

**Draft Recommendation for
Space Data System Practices**

REQUIREMENTS FOR BODIES
PROVIDING AUDIT AND
CERTIFICATION OF CANDIDATE
TRUSTWORTHY DIGITAL
REPOSITORIES
~~REQUIREMENTS FOR
BODIES PROVIDING AUDIT AND
CERTIFICATION OF TRUSTWORTHY
DIGITAL REPOSITORIES~~

DRAFT RECOMMENDED PRACTICE

CCSDS 000.0-R-0

RED BOOK
January 2010

DRAFT CCSDS RECOMMENDED PRACTICE FOR REQUIREMENTS FOR BODIES
PROVIDING AUDIT AND CERTIFICATION OF CANDIDATE TRUSTWORTHY DIGITAL
REPOSITORIES~~(SUBJECT)~~

AUTHORITY

Issue:	Red Book, Issue 1
Date:	January 2010
Location:	Not Applicable

**(WHEN THIS RECOMMENDED PRACTICE IS FINALIZED, IT WILL CONTAIN
THE FOLLOWING STATEMENT OF AUTHORITY:)**

This document has been approved for publication by the Management Council of the Consultative Committee for Space Data Systems (CCSDS) and represents the consensus technical agreement of the participating CCSDS Member Agencies. The procedure for review and authorization of CCSDS documents is detailed in the *Procedures Manual for the Consultative Committee for Space Data Systems*, and the record of Agency participation in the authorization of this document can be obtained from the CCSDS Secretariat at the address below.

This document is published and maintained by:

CCSDS Secretariat
Space Communications and Navigation Office, 7L70
Space Operations Mission Directorate
NASA Headquarters
Washington, DC 20546-0001, USA

STATEMENT OF INTENT

(WHEN THIS RECOMMENDED PRACTICE IS FINALIZED, IT WILL CONTAIN THE FOLLOWING STATEMENT OF INTENT:)

The Consultative Committee for Space Data Systems (CCSDS) is an organization officially established by the management of its members. The Committee meets periodically to address data systems problems that are common to all participants, and to formulate sound technical solutions to these problems. Inasmuch as participation in the CCSDS is completely voluntary, the results of Committee actions are termed **Recommendations** and are not considered binding on any Agency.

This **Recommended Practice** is issued by, and represents the consensus of, the CCSDS members. Endorsement of this **Recommended Practice** is entirely voluntary. Endorsement, however, indicates the following understandings:

- o Whenever a member establishes a CCSDS-related **practice**, this **practice should** be in accord with the relevant **Recommended Practice**. Establishing such a **practice** does not preclude other provisions which a member may develop.
- o Whenever a member establishes a CCSDS-related **practice**, that member will provide other CCSDS members with the following information:
 - The **practice** itself.
 - The anticipated date of initial operational capability.
 - The anticipated duration of operational service.
- o Specific service arrangements shall be made via memoranda of agreement. Neither this **Recommended Practice** nor any ensuing **practice** is a substitute for a memorandum of agreement.

No later than five years from its date of issuance, this **Recommended Practice** will be reviewed by the CCSDS to determine whether it should: (1) remain in effect without change; (2) be changed to reflect the impact of new technologies, new requirements, or new directions; or (3) be retired or canceled.

In those instances when a new version of a **Recommended Practice** is issued, existing CCSDS-related member Practices and implementations are not negated or deemed to be non-CCSDS compatible. It is the responsibility of each member to determine when such Practices or implementations are to be modified. Each member is, however, strongly encouraged to direct planning for its new Practices and implementations towards the later version of the Recommended Practice.

DRAFT CCSDS RECOMMENDED PRACTICE FOR REQUIREMENTS FOR BODIES
PROVIDING AUDIT AND CERTIFICATION OF CANDIDATE TRUSTWORTHY DIGITAL
REPOSITORIES~~(SUBJECT)~~

FOREWORD

This document is a technical Recommendation to use for setting the requirements for bodies providing audit and certification of trustworthy digital repositories.

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This Recommended Practice is therefore subject to CCSDS document management and change control procedures, which are defined in the *Procedures Manual for the Consultative Committee for Space Data Systems*. Current versions of CCSDS documents are maintained at the CCSDS Web site:

<http://www.ccsds.org/>

Questions relating to the contents or status of this document should be addressed to the CCSDS Secretariat at the address indicated on page i.

DRAFT CCSDS RECOMMENDED PRACTICE FOR REQUIREMENTS FOR BODIES
PROVIDING AUDIT AND CERTIFICATION OF CANDIDATE TRUSTWORTHY DIGITAL
REPOSITORIES{SUBJECT}

At time of publication, the active Member and Observer Agencies of the CCSDS were:

Member Agencies

- Agenzia Spaziale Italiana (ASI)/Italy.
- British National Space Centre (BNSC)/United Kingdom.
- Canadian Space Agency (CSA)/Canada.
- Centre National d'Etudes Spatiales (CNES)/France.
- China National Space Administration (CNSA)/People's Republic of China.
- Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)/Germany.
- European Space Agency (ESA)/Europe.
- Russian Federal Space Agency (RFSA)/Russian Federation.
- Instituto Nacional de Pesquisas Espaciais (INPE)/Brazil.
- Japan Aerospace Exploration Agency (JAXA)/Japan.
- National Aeronautics and Space Administration (NASA)/USA.

Observer Agencies

- Austrian Space Agency (ASA)/Austria.
- Belgian Federal Science Policy Office (BFSP0)/Belgium.
- Central Research Institute of Machine Building (TsNIIMash)/Russian Federation.
- Centro Tecnico Aeroespacial (CTA)/Brazil.
- Chinese Academy of Sciences (CAS)/China.
- Chinese Academy of Space Technology (CAST)/China.
- Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
- Danish National Space Center (DNSC)/Denmark.
- European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)/Europe.
- European Telecommunications Satellite Organization (EUTELSAT)/Europe.
- Hellenic National Space Committee (HNSC)/Greece.
- Indian Space Research Organization (ISRO)/India.
- Institute of Space Research (IKI)/Russian Federation.
- KFKI Research Institute for Particle & Nuclear Physics (KFKI)/Hungary.
- Korea Aerospace Research Institute (KARI)/Korea.
- CSIR Satellite Applications Centre (CSIR)/Republic of South Africa.
- Ministry of Communications (MOC)/Israel.
- National Institute of Information and Communications Technology (NICT)/Japan.
- National Oceanic and Atmospheric Administration (NOAA)/USA.
- National Space Organization (NSPO)/Chinese Taipei.
- Naval Center for Space Technology (NCST)/USA.
- Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
- Swedish Space Corporation (SSC)/Sweden.
- United States Geological Survey (USGS)/USA.

DRAFT CCSDS RECOMMENDED PRACTICE FOR REQUIREMENTS FOR BODIES
PROVIDING AUDIT AND CERTIFICATION OF CANDIDATE TRUSTWORTHY DIGITAL
REPOSITORIES~~(SUBJECT)~~

PREFACE

This document is a draft CCSDS Recommended Practice. Its 'Red Book' status indicates that the CCSDS believes the document to be technically mature and has released it for formal review by appropriate technical organizations. As such, its technical contents are not stable, and several iterations of it may occur in response to comments received during the review process.

Implementers are cautioned **not** to fabricate any final equipment in accordance with this document's technical content.

DRAFT CCSDS RECOMMENDED PRACTICE FOR REQUIREMENTS FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF CANDIDATE TRUSTWORTHY DIGITAL REPOSITORIES~~{SUBJECT}~~

DOCUMENT CONTROL

Document	Title and Issue	Date	Status
CCSDS 000.0-R-0	Requirements for bodies providing audit and certification of trustworthy digital repositories, Draft Recommended Practice, Issue 1	January 2010	Current draft

Contents

DOCUMENT CONTROL	VI
1 INTRODUCTION	1-0
1.1 PURPOSE	1-0
1.2 SCOPE	1-0
1.3 APPLICABILITY	1-0
1.4 RATIONALE	1-0
1.5 STRUCTURE OF THIS DOCUMENT	1-1
1.6 SECURITY CONSIDERATIONS	1-1
1.7 DEFINITIONS	1-1
1.7.1 ACRONYMS AND ABBREVIATIONS	1-1
1.7.2 TERMINOLOGY	1-1
1.7.3 NOMENCLATURE	1-3
1.8 CONFORMANCE	1-3
1.9 REFERENCES	1-3
2 OVERVIEW	2-1
3 GOOD PRACTICE	3-2
4 PRINCIPLES	4-3
5 GENERAL REQUIREMENTS	5-45-6
5.1 LEGAL AND CONTRACTUAL MATTERS	5-45-6
5.2 MANAGEMENT OF IMPARTIALITY	5-45-6
5.2.1 TDR 5.2 CONFLICTS OF INTEREST	5-45-8
5.3 LIABILITY AND FINANCING	5-55-9
6 STRUCTURAL REQUIREMENTS	6-66-10
6.1 ORGANIZATIONAL STRUCTURE AND TOP MANAGEMENT	6-66-10
6.2 COMMITTEE FOR SAFEGUARDING IMPARTIALITY	6-66-10
7 RESOURCE REQUIREMENTS	7-77-12
7.1 COMPETENCE OF MANAGEMENT AND PERSONNEL	7-77-12
7.1.1 TDR 7.1 MANAGEMENT COMPETENCE	7-77-12
7.2 PERSONNEL INVOLVED IN THE CERTIFICATION ACTIVITIES	7-87-13
7.2.1 TDR 7.2 COMPETENCE OF CERTIFICATION BODY PERSONNEL	7-87-14
7.3 USE OF INDIVIDUAL EXTERNAL AUDITORS AND EXTERNAL TECHNICAL EXPERTS	7-107-17
7.3.1 TDR 7.3 USING EXTERNAL AUDITORS OR EXTERNAL TECHNICAL EXPERTS AS PART OF THE AUDIT TEAM	7-117-17
7.4 PERSONNEL RECORDS	7-117-18
7.5 OUTSOURCING	7-117-18
8 INFORMATION REQUIREMENTS	8-128-19
8.1 PUBLICLY ACCESSIBLE INFORMATION	8-128-19
8.1.1 TDR 8.1 PROCEDURES FOR GRANTING, MAINTAINING, EXTENDING, REDUCING, SUSPENDING AND WITHDRAWING CERTIFICATION	8-128-19
8.2 CERTIFICATION DOCUMENTS	8-128-19
8.2.1 TDR 8.2 TDR CERTIFICATION DOCUMENTS	8-128-20

DRAFT CCSDS RECOMMENDED PRACTICE FOR **REQUIREMENTS FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF CANDIDATE TRUSTWORTHY DIGITAL REPOSITORIES**~~{SUBJECT}~~

8.3	DIRECTORY OF CERTIFIED CLIENTS.....	8-128-20
8.4	REFERENCE TO CERTIFICATION AND USE OF MARKS	8-138-21
8.4.1	TDR 8.4 CONTROL OF CERTIFICATION MARKS	8-138-21
8.5	CONFIDENTIALITY	8-138-22
8.5.1	TDR 8.5 ACCESS TO ORGANIZATIONAL RECORDS	8-138-22
8.6	INFORMATION EXCHANGE BETWEEN A CERTIFICATION BODY AND ITS CLIENTS	8-138-23
9	PROCESS REQUIREMENTS	9-149-25
9.1	9.1 GENERAL REQUIREMENTS	9-149-25
9.1.1	TDR 9.1.1 GENERAL TDR AUDIT REQUIREMENTS.....	9-149-27
9.1.2	TDR 9.1.2 SCOPE OF CERTIFICATION	9-149-28
9.1.3	TDR 9.1.3 AUDIT TIME.....	9-159-28
9.1.4	TDR 9.1.4 MULTIPLE SITES.....	9-169-29
9.1.5	TDR 9.1.5 AUDIT METHODOLOGY	9-179-30
9.1.6	TDR 9.1.6 CERTIFICATION AUDIT REPORT	9-179-31
9.2	INITIAL AUDIT AND CERTIFICATION.....	9-209-33
9.2.1	TDR 9.2.1 AUDIT TEAM COMPETENCE	9-209-36
9.2.2	TDR 9.2.2 GENERAL PREPARATIONS FOR THE INITIAL AUDIT.....	9-219-37
9.2.3	TDR 9.2.3 INITIAL CERTIFICATION AUDIT	9-229-37
9.2.4	TDR 9.2.4 INFORMATION FOR GRANTING INITIAL CERTIFICATION	9-249-40
9.2.5	TDR 9.2.5 CERTIFICATION DECISION.....	9-249-40
9.3	9.3 SURVEILLANCE ACTIVITIES.....	9-269-42
9.3.1	TDR 9.3 SURVEILLANCE AUDITS.....	9-269-43
9.4	RECERTIFICATION.....	9-279-44
9.4.1	TDR 9.4 RECERTIFICATION AUDITS.....	9-279-45
9.5	9.5 SPECIAL AUDITS	9-289-46
9.5.1	TDR 9.5 SPECIAL CASES	9-289-46
9.6	SUSPENDING, WITHDRAWING OR REDUCING SCOPE OF CERTIFICATION	9-299-47
9.7	APPEALS	9-309-48
9.8	COMPLAINTS	9-319-49
9.8.1	TDR 9.8 COMPLAINTS	9-319-50
9.9	RECORDS OF APPLICANTS AND CLIENTS	9-319-50
10	MANAGEMENT SYSTEM REQUIREMENTS FOR CERTIFICATION BODIES 10-3210-52	
10.1	OPTIONS.....	10-3210-52
10.2	OPTION 1 – MANAGEMENT SYSTEM REQUIREMENTS IN ACCORDANCE WITH ISO 9001	10-3210-52
10.3	OPTION 2 – GENERAL MANAGEMENT SYSTEM REQUIREMENTS.....	10-3310-53
10.3.1	TDR 10.3 TDR IMPLEMENTATION.....	10-3310-56
11	SECURITY.....	11-1
11.1	INTRODUCTION.....	11-1
11.2	SECURITY CONCERNS WITH RESPECT TO THE CCSDS DOCUMENT ..	11-1
11.3	POTENTIAL THREATS AND ATTACK SCENARIOS.....	11-1
11.4	CONSEQUENCES OF NOT APPLYING SECURITY TO THE TECHNOLOGY	11-1

DRAFT CCSDS RECOMMENDED PRACTICE FOR REQUIREMENTS FOR BODIES
PROVIDING AUDIT AND CERTIFICATION OF CANDIDATE TRUSTWORTHY DIGITAL
REPOSITORIES~~(SUBJECT)~~

DRAFT CCSDS RECOMMENDED PRACTICE FOR REQUIREMENTS FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF CANDIDATE TRUSTWORTHY DIGITAL REPOSITORIES~~{SUBJECT}~~

1 INTRODUCTION

1.1 PURPOSE

The main purpose of this document is to define a CCSDS Recommended Practice on which to base the operations of the organization(s) which performs audits for assessing the trustworthiness of digital repositories using [1] and provides the appropriate certification.

Comment [mc1]: Do we need to revise the title of this document?

1.2 SCOPE

This International Standard specifies requirements and provides guidance for bodies providing audit and certification of a trustworthy digital repository (TDR), ~~in addition to based on~~ the requirements contained within ISO/IEC 17021 and <ISO XXXXX - RAC Document>. It is primarily intended to support the accreditation of certification bodies providing TDR certification.

Comment [DG2]: Agreed 20100125

Comment [mc3]: Do we need to revise the title of this document?

The requirements contained in this International Standard need to be demonstrated in terms of competence and reliability by any body providing TDR certification, ~~and the guidance contained in this International Standard provides additional interpretation of these requirements for any body providing TDR certification.~~

Comment [mc4]: The RAC document?

Comment [DG5]: 20100308

1.3 APPLICABILITY

This document is meant primarily for those setting up and managing the organization performing the auditing and certification of digital repositories.

It should also be of use to those who work in or are responsible for digital repositories seeking objective measurement of the trustworthiness of their repository and wishing to understand the processes involved, although it is recognized that not all digital repositories will need to undergo such third party audit and certification.

1.4 RATIONALE

There is a hierarchy of standards concerned with good auditing practice [3]-[6]. This document is positioned within this hierarchy in order to ensure that these good practices can be applied to the evaluation of TDRs.

Comment [mc6]: digital repositories?

ISO/IEC 17021 [6] is an International Standard which sets out criteria for bodies operating audit and certification of organizations' management systems. If such bodies are to be accredited as complying with ISO/IEC 17021 with the objective of auditing and certifying Trusted Digital Repositories (TDR) in accordance with <ISO XXXXX - RAC Document>, some ~~additional~~ requirements and guidance ~~that are additional~~ to ISO/IEC 17021 are necessary.

Comment [mc7]: Trustworthy?

Comment [DG8]: HT20100308

These are provided by this International Standard.

DRAFT CCSDS RECOMMENDED PRACTICE FOR REQUIREMENTS FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF CANDIDATE TRUSTWORTHY DIGITAL REPOSITORIES~~(SUBJECT)~~

The text in this International Standard follows the structure of ISO/IEC 17021, and the additional TDR-specific requirements and guidance on the application of ISO/IEC 17021 for TDR certification are identified by the letters “TDR”.

Comment [mc9]: What does this mean? I thought we were preparing a document with only the additional requirements for auditing TDRs?

1.5 STRUCTURE OF THIS DOCUMENT

This document is divided into informative and normative sections and annexes.

Sections 1-2 of this document are informative and give a high level view of the rationale, the conceptual environment, some of the important design issues and an introduction to the terminology and concepts.

- Section 1 gives purpose and scope, rationale, a view of the overall document structure, and the acronym list, glossary, and reference list for this document.
- Section 2 provides an overview of auditing practices.
- Sections 3 to 10 provide the normative metrics against which an organization providing audit and certification of TDRs may be judged.
- Annex A provides Informative References (XXX – if any).

Comment [mc10]: Isn't this normative information?

1.6 SECURITY CONSIDERATIONS

Additional security considerations are dealt with in informational section 11.

1.7 DEFINITIONS

1.7.1 ACRONYMS AND ABBREVIATIONS

CCSDS	Consultative Committee for Space Data Systems
ISO	International Organization for Standardization
OAIS	Open Archival Information System
TDR	Trustworthy Digital Repository

1.7.2 TERMINOLOGY

Digital preservation interests a range of different communities, each with a distinct vocabulary and local definitions for key terms. A glossary is included in this document, but it is important to draw attention to the usage of several key terms.

In general, key terms in this document have been adopted from the OAIS Reference Model. One of the great strengths of the OAIS Reference Model [2] has been to provide a common terminology made up of terms “not already overloaded with meaning so as to reduce conveying unintended meanings”. Because the OAIS has become a foundational document for

DRAFT CCSDS RECOMMENDED PRACTICE FOR REQUIREMENTS FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF CANDIDATE TRUSTWORTHY DIGITAL REPOSITORIES~~{SUBJECT}~~

digital preservation, the common terms are well understood and are therefore used within this document.

The OAIS Reference Model uses “digital archive” to mean the organization responsible for digital preservation. In this document, the term “repository” or phrase “digital repository” is used to convey the same concept in all instances except when quoting from the OAIS. It is important to understand that in all instances in this document, “repository” and “digital repository” are used to convey digital repositories and archives that have, or contribute to, long-term preservation responsibilities and functionality. This document uses the OAIS concept of the “Designated Community.” A repository may have a single, generalized “Designated Community” (e.g., every citizen of a country), while other repositories may have several, distinct Designated Communities with highly specialized needs, each requiring different functionality or support from the repository; this document uses the term Designated Community to cover this second case also.

The term “Trustworthy Digital Repository” (TDR) is used in this document to indicate those repositories which are either already certified or else are potential candidates for such certification: sometimes the wording “the repository being audited” is used.

1.7.2.1 Glossary

For the purposes of this document, the terms and definitions given in ISO/IEC 17021, <ISO XXXXX - RAC Document> and the following apply.

Certificate: certificate issued by a certification body in accordance with the conditions of its accreditation and bearing an accreditation symbol or statement

Certification body: third party that assesses and certifies the TDR of a client organization with respect to published TDR standards, and any supplementary documentation required under the system

Certification document: document indicating that a client organization’s TDR conforms to specified TDR standards and any supplementary documentation required under the system

Initial audit committee: The initial audit committee will consist of internationally recognized experts in digital preservation, the membership building on members of the authors of the <ISO XXXXX - RAC Document

Mark: legally registered trade mark or otherwise protected symbol which is issued under the rules of an accreditation body or of a certification body, indicating that adequate confidence in the systems operated by a body has been demonstrated or that relevant products or individuals conform to the requirements of a specified standard

Organization: company, corporation, firm, enterprise, authority or institution, or part or combination thereof, whether incorporated or not, public or private, that has its own functions and administration and is able to ensure that digital preservation is exercised

Comment [mc11]: No! The term trustworthy digital repository should only apply to repositories that have already been certified. Using this term for candidate repositories as well only serves as a source of confusion.

Comment [mc12]: document?

Comment [mc13]: candidate repository?

Comment [mc14]: repository

DRAFT CCSDS RECOMMENDED PRACTICE FOR REQUIREMENTS FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF CANDIDATE TRUSTWORTHY DIGITAL REPOSITORIES~~(SUBJECT)~~

1.7.3 NOMENCLATURE

The following conventions apply throughout this Recommended Practice:

- a) the words ‘shall’ and ‘must’ imply a binding and verifiable specification;
- b) the word ‘should’ implies an optional, but desirable, specification;
- c) the word ‘may’ implies an optional specification;
- d) the words ‘is’, ‘are’, and ‘will’ imply statements of fact.”

1.8 CONFORMANCE

An organization which provides audit and certification for the repository being audited~~TDRs~~ conforms to this recommended practice if it fulfils all the binding and verifiable specifications in this document.

Comment [mc15]: Actually this one should be TDR.

1.9 REFERENCES

The following documents contain provisions which, through reference in this text, constitute provisions of this Recommended Standard. At the time of publication, the editions indicated were valid. All documents are subject to revision, and users of this Recommended Practice are encouraged to investigate the possibility of applying the most recent editions of the documents indicated below. The CCSDS Secretariat maintains a register of currently valid CCSDS Recommended Standards.

- [1] CCSDS XXXX Audit and certification of Trustworthy Digital Repositories
- [2] Consultative Committee for Space Data Systems (CCSDS). 2002. Reference Model for an Open Archival Information System. (ISO Standard 14721). <http://www.ccsds.org/publications/archive/650x0b1.pdf> or later version.
- [3] ISO 9000:2005, Quality management systems — Fundamentals and vocabulary
- [4] ISO 19011:2002, Guidelines for quality and/or environmental management systems auditing1)
- [5] ISO/IEC 17021:2006, Conformity assessment — Requirements for bodies providing audit and certification of management systems
- [6] ISO/IEC 17000:2004, Conformity assessment — Vocabulary and general principles

NOTE – Informative references are listed in annex **B**

Comment [mc16]: A? See 1.5 above.

2 OVERVIEW

This document addresses issues arising from applying good audit practice to auditing and certifying whether and to what extent digital repositories can be trusted to look after digitally encoded information for the long-term, or at least for the period of their custodianship of that digitally encoded information.

It covers principles needed to inspire confidence that third party certification of the management of the digital repository has been performed with

- impartiality,
- competence,
- responsibility,
- openness,
- confidentiality, and
- responsiveness to complaints

This document specifies the ways of ensuring that these the body providing such third party certification can inspire this confidence. It does this by building on the more general specifications of standards [4]-[6].

Section 5 deals with the legal aspects and guarantees of impartiality and avoidance of conflicts of interest.

The structure and management of the organization is specified in section 6, which is supported by the competences of the management and personnel, specified in section 7.

Section 8 sets out how the information about which organizations have been certified is made available.

The requirements on the procedures for defining the scope and performance of the audit, the initial certification decision and the ways in which that certification may be confirmed, reduced in scope, suspended or withdrawn are given in section 9. This section also specified who complaints are dealt with.

Comment [mc17]: What does this mean?

Comment [mc18]: Words missing?

The management system of the auditing body itself is specified in section 10.

DRAFT CCSDS RECOMMENDED PRACTICE FOR REQUIREMENTS FOR BODIES
PROVIDING AUDIT AND CERTIFICATION OF CANDIDATE TRUSTWORTHY DIGITAL
REPOSITORIES~~{SUBJECT}~~

3 GOOD PRACTICE

XXX PLACE HOLDER – MAY BE DELETED TO MAKE NUMBERING CONSISTENT

4 PRINCIPLES

The principles from ISO/IEC 17021:2006, Clause 4 apply.

5 GENERAL REQUIREMENTS

5.1 LEGAL AND CONTRACTUAL MATTERS

The requirements from ISO/IEC 17021:2006, Clause 5.1 apply.

5.2 5.2 MANAGEMENT OF IMPARTIALITY

The requirements from ISO/IEC 17021:2006, Clause 5.2 apply. In addition, the following TDR-specific requirements and guidance apply.

5.2.1 TDR 5.2 CONFLICTS OF INTEREST

Certification bodies can carry out the following duties without them being considered as consultancy or having a potential conflict of interest:

- a) certification, including information meetings, planning meetings, examination of documents, auditing (not internal TDR auditing or internal TDR reviews) and follow up of non-conformities;
- b) arranging and participating as a lecturer in training courses, provided that, where these courses relate to digital preservation management, related management systems or auditing, certification bodies should confine themselves to the provision of generic information and advice which is freely available in the public domain, i.e. they should not provide company-specific advice which contravenes the requirements of c) below;
- c) making available or publishing on request information describing the certification body's interpretation of the requirements of the certification audit standards;
- d) activities prior to audit, solely aimed at determining readiness for certification audit; however, such activities should not result in the provision of recommendations or advice that would contravene this clause and the certification body should be able to confirm that such activities do not contravene these requirements and that they are not used to justify a reduction in the eventual certification audit duration;
- e) performing second and third party audits according to standards or regulations other than those being part of the scope of accreditation;
- f) adding value during certification audits and surveillance visits, e.g., by identifying opportunities for improvement, as they become evident during the audit, without recommending specific solutions. The certification body shall be independent from the body or bodies (including any individuals) which provide the internal TDR audit of the client organization's TDR subject to certification.

Comment [mc19]: What does this mean?

Comment [mc20]: Under 17021:2006 isn't the certification body required to do this?

Comment [mc21]: Why do we want to have this exception/exclusion?

Comment [mc22]: What does this term mean? Where is it defined?

Comment [mc23]: candidate repository?

5.3 LIABILITY AND FINANCING

The requirements from ISO/IEC 17021:2006, Clause 5.3 apply.

6 STRUCTURAL REQUIREMENTS

6.1 ORGANIZATIONAL STRUCTURE AND TOP MANAGEMENT

The requirements from ISO/IEC 17021:2006, Clause 6.1 apply.

6.2 COMMITTEE FOR SAFEGUARDING IMPARTIALITY

The requirements from ISO/IEC 17021:2006, Clause 6.2 apply.

7 RESOURCE REQUIREMENTS

7.1 COMPETENCE OF MANAGEMENT AND PERSONNEL

The requirements from ISO/IEC 17021:2006, Clause 7.1 apply. In addition, the following TDR-specific requirements and guidance apply.

7.1.1 TDR 7.1 MANAGEMENT COMPETENCE

The essential elements of competence required to perform TDR certification are to select, provide and manage those individuals whose skills and collective competence is appropriate to the activities to be audited and the related digital preservation issues.

7.1.1.1 Competence analysis and contract review

The certification body shall ensure that it has knowledge of the technological and legal developments relevant to the TDR of the client organization, which it assesses. The certification body shall have an effective system for the analysis of the competencies in digital preservation management which it needs to have available, with respect to all the technical areas in which it operates.

Comment [mc24]: candidate repository?

For each client, the certification body shall be able to demonstrate that it has performed a competence analysis (assessment of skills in response to evaluated needs) of the requirements of each relevant sector prior to undertaking the contract review. The certification body shall then review the contract with the client organization, based on the results of this competence analysis. In particular, the certification body shall be able to demonstrate that it has the competence to complete the following activities:

- a) understand the areas of activity of the client organization and the associated business risks;
- b) define the competencies needed in the certification body to certify in relation to the identified activities, and digital preservation related threats to assets, vulnerabilities and impacts on the client organization;
- c) confirm the availability of the required competencies.

Comment [SCL25]: Might need to rephrase this.

Comment [mc26]: Why is this necessary? See 17021, Clause 7.2.

7.1.1.2 Resources

The management of the certification body shall have the necessary processes and resources to enable it to determine whether or not individual auditors are competent for the tasks they are required to perform within the scope of certification in which they are operating. The competence of auditors may be established by verified background experience and specific training or briefing (see also Annex B). The

Comment [mc27]: There is no Annex B.

DRAFT CCSDS RECOMMENDED PRACTICE FOR REQUIREMENTS FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF CANDIDATE TRUSTWORTHY DIGITAL REPOSITORIES~~{SUBJECT}~~

certification body shall be able to communicate effectively with all those clients it provides services to.

Comment [mc28]: Why is this necessary? See 17021 , Clause 7.2.

7.2 PERSONNEL INVOLVED IN THE CERTIFICATION ACTIVITIES

The requirements from ISO/IEC 17021:2006, Clause 7.2 apply. In addition, the following TDR-specific requirements and guidance apply.

7.2.1 TDR 7.2 COMPETENCE OF CERTIFICATION BODY PERSONNEL

Certification bodies shall have personnel competent to

- a) select and verify the competence of TDR auditors for audit teams appropriate for the audit;
- b) brief TDR auditors and arrange any necessary training;
- c) decide on the granting, maintaining, withdrawing, suspending, extending, or reducing of certifications;
- d) set up and operate an appeals and complaints process.

Comment [mc29]: Why is this necessary? It appears to be adequately covered in 17021.

7.2.1.1 Training of audit teams

~~The following training requirements apply to all members of the audit team, with the exception of d), which can be shared among members of the audit team.~~ The certification body shall have criteria for the training of audit team members that ensures

Comment [DG30]: Insert MEMBERS "audit team MEMBERS"

- a) knowledge of the TDR standard and other relevant normative documents;
- ~~b) understanding of digital preservation;~~
- ~~e)b) understanding of risk assessment and risk management from the business perspective of digitally encoded information;~~
- ~~e)c) technical knowledge of the digital preservation aspects which apply to the activity to be audited;~~
- ~~e)d) general knowledge of regulatory requirements relevant to TDRs;~~
- ~~e)e) knowledge of management systems;~~
- ~~e)f) understanding of the principles of auditing based on ISO 19011;~~
- ~~h) knowledge of TDR effectiveness review and measurement of control effectiveness.~~

Comment [DG31]: We deleted this on the WIKI

Comment [mc32]: What does this mean?

Comment [SCL33]: Clarify

Comment [DG34]: Deleted

Comment [mc35]: Why are these necessary? Aren't they already covered in 17021?

Comment [DG36]: Deleted

~~These training requirements apply to all members of the audit team, with the exception of d), which can be shared among members of the audit team.~~

Comment [DG37]: Move to start of the above bullets

DRAFT CCSDS RECOMMENDED PRACTICE FOR REQUIREMENTS FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF CANDIDATE TRUSTWORTHY DIGITAL REPOSITORIES~~(SUBJECT)~~

7.2.1.1.1 When selecting the audit team to be appointed for a specific certification audit the certification body shall ensure that the skills brought to each assignment are appropriate. The team shall

- a) have appropriate technical knowledge of the specific activities within the scope of the TDR for which certification is sought and, where relevant, with associated procedures and their potential digital preservation risks (technical experts who are not auditors may fulfill this function);
- b) have a sufficient degree of understanding of the client organization to conduct a reliable certification audit of its TDR in managing the digital preservation aspects of its activities, products and services;
- c) have appropriate understanding of the regulatory requirements applicable to the client organization's TDR.

Comment [mc38]: candidate repository.

Comment [mc39]: candidate repository?

Comment [mc40]: candidate repository?

7.2.1.1.2 When required, the audit team may be complemented by technical experts who can demonstrate specific competence in a field of technology appropriate to the audit. Note should be taken that technical experts cannot be used in place of TDR auditors but could advise auditors on matters of technical adequacy in the context of the management system being subjected to audit. The certification body shall have a procedure for

- a) selecting auditors and technical experts on the basis of their competence, training, qualifications and experience;
- b) initially assessing the conduct of auditors and technical experts during certification audits and subsequently monitoring the performance of auditors and technical experts.

Comment [DG/BA41]: Suggested change by BA

7.2.1.2 Management of the decision making process

The management function shall have the technical competence and ability in place to manage the process of decision-making regarding the granting, maintaining, extending, reducing, suspending and withdrawing of TDR certification to the requirements of <ISO XXXXX - RAC Document>.

7.2.1.3 Pre-requisite levels of education, work experience, auditor training and audit experience for auditors conducting TDR audits (except the initial audit committee)

7.2.1.3.1 The following criteria shall be applied for each auditor in the TDR audit team. The auditor shall

- a) have an education at secondary level;
- b) have at least four years full time practical workplace experience in information technology, of which at least two years are in a role of function

Comment [mc42]: If we just said 7.2. applied, we wouldn't have to get into this level of detail.

Comment [SCL43]: Review these requirements.

Comment [DG44]: Define the first audit cttee anmd let them approve things

Comment [DG45]: Data management and digital preservation

DRAFT CCSDS RECOMMENDED PRACTICE FOR REQUIREMENTS FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF CANDIDATE TRUSTWORTHY DIGITAL REPOSITORIES{SUBJECT}

relating to digital preservation data management, libraries, archives or information technology with a focus on digital preservation;

- c) have successfully completed five days of training in a course approved by the initial audit committee, the scope of which covers TDR audits and audit management **shall be considered** appropriate;
- d) have gained experience in the entire process of assessing **digital preservation** prior to assuming responsibility for performing as an auditor. This experience should have been gained by participation in a minimum of four two certification audits for a total of at least 20 days, including review of documentation and risk analysis, implementation assessment and audit reporting with at least the majority of the team on site, including the ones familiar with the particular area being audited;
- e) have experience which is reasonably current, and some familiarity with current research in digital preservation;
- ~~f) be able to put complex operations in a broad perspective and to understand the role of individual units in larger client organizations;~~
- f) keep their knowledge and skills in digital preservation and auditing up to date through continual professional development;
- g) Be accredited by the initial audit committee.

Comment [mc46]: I don't understand this phrase and its connection to the rest of the sentence. Are there words missing?

Comment [mc47]: TDRs?

Technical experts shall comply with criteria a), b), e) and f).

7.2.1.3.2 In addition to the requirements in 7.2.1.3.1, audit team leaders shall fulfill the following requirements, which shall be demonstrated in audits under guidance and supervision:

- a) have knowledge and attributes to manage the certification audit process;
- b) have been an auditor in at least ~~three two~~ complete TDR **audits**;
- c) have demonstrated the capability to communicate effectively, both orally and in writing.

Comment [DG48]: Two (for issue 1)

Comment [DG49]: Under guidance and supervision

7.3 USE OF INDIVIDUAL EXTERNAL AUDITORS AND EXTERNAL TECHNICAL EXPERTS

The requirements from ISO/IEC 17021:2006, Clause 7.3 apply. In addition, the following TDR-specific requirements and guidance applies.

DRAFT CCSDS RECOMMENDED PRACTICE FOR REQUIREMENTS FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF CANDIDATE TRUSTWORTHY DIGITAL REPOSITORIES~~(SUBJECT)~~

7.3.1 TDR 7.3 USING EXTERNAL AUDITORS OR EXTERNAL TECHNICAL EXPERTS AS PART OF THE AUDIT TEAM

When using individual external auditors or external technical experts as part of the audit team, the certification body shall ensure that they are competent and comply with the applicable provisions of this publication and are not involved, either directly or through its employer with the design, implementation or maintenance of a TDR or related management system(s) in such a way that impartiality could be compromised.

7.3.1.1 Use of technical experts

Technical experts with specific knowledge regarding the process and digital preservation issues and legislation affecting the client organization, but who do not satisfy all of the criteria in 7.2, may be part of the audit team. Technical experts shall work under the supervision of an auditor.

Comment [mc50]: Which process?

7.4 PERSONNEL RECORDS

The requirements from ISO/IEC 17021:2006, Clause 7.4 apply.

7.5 OUTSOURCING

The requirements from ISO/IEC 17021:2006, Clause 7.5 apply.

8 INFORMATION REQUIREMENTS

8.1 PUBLICLY ACCESSIBLE INFORMATION

The requirements from ISO/IEC 17021:2006, Clause 8.1 apply. In addition, the following TDR-specific requirements and guidance apply.

8.1.1 TDR 8.1 PROCEDURES FOR GRANTING, MAINTAINING, EXTENDING, REDUCING, SUSPENDING AND WITHDRAWING CERTIFICATION

Comment [mc51]: Why is 8.1.1. necessary?

The certification body shall require the client organization to have a documented and implemented TDR which conforms to <ISO XXXXX - RAC Document> and other documents required for certification.

Comment [mc52]: digital repository?

The certification body shall have documented procedures for

- a) the initial certification audit of a client organization's TDR, in accordance with the provisions of ISO 19011, ISO/IEC 17021 and other relevant documents;
- b) surveillance and recertification audits of a client organization's TDR in accordance with ISO 19011 and ISO/IEC 17021 on a periodic basis, with exceptions agreed with the initial audit committee for continuing conformity with relevant requirements and for verifying and recording that a client organization takes corrective action on a timely basis to correct all nonconformities.

Comment [mc53]: digital repository?

8.2 CERTIFