (CAB) advises the change manager in the assessment, prioritization and scheduling of changes. They will attend periodically scheduled meetings, address the proposed changes and review the resolved changes.

4.4 Example of change process

1. **Initiating a change**: The ICT team requests a change, formalizes the change (what, why, who, when, how) and provides information about risk, impact and costs.

2. **Filtering and assessing a change**: Management determines whether the change request should be accepted or rejected and assigns a priority to the change (emergency, high, medium, low).

3. **Authorizing a change:** CAB meetings should be organized on a regular basis to formally review and authorize changes.

4. **Testing a change**: Testing should include aspects of change such as performance, security and functionality.

5. **Change implementation**: The ICT team uses this process to implement infrastructural changes.

6. **Change closure**: The ICT team reviews the change and closes the process.

APPENDIX F. WIS IT SECURITY INCIDENT RESPONSE PROCESS

1. Reason for a process

1.1 WMO Members and cooperating organizations have used IT systems connected to each other over both private and public networks for many years.

1.2 In the past, standard data formats and single-purpose protocols reduced the risk of one Member or cooperating organization affecting another. Protocols were non-standard and locked down to a single purpose function, accessed by bespoke applications written specifically for meteorological use, probably by Members' organizations themselves. Communications were over point-to-point serial links, which had a degree of physical security.

1.3 Since then, systems and organizations have become increasingly interconnected, whether via private or public networks or in the cloud. These data pass through infrastructure that is shared globally.

1.4 Today there are more connections and a greater number of protocols and applications used than ever (for example, point-to-point use of http protocols), and many have multiple purposes. An increased use of encrypted protocols and sophisticated security solutions mitigates this risk, but not fully.

1.5 Responsibility for IT security rests clearly with the Member's organization (not WMO). Though all Members and cooperating organizations should ideally implement best IT security practices, not every Member or cooperating organization will have the same IT security requirements, nor will it adopt the same standards. WMO Members and cooperating organizations should have their own internal IT security incident management processes.

1.6 There is, therefore, a small but tangible risk that any single WMO Member or cooperating organization may pose an IT security risk to another. There is no pre-existing formal process beyond those used by WMO Members and cooperating organizations to manage their own operations.

1.7 Without a process to manage IT security issues between WMO Members and cooperating organizations, there is a risk that communications about IT security events would not be clear. As a result, wrong decisions could be taken that may affect operations unnecessarily, or open WMO Members and cooperating organizations to an increased level of risk without their knowledge.

1.8 It is best practice to be prepared for any future IT security incidents by having a WIS IT security incident reporting process (separate from the normal operational data exchange processes), and to encourage the sharing of information and expertise in IT security.

1.9 Some WMO Members or cooperating organizations may not be allowed by their governments to share information about IT security incidents. This process recognises that fact and allows for it, but encourages sharing.

2. Attributes of the WIS IT security incident reporting process

2.1 This is a simple process which allows communication about IT security incidents to be shared, reducing the risk of miscommunication.

2.2 Given the diversity of IT security experience of Members' organizations, the process is collaborative – a shared challenge in maintaining effective operation. The process is also simple to follow, to encourage its use.

2.3 This process is for the purpose of communication. It is not intended to resolve IT security problems (that lies with individual Members' organizations), but rather to allow a single authoritative voice to remove confusion and reduce misinformation following a possible incident.

2.4 WMO can, however, promote best IT security practices, such as having an IT security incident response process.

2.5 The process allows other IT security best practices to be shared and encourages "post-event" sharing of lessons learned.

2.6 The process gives a clear role to Members' organizations that operate GISCs. They will have a GISC IT Security Matters Focal Point who will act as a disseminator/collector of information for connected Members' organizations.

2.7 It should also be noted that:

(a) Detailed information on IT security incidents (current or historic);

(b) Corresponding communications between the WMO IT Security Matters Focal Point, WMO Members, cooperating organizations and the GISC IT Security Matters Focal Point (including GISC Operation Centres);

(c) Post-incident lessons learned;

shall not be made publicly available but shall remain within the WMO closed user group in the WMO IT Security Collaboration Facility unless otherwise agreed by the affected parties. Notwithstanding, such information might be used in the development of IT security best practices whilst safeguarding the identity of those affected.

2.8 It should be noted that the operational details of this process should not be published outside the WIS IT security.

3. Process resources

The resources needed to support the WIS IT security incident reporting process are defined in Table 3.

