

by depositors, GCOS would expect that the global climate repositories hold (CIV) data			WMO - WIS Manual (2023) Data Management Principle - Mapping (for reference)	GCOS Comments (General and GCOS relevance)	GCOS Recommendations (Mandatory or Optional)	Your Comments (Is this relevant? Is it applicable? Should be mandatory?)	Difficulties (describe the main difficulties you had - or would have - in complying with this CTS requirement)	Rank the difficulty: 0 - no problem 0.5 - difficult 1 - impossible
No.	Title	Description						
0	Background Information & Context	This section provides the information necessary for reviewers to fully assess the applicants' response statements. It is important to the entire application that the correct options are selected and that sufficiently detailed responses are provided.	No direct example. More the description/metadata for the system and data to which the principles apply in theory all the WMO principles link to this requirement.	This is not a requirement on the data repository itself but on the provision of information about the repository, it's context and the 'certification' process. For example: type of data, it's community, level of curation, certification process.	Mandatory. Without knowing the information and context for which the certification/assessment applies, the process is of little use and therefore redundant.			
1	Mission & Scope - The repository has an explicit mission to provide access to and preserve digital objects.	Repositories take responsibility for the curation of digital objects, and for ensuring that materials are held in the appropriate environment for appropriate periods of time. For Trustworthy Repositories it must be clear to depositors and users that active preservation and continued access to the digital objects is an explicit role of the repository.	Principle 1: Information is a valued asset Principle 2: Information must be managed Principle 8: Information management is subject to accountability and governance	Fundamental requirement for any data repository is to define what its mission is, it must provide access to the information and ensure its preservation. Required to demonstrate FAIR and key to sustainability.	Mandatory			
2	Rights Management - The repository maintains all applicable rights and monitors compliance.	The repository manages, and communicates to relevant stakeholders, all rights (permissions, prohibitions, obligations) covering data and metadata deposit, storage, preservation, access, and use. This requirement relates to the system, methods and artefacts (e.g. licenses, agreements, terms and conditions, and related policies and procedures) in place for rights management. The repository must obtain all necessary rights from the depositor, and demonstrate that there are sufficient controls in place to ensure they are applied and monitored.	Principle 2: Information must be managed Principle 7: Information should be reusable Principle 8: Information management is subject to accountability and governance	The repository acts as the interface between the data providers and the users. It also has the responsibility to document the access rights and monitor compliance. Perhaps linking the data to the WMO data policy would be sufficient for all climate data?	This might be difficult for all repositories to show compliance, especially the monitoring/controlling compliance. But at least a repository must describe the right management for the data they hold.			
3	Continuity of Service - The Repository has a plan to ensure ongoing access to and preservation of its data and metadata.	The repository must have measures in place to address the risks inherent in changing circumstances, including in mission and/or scope. This requirement covers the stable management of repository services over time (business continuity) and the response when services have problems (disaster recovery). It also includes preparations for handover of digital objects and services to another repository (succession planning). The deposit, storage, preservation, and access services offered by the repository to depositors and users are all in scope.	Principle 1: Information is a valued asset Principle 2: Information must be managed Principle 3: Information must be fit for purpose Principle 7: Information should be reusable Principle 8: Information management is subject to accountability and governance	Long-term access and sustainability. Minimum should be a risk acceptance, and a back-up plan to sustain the information should the repository not be able to continue	Mandatory			
4	Legal & Ethical - The repository ensures to the extent possible that data and metadata are created, curated, preserved, accessed and used in compliance with legal and ethical norms.	This requirement relates to repository awareness and processes around legal and ethical issues, including privacy and confidentiality, that impact the system, methods and artefacts (e.g. licenses, agreements, terms and conditions, and related policies and procedures) in place for those who agree to have their digital objects held by the repository. Evidence should demonstrate practices that reflect the legal status and sensitivity of digital objects, including guidance for depositors and users.	Principle 2: Information must be managed Principle 8: Information management is subject to accountability and governance	All repositories should understand, and document, the legal and ethical governance and issues for the data they hold.	Is this relevant to your data repository? This might be difficult for all repositories to ensure/show compliance, especially for the use. But it does say "to the extent possible". From a climate perspective we need to know political relevance			
5	Governance & Resources - The repository has adequate funding and sufficient numbers of staff managed through a clear system of governance to effectively carry out the mission.	This requirement reflects a need for transparency of financing, governance, responsibilities, and decision making. Evidence should demonstrate that the repository has a clear system of governance and sufficient human and financial resources to carry out its mission.	Principle 2: Information must be managed Principle 8: Information management is subject to accountability and governance	This is a must for a sustainable system and is fundamental for climate data repositories.	Mandatory			
6	Expertise & Guidance - The repository adopts mechanisms to secure ongoing expertise, guidance and feedback either in-house, or external.	A repository must identify the skills necessary to deliver the services it offers, and source and maintain those skills either as internal resources or through external engagement. An effective repository strives to accommodate evolution in data types, data volumes, and data rates, as well as to adopt the most effective new technologies in order to remain valuable to its Designated Community.	Principle 1: Information is a valued asset Principle 2: Information must be managed	Do all repositories provide expertise and guidance? For the curation, preservation and access this is important, but how the data is created and how it is used perhaps not a mandatory requirement.	Some aspects mandatory and some optional.			
7	Provenance and authenticity - The repository guarantees the authenticity of the digital objects and provides provenance information.	The repository should provide evidence to show that it operates a data and metadata management system that maintains provenance information to ensure authenticity from deposit, and through curation and preservation to the point of access. Any intentional changes to data and metadata should be documented, including the rationale and origin of the change. Authenticity covers reliability and provenance, including the relationship between the deposited digital objects and those provided at the point of access.	Principle 2: Information must be managed Principle 3: Information must be fit for purpose Principle 5: Information must be well documented	Very important for climate data.	Mandatory			
8	Deposit & Appraisal - The repository accepts data and metadata based on defined criteria to ensure relevance and understandability for users.	The appraisal function during deposit is critical to evaluate whether digital objects meet criteria for selection and to ensure appropriate management for their preservation. Appraisal ensures that deposited digital objects are relevant and are, or can become, understandable to the Designated Community.	Principle 2: Information must be managed Principle 3: Information must be fit for purpose Principle 5: Information must be well documented	GCOS needs to know the rules that the repository follows to accept data and metadata.	Mandatory			
9	Preservation plan - The repository assumes responsibility for long term preservation and manages this function in a planned and documented way.	The repository, depositor, and Designated Community need to understand the level of responsibility undertaken for the long term preservation of data and metadata. Procedures must be documented and their completion assured.	Principle 1: Information is a valued asset Principle 2: Information must be managed Principle 3: Information must be fit for purpose Principle 4: Information must be standardized and interoperable Principle 5: Information must be well documented	Similar to requirement 3? More explicit about the long term preservation which is a key GCOS requirement.	Mandatory			
10	Quality Assurance - The repository addresses technical quality and standards compliance, and ensures that sufficient information is available for end users to make quality-related evaluations.	Different repositories undertake different levels of curation on data, metadata and documentation depending on the needs and expectations of their depositors and Designated Community. Quality assurance by the repository ensures that digital objects comply with a range of standard criteria including acceptable formats, metadata schema, metadata content and links to other digital objects. This relates to 'technical quality' rather than the 'scientific quality' of the original digital objects creation or collection prior to deposit, though the repository must ensure there is sufficient information about the digital objects for the Designated Community to assess their fitness for use. Data, or associated metadata, may have quality issues relevant to their research value, but this does not preclude their use if a user can make a well-informed decision on their suitability through provided documentation.	Principle 1: Information is a valued asset Principle 2: Information must be managed Principle 3: Information must be fit for purpose Principle 5: Information must be well documented Principle 6: Information must be discoverable, accessible and retrievable Principle 7: Information should be reusable	Ideally yes but...	Mandatory to have a statement on the quality assurance process / Optional to provide the full quality assessment process			
11	Workflows - Digital object management takes place according to defined workflows from deposit to access.	For Quality Assurance (R10) to be achieved, it is necessary to avoid ad hoc actions and to deliver consistency of practice for all digital objects and across repository functions. This requires that workflows be defined, documented, and change-managed. Workflows may be specified in a mixture of standard operating procedures, business process descriptions and diagrams that guide normal practice and provide mechanisms for handling exceptions.	Principle 2: Information must be managed Principle 3: Information must be fit for purpose Principle 5: Information must be well documented Principle 8: Information management is subject to accountability and governance	Documentation and control management on workflows (processes)	Optional - Statement on the documentation and control management in place.			
12	Discovery and Identification - The repository enables users to discover the digital objects and refer to them in a persistent way through proper citation.	Effective data and metadata sharing discovery is key to resource discovery. Once discovered, digital objects should be referenceable through full citations, including persistent identifiers (PIDs) to help ensure that they can be accessed into the future.	Principle 4: Information must be standardized and interoperable Principle 5: Information must be well documented Principle 6: Information must be discoverable, accessible and retrievable Principle 7: Information should be reusable	How date is cited is important. Not only for the climate data but also the repository.	Mandatory			
13	Reuse - The repository enables reuse of the digital objects over time, ensuring that appropriate information is available to support understanding and use.	Repositories must ensure that data and metadata continue to be understood and used effectively into the future despite changes in technology and the Designated Community's knowledge base. This requirement evaluates the measures taken to ensure that data and metadata are reusable.	Principle 1: Information is a valued asset Principle 2: Information must be fit for purpose Principle 6: Information must be discoverable, accessible and retrievable Principle 7: Information should be reusable	Repository specific. Perhaps just a statement from the repository as how this is managed?	Optional - Statement from the repository.			
14	Storage & Integrity - The repository applies documented processes to ensure data and metadata storage and integrity.	In addition to maintaining 'archival' copies of digital objects, repositories need to store data and metadata from the point of deposit, for curation and preservation, and for access by users. For each storage location, measures should be in place to ensure that unintentional or unauthorised changes can be detected and correct versions of data and metadata recovered.	Principle 2: Information must be managed Principle 3: Information must be fit for purpose Principle 5: Information must be well documented Principle 7: Information should be reusable	Repository specific. Perhaps just a statement from the repository as how this is managed? Connected to req. No. 9	Optional - Statement from the repository.			
15	Technical Infrastructure - The repository is managed on well-supported operating systems and other core infrastructural software and hardware appropriate to the services it provides to its Designated Community.	Repositories must operate on reliable and stable core infrastructure that maximises service availability. The details of technical infrastructure will vary widely across repositories. Responses and evidence should focus on demonstrating that the repository solution, including hardware and software is well managed and appropriate to the needs of the repository functions and the Designated Community of users.	Principle 2: Information must be managed Principle 3: Information must be fit for purpose Principle 5: Information must be well documented Principle 6: Information must be discoverable, accessible and retrievable Principle 8: Information management is subject to accountability and governance	Repository specific. Perhaps just a statement from the repository as how this is managed?	Optional - Statement from the repository.			
16	Security - The repository protects the facility and its data, metadata, products, services, and users.	The repository should analyze potential threats, assess risks, and create a consistent security system. It should consider damage scenarios based on malicious actions, human error, or technical failure that pose a threat to the repository and its data, metadata, products, services, and users. It should measure the likelihood and impact of such scenarios, decide which risk levels are acceptable, and determine which measures should be taken to counter the threats to the repository and its Designated Community. This should be an ongoing process.	Principle 2: Information must be managed Principle 8: Information management is subject to accountability and governance	This was the topic of a presentation at our Bonn workshop, and security is not only important but is a significant risk. Especially in today's world of cyber crimes. All repositories should both be aware of, and implement the necessary measures for, security risks	Mandatory			

## **Principle 1: Information is a valued asset**

1.1 An information asset is information that has value. This value may be related to the cost of generating and collecting the information, a value associated with the immediate use or a value associated with the longer term preservation and subsequent reuse of the information.

1.2 This value should be recognizable and quantifiable, and the asset should have an identifiable lifecycle. Risks associated with, and to, an information asset should also be identified. As such, information management must be considered an integral part of a climate data centre's responsibilities and needs to be

## **Principle 2: Information must be managed**

2.1 An information asset must be managed throughout its lifecycle, from creation to use to eventual disposal, in a way that makes it valuable, maximizes its benefits and reflects its value in time and its different uses.

2.2 Information managers must consider the entire information lifecycle, from identifying needs and business cases to creating, quality assurance, maintenance, reuse, archiving, and disposal. Careful consideration must be given to disposal, ensuring that information is destroyed only when it has ceased to be useful for all categories of users.

## **Principle 3: Information must be fit for purpose**

3.1 Information should be developed and managed in accordance with its function and use for internal and external users.

3.2 Data centres should regularly assess information to ensure that it is fit for its purpose and that processes, procedures, and documentation are adequate.

## **Principle 4: Information must be standardized and interoperable**

4.1 Information must be stored and exchanged in standardized formats to ensure wide usability in the short and long term. It is essential for long-term archiving that information is stored in a form that can be understood and used after several decades.

4.2 Standardization is essential for structured information such as data set definitions and metadata to support interoperability.

4.3 Interoperability is essential for users to utilize information through different systems and software. Open standards help ensure interoperability with their openness and wide adoption across various communities. The use of closed and proprietary standards is strongly discouraged.

## **Principle 5: Information must be well documented**

5.1 Climate data centres should comprehensively document information processes, policies, and procedures to facilitate broad and long-term use.

5.2 Climate data centres should keep documentation up to date to ensure full traceability of processes along the information lifecycle, particularly for its creation. Previous versions of the documentation should be retained, versioned, archived and made readily available for future use. In addition, versions should be assigned a unique and persistent identifier for future unambiguous identification.

## **Principle 6: Information must be discoverable, accessible and retrievable**

6.1 Information should be easy to find through the Web, and for this purpose, the publisher should share discovery metadata with a catalogue service. The catalogue service should include a Web Application Programming Interface (API) to be used by other applications in order to offer user-tailored search portals.

6.2 For information to be easily retrievable once discovered, it should be accessible using standard data

## **Principle 7: Information should be reusable**

7.1 In order to maximize the economic benefits of an information asset it should be made as widely available and as accessible as possible.

7.2 The WMO Unified Data Policy encourages the reuse of data and information through the open and unrestricted exchange of core WMO data. The WMO encourages the free and unrestricted exchange of information in all circumstances.

7.3 The publisher should provide an explicit and well-defined license for each information item or data set as part of the associated metadata.

7.4 The Findable, Accessible, Interoperable and Reusable (FAIR) data principles promote open data with the ultimate goal of optimizing reuse of data. These principles should be followed where possible. Note:

## **Principle 8: Information management is subject to accountability and governance.**

8.1 Information management processes must be governed as the information moves through its lifecycle. All information must have a designated owner, steward, curator and custodian. These roles may be invested in the same person but should be clearly defined at the time of creation. A climate data centre with responsibility for managing information should ascertain:

- General information management practices, procedures and protocols, including well-defined roles, responsibilities and restrictions on managing the information;
- Definition and enforcement of appropriate retention policy, taking into account stakeholder needs and variations in value over the information lifecycle;
- Licensing and defining and enforcing any access restrictions.

8.2 The designated owner should have budget and decision-making authority about preservation and data