Table 3. Resources supporting the WIS IT security incident reporting process

Resource	*Description*	*Mechanism*
Lead WIS IT Security Matters Focal Points for WMO Members and cooperating organizations	To be found in the WMO Country Profile Database (CPDB). Members are responsible for keeping the content of the CPDB up to date. (Protected information)	WMO Country Profile Database
List of connections between WIS centres and GISCs	Knowledge of WIS connections. (Public information)	WMO Country Profile Database (list of WIS centres and their principal GISCs)
WMO IT Security Matters Focal Point	Provided by the WMO Secretariat. He/she should be available 24/7 for contact if required, with target response time of 1 hour (see service definitions below). (Protected information)	One agreed contact number and email address
GISC IT Security Matters Focal Point	Operational contact point for each GISC. (Protected information)	WMO Country Profile Database
WIS IT security incident severity scale	Common top-level description of the status of a security incident. (Public information)	Defined in section 4 of this process

Resource	*Description*	*Mechanism*
WIS IT Security Collaboration Facility to record and report the status of WIS IT security incidents	The WIS IT Security Collaboration Facility is a closed-group collaboration facility, administered by the WMO Secretariat. (The status of WIS IT security incidents is protected information)	WMO Country Profile Database
WIS IT Security Collaboration Facility to assign a unique identifier to an incident	WIS IT Security Collaboration Facility (see description above). (Incident identifiers are protected information)	WMO Country Profile Database
WIS IT Security Collaboration Facility to share best IT Security practice.	WIS IT Security Collaboration Facility (see description above). (Some of this information is protected, other parts are public)	WMO Country Profile Database

4. WIS IT security incident severity scale

4.1 An IT security incident can be defined as an event in the day-to-day operation of an IT service, in which a violation of the security policy may have occurred or a security safeguard may have failed.

4.2 The scale below (see Table 4) is designed to aid fast communication of the nature of an IT security event. Like the process this is lightweight and informal.

Table 4. WIS IT security incident severity scale

Incident severity	*Description*	*Suggested action (for other WMO Members' organizations)*
0	No current issue	For information only. Take no special action
1	Known local issue	No likely impact outside affected Member
2	Investigations ongoing	Severity, impact and scope unknown – maintain vigilance
3	Systems in the same security zone as the WIS centre are affected in some way	Increase vigilance
4	A system connected in some way to a WIS centre is compromised	Increase vigilance, consider risk avoidance mechanisms
5	The WIS centre is compromised	Apply appropriate operational risk avoidance mechanisms in consultation with your GISC operator.

4.3 The incident severity should initially be considered by the originator (to encourage IT security thinking), but not at the cost of significant time delay. The GISC IT Security Matters Focal Point receiving the incident report can advise as required.

4.4 The intention is that the security incident severity number is not used alone, but alongside the description, for example "Security Incident Severity 2 – Investigations Ongoing".

5. WIS IT security incident process – Action by an affected WMO Member or cooperating organization

The processes are shown below (Figures 3, 4 and 5) and are summarized here for Members' organizations:

(a) If a WMO Member or cooperating organization thinks it has an IT security incident, it should do the following:

(i) Determine how freely this information can be shared and assess the severity of the incident (using Table 4);

(ii) Report the incident and discuss it with the WMO IT Security Matters Focal Point;

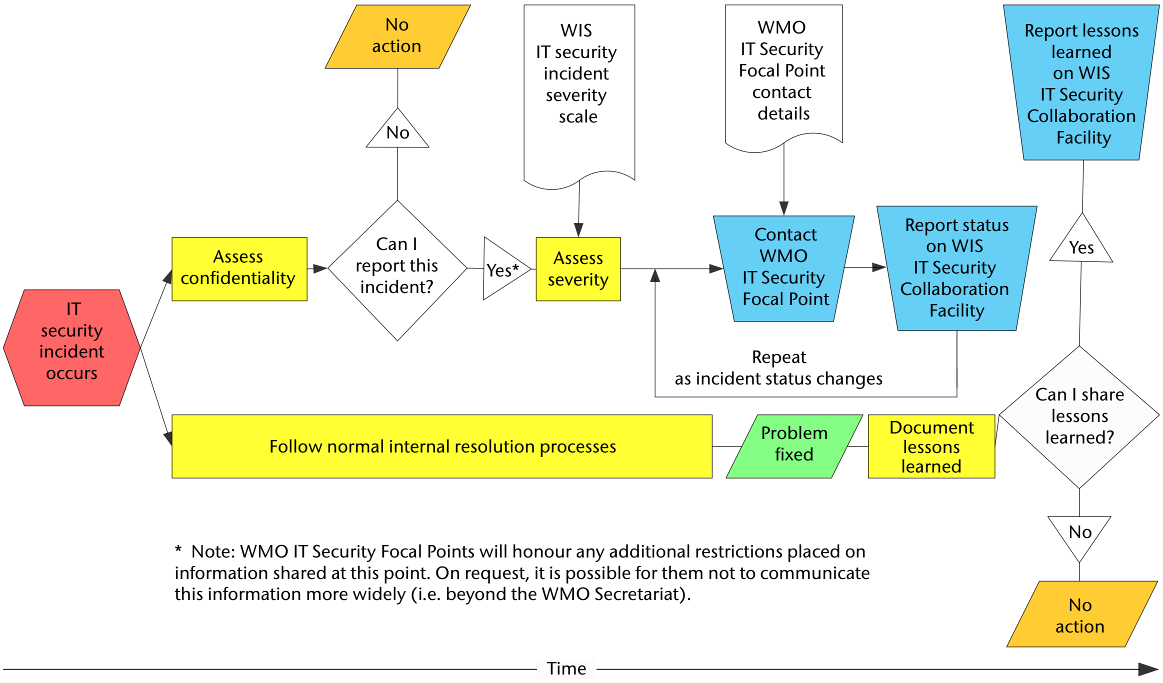
(iii) Report the incident on the WIS IT Security Collaboration Facility;

(iv) Update information on the status/severity of the incident as it changes and communicate it to the WMO IT Security Matters Focal Point and the WIS IT Security Collaboration Facility;

(v) Share lessons learned, once the incident has been resolved, on the WIS IT Security Collaboration Facility (subject to restrictions on sharing such information);

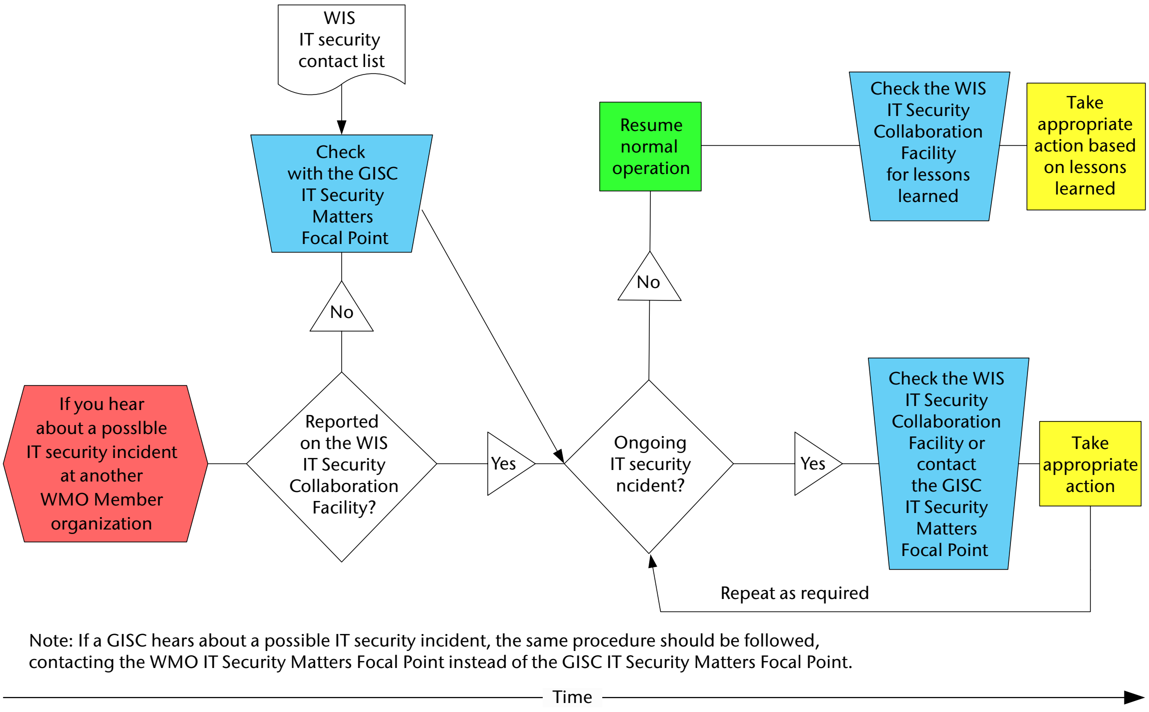
(b) If a WMO Member or cooperating organization hears there is an IT security incident, it should check the WIS IT Security Collaboration Facility and, if needed, check with its GISC IT Security Matters Focal Point and then take appropriate action;

(c) If a WMO Member or cooperating organization is contacted by its GISC IT Security Matters Focal Point about an IT security incident, it should take appropriate action as advised.


IT security incident occurs
Assess confidentiality
Can I report this incident?
No
No action
Yes*
WIS IT security incident severity scale
Assess severity
WMO IT Security Focal Point contact details
Contact WMO IT Security Focal Point
Report status on WIS IT Security Collaboration Facility
Repeat as incident status changes
Follow normal internal resolution processes
Problem fixed
Document lessons learned
Can I share lessons learned?
Yes
Report lessons learned on WIS IT Security Collaboration Facility
No
No action
Time

* Note: WMO IT Security Focal Points will honour any additional restrictions placed on information shared at this point. On request, it is possible for them not to communicate this information more widely (i.e. beyond the WMO Secretariat).

Figure 3. Procedure to be followed by an affected Member or cooperating organization



Note: If a GISC hears about a possible IT security incident, the same procedure should be followed, contacting the WMO IT Security Matters Focal Point instead of the GISC IT Security Matters Focal Point.

Figure 4. Procedure to be followed in the event of another Member or cooperating organization being affected

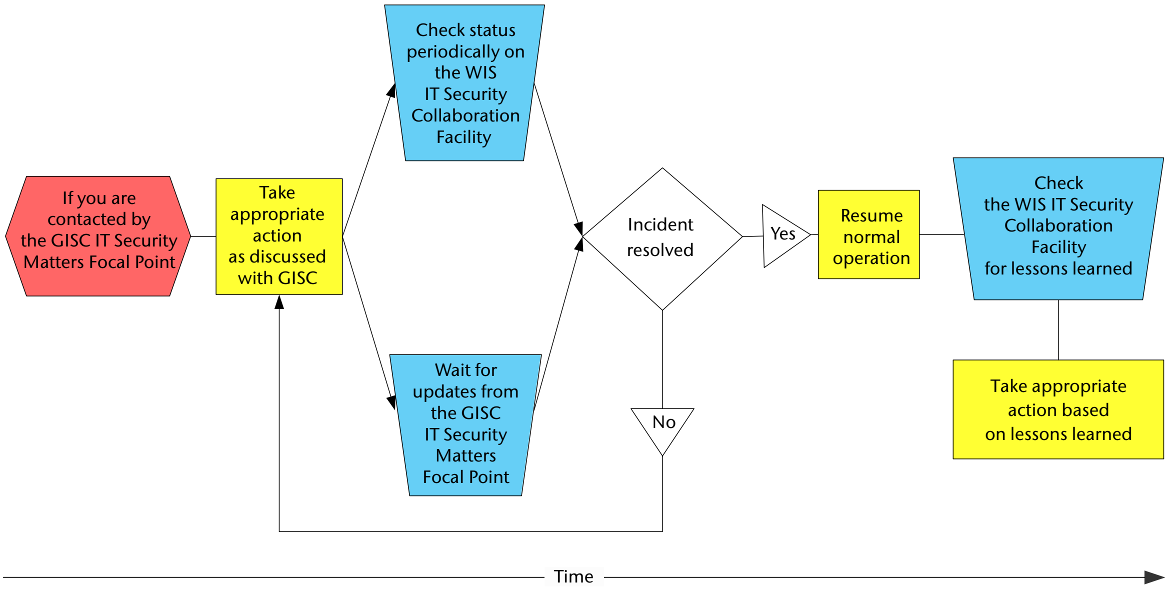


Figure 5. Procedure to be followed if a Member or cooperating organization is contacted by the GISC IT Security Matters Focal Point

6. IT security incident process - Action by the WMO IT Security Matters Focal Point

The processes are shown below (Figures 6 and 7) and are summarized here for the WMO IT Security Matters Focal Point:

(a) When the WMO IT Security Matters Focal Point receives a call from a WMO Member or cooperating organization reporting an IT security incident, he/she should:

(i) Discuss the incident with the reporting WMO Member or cooperating organization to verify the assessment of severity and extent of impact;

(ii) Assign a number to the incident so that it can be easily identified;

(iii) Understand and act upon the sensitivity for information sharing requested by the Member's organization. If the information can be shared beyond the WMO IT Security Matters Focal Point:

a. Report the incident on the WIS IT Security Collaboration Facility if the WMO Member or cooperating organization has not already done so;

b. Inform the principal GISC IT Security Matters Focal Point to which the WMO Member or cooperating organization is attached;

c. Assess potential impact and remedial action using their combined knowledge and experience, so that a single message goes out from the GISC community;

d. Inform the other relevant affected GISC IT Security Matters Focal Points of the incident;

(iv) Inform them of a change in status of the event; this information is then to be cascaded in the same manner as above.

(b) When the WMO IT Security Matters Focal Point receives a request for information about an incident from a GISC IT Security Matters Focal Point, he/she will check known incidents and respond accordingly. If there is no known incident, the WMO IT Security Matters Focal Point will contact the WMO Member or cooperating organization and, if necessary, will follow the process described under (a) above.

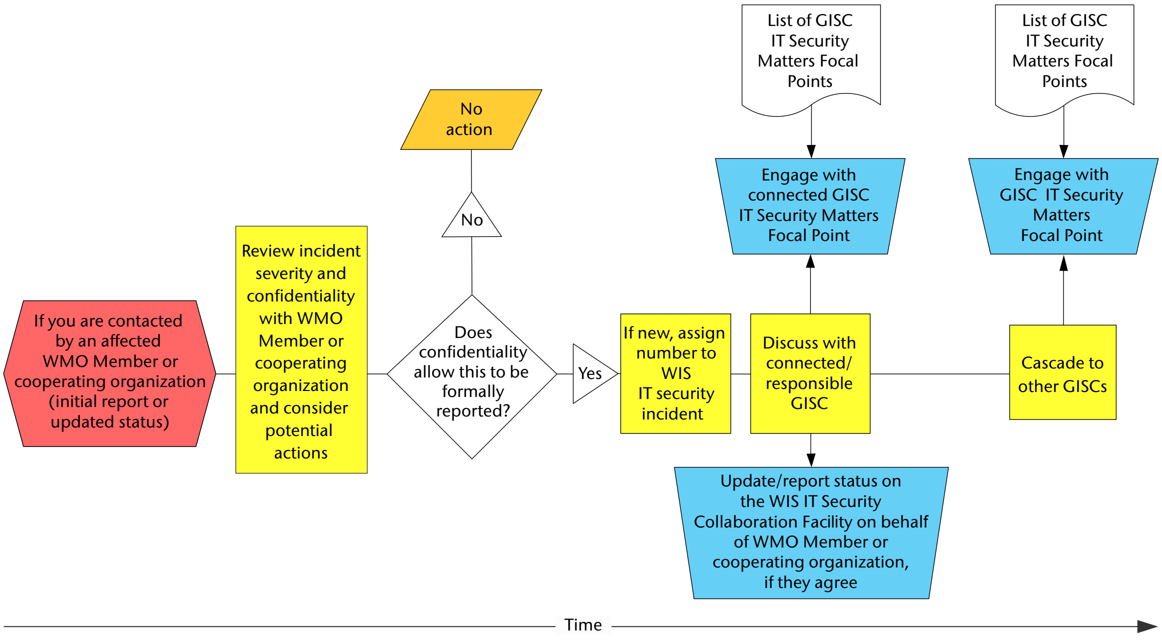

List of GISC IT Security Matters Focal Points
List of GISC IT Security Matters Focal Points
No action
No
Engage with connected GISC IT Security Matters Focal Point
Engage with GISC IT Security Matters Focal Point
Review incident severity and confidentiality with WMO Member or cooperating organization and consider potential actions
If you are contacted by an affected WMO Member or cooperating organization (initial report or updated status)
Does confidentiality allow this to be formally reported?
Yes
If new, assign number to WIS IT security incident
Discuss with connected/ responsible GISC
Cascade to other GISCs
Update/report status on the WIS IT Security Collaboration Facility on behalf of WMO Member or cooperating organization, if they agree
Time

Figure 6. Procedure to be followed by the WMO IT Security Matters Focal Point if contacted by a WMO Member or cooperating organization

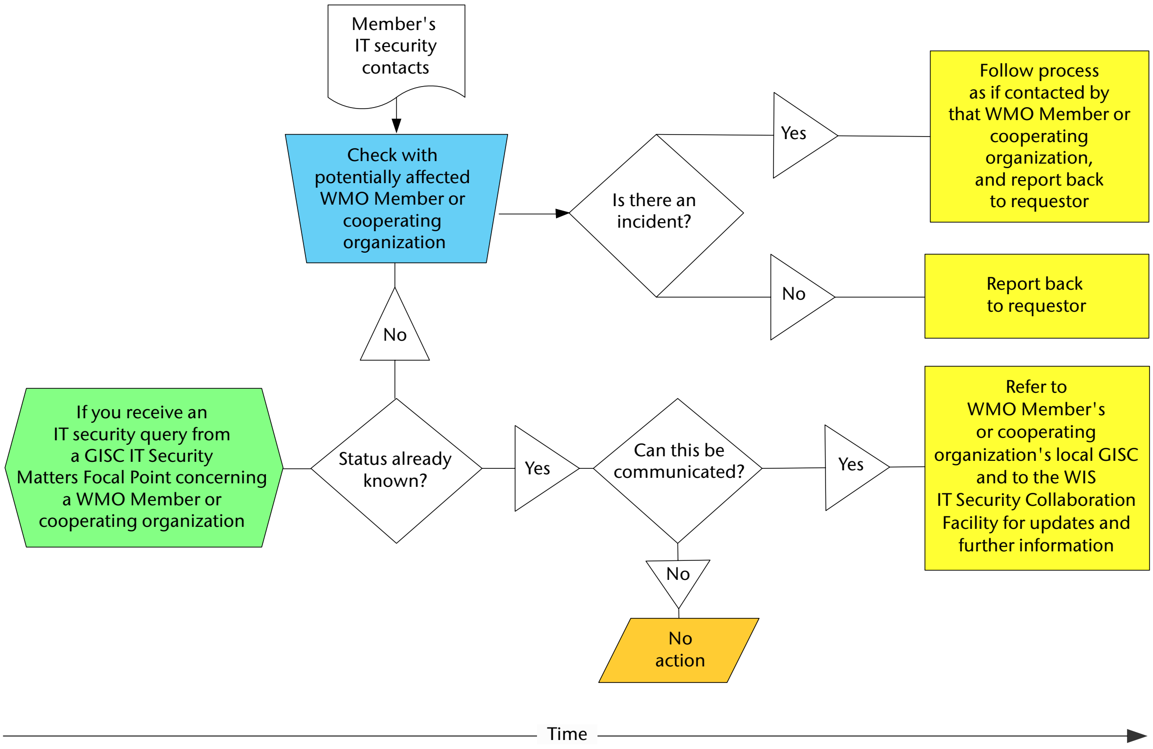

Member's IT security contacts
Check with potentially affected WMO Member or cooperating organization
Is there an incident?
Yes
Follow process as if contacted by that WMO Member or cooperating organization, and report back to requestor
No
Report back to requestor
No
If you receive an IT security query from a GISC IT Security Matters Focal Point concerning a WMO Member or cooperating organization
Status already known?
Yes
Can this be communicated?
Yes
Refer to WMO Member's or cooperating organization's local GISC and to the WIS IT Security Collaboration Facility for updates and further information
No
No action
Time

Figure 7. Procedure to be followed by the WMO IT Security Matters Focal Point if contacted by a GISC counterpart

7. IT security incident process – Action by the GISC IT Security Matters Focal Point

In many cases, it is recognized that the GISC IT Security Matters Focal Point will be the same as the GISC operational support team. The process is shown below (Figure 8) and is summarized here for the GISC IT Security Matters Focal Points:

(a) The GISC IT Security Matters Focal Point receives information from the WMO IT Security Matters Focal Point about a security incident:

(i) If this is an initial contact about an incident, he/she will discuss the potential impact and remedial action with the WMO IT Security Matters Focal Point;

(ii) Where relevant, the GISC IT Security Matters Focal Point will disseminate the information to WMO Members and cooperating organizations that are connected to the GISC;

(iii) Any updates from the WMO IT Security Matters Focal Point will be disseminated in the same way;

(b) The GISC IT Security Matters Focal Point will act as a contact point for queries about IT security incidents from those WMO Members or cooperating organizations connected to it. If the focal point receives a query about a WIS centre connected to another GISC, he/she will refer the enquirer to the information available, if this has already been published (for example, on the WIS IT Security Collaboration Facility). If the information is not available, the GISC Focal Point will contact the WMO IT Security Matters Focal Point for an answer and get back to the requester.

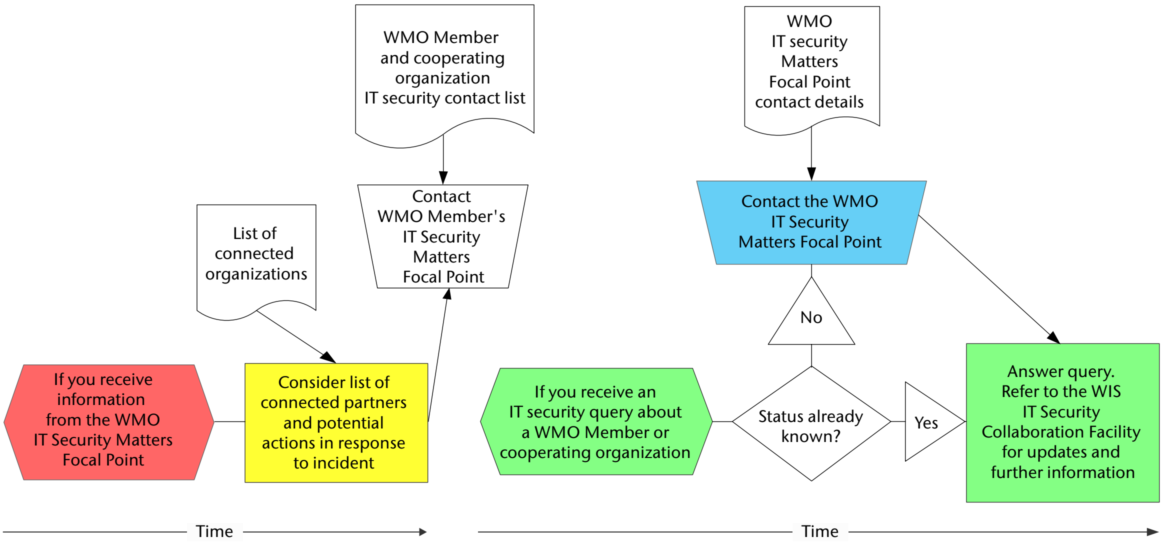

WMO Member and cooperating organization IT security contact list
Contact WMO Member's IT Security Matters Focal Point
List of connected organizations
If you receive information from the WMO IT Security Matters Focal Point
Consider list of connected partners and potential actions in response to incident
Time
WMO IT security Matters Focal Point contact details
Contact the WMO IT Security Matters Focal Point
No
If you receive an IT security query about a WMO Member or cooperating organization
Status already known?
Yes
Answer query. Refer to the WIS IT Security Collaboration Facility for updates and further information
Time

Figure 8. Procedure to be followed by the GISC IT Security Matters Focal Point if contacted by his/her WMO counterpart or by a Member or cooperating organization

8. Sharing IT security best practices

8.1 There are already some international mechanisms in place between WMO Members and cooperating organizations, such as the European Centre for Medium-range Weather Forecasts (ECMWF) Security Forum that meets annually at ECMWF. This, however, is a closed group of predominantly Region VI countries. There may be similar groups in other Regions.

8.2 The same WIS IT Security Collaboration Facility used to report and monitor WIS IT security incidents will also be used to share additional IT security information. Though a closed user group restricted to WMO Members and cooperating organizations, this is a global facility, encouraging the free exchange of information within WMO about IT security best practices, as well as existing and common threats. The exchange of information will also include the sharing by WMO Members and cooperating organizations of practical experience gained from managing IT security incidents, where this information can be shared.

9. Service definitions

9.1 Though the process is minimal, the WMO and GISC IT Security Matters Focal Points and the Lead WMO WIS IT Security Matters Focal Points are delivering a service, whose characteristics are summarized in Table 5 below.

Table 5. Service characteristics of WIS IT Security Matters Focal Points

Service aspects	*What/who?/how?*	*Comment*
Mechanism	By telephone	Submitters can place their own information on the WIS IT Security Collaboration Facility, but GISC and WMO IT Security Matters Focal Points will disseminate it personally by telephone, as well as through the WIS IT Security Collaboration Facility.
Availability	24/7	WIS centres and the WMO IT Security Matters Focal Point should have 24/7 capability.

Service aspects	*What/who?/how?*	*Comment*
Response time	Target within one hour; the GISC or WMO IT Security Matters Focal Point escalates/notifies the incident as appropriate.	Not all sites contacted will have 24/7 operations, so in some cases the response will have to wait until the centre is open.
Governance process	WMO Secretariat	Makes the resources available, monitors the effectiveness of the process, and ensures that reports are generated.
Service monitoring	The WMO Secretariat provides measurements of response time and availability.	Provides measurements and keeps the information.
Reporting	The WMO Secretariat produces an annual report on the number of incidents managed, as well as the service metrics.	To be distributed to all GISC IT Security Matters Focal Points, or made available on the WIS IT Security Collaboration Facility.

TERMS OF REFERENCE FOR WIS IT SECURITY MATTERS FOCAL POINTS

WIS IT Security Matters Focal Points

Lead WIS IT Security Matters Focal Points are nominated by the Permanent Representatives of Members with WMO. Heads of authorized non-governmental organizations (NGO) contributing to WIS may also nominate a focal point on WIS IT security matters. These focal points provide the operational channel of communication with the WMO IT Security Matters Focal Point (WMO Secretariat) and GISC IT Security Matters Focal Points.

The terms of reference for the Lead WIS IT Security Matters Focal Point are:

(a) To act as a focal point for all WIS IT security matters on the territory of the WMO Member or in the cooperating organization;

(b) To receive notifications of amendments to the *Guide to Information Technology Security* (WMO-No. 1115) and associated procedures and guidance, and to propagate the information to WIS centres on the territory of the WMO Member or to the cooperating organization;

(c) To comment on amendments to WIS IT security as defined in the *Guide to Information Technology Security* (WMO-No. 1115) and associated procedures and guidance through the fast-track procedure, on behalf of the WMO Secretariat;

(d) To request amendments to the *Guide to Information Technology Security* (WMO-No. 1115) and associated procedures and guidance concerning WIS IT Security on behalf of the WMO Secretariat;

(e) To communicate with the WMO IT Security Matters Focal Point (WMO Secretariat) and GISC IT Security Matters Focal Points on behalf of WMO on issues relating to WIS IT Security;

(f) To assist GISC IT Security Matters Focal Points in defining and carrying out functions related to WIS IT Security;

(g) To coordinate WIS IT security matters with the WIS centres of the WMO Member or cooperating organization;

(h) To receive notifications of WIS IT security incidents and other relevant information from GISC IT Security Matters Focal Points, as per established protocols;

(i) To disseminate notifications of WIS IT security incidents and other relevant information from GISC IT Security Matters Focal Points, using established protocols;

(j) To act as a central coordinating contact during a WIS IT security incident by managing communications between the WMO IT Security Matters Focal Point (WMO Secretariat), affected (or potentially affected) centres and other non-affected centres;

(k) To provide 24/7 capability for the delivery if WIS IT security functions (or delegate that task to an existing 24/7 operation).

WMO IT Security Matters Focal Point

The WIS IT Security Matters Focal Point within the WMO Secretariat is nominated by the WMO Secretariat (this is not a national role). This focal point provides the operational channel of communication between Lead WIS IT Security Matters Focal Points and GISC IT Security Matters Focal Points.

The terms of reference of the WMO IT Security Matters Focal Point, in addition to his/her role in the Secretariat, are:

(a) To communicate with the WMO Secretariat and GISC IT Security Matters Focal Points on behalf of WMO on issues relating to WIS IT Security;

(b) To assist Lead WIS IT Security Matters Focal Points within GISCs in defining and carrying out functions related to WIS IT security;

(c) To receive notifications of WIS IT security incidents, and other relevant information from GISC IT Security Matters Focal Points, using established protocols;

(d) To disseminate notifications of WIS IT security incidents and other relevant information from GISC IT Security Matters Focal Points, using established protocols;

(e) To act as a central coordinating contact during a WIS IT security incident by managing communications between the affected (or potentially affected) centres and other non-affected centres;

(f) To provide a 24/7 capability for the delivery of the WMO IT Security Matters Focal Point service described in Appendix F of this Guide;

(g) To maintain the contact details of WIS-related IT Security Matters Focal Points.

GISC IT Security Matters Focal Points

GISC IT Security Matters Focal Points are nominated by the Permanent Representatives of WMO Members that operate a GISC. These focal points provide the operational channel of communication with the WMO IT Security Matters Focal Point (the WMO Secretariat) and other Lead WIS IT Security Matters Focal Points.

The terms of reference of the GISC IT Security Matters Focal Points are:

(a) To receive notifications of amendments to the *Guide to Information Technology Security* (WMO-No. 1115) and associated procedures and guidance, and to propagate the information within their State or Territory;

(b) To comment on amendments to WIS IT security as defined in the *Guide to Information Technology Security* (WMO-No. 1115) and associated procedures and guidance through the fast-track procedure, on behalf of the Permanent Representative;

(c) To request amendments to the *Guide to Information Technology Security* (WMO-No. 1115) and associated procedures and guidance concerning WIS IT Security on behalf of the Permanent Representative;

(d) To communicate with the WMO Secretariat and the WMO IT Security Matters Focal Point on behalf of the Permanent Representative on issues relating to WIS IT Security;

(e) To assist centres within their area of responsibility in defining and carrying out functions related to WIS IT Security;

(f) To send notifications of WIS IT security incidents and other relevant information to the WIS IT Security Matters Focal Points within their area of responsibility and to GISC IT Security Matters Focal Points, using established protocols;

(g) To act as a central coordinating contact during a WIS IT security incident by managing communications with the Lead WIS IT Security Matters Focal Points within their area of responsibility, and between them and the WMO IT Security Matters Focal Point;

(h) To provide a 24/7 capability for the delivery of the GISC IT Security Matters Focal Point service described in Appendix F of this Guide.

For more information, please contact:

World Meteorological Organization

7 bis, avenue de la Paix – P.O. Box 2300 – CH 1211 Geneva 2 – Switzerland

Communication and Public Affairs Office

Tel.: +41 (0) 22 730 87 40/83 14 – Fax: +41 (0) 22 730 80 27

Email: cpa@wmo.int

public.wmo.int

JN 191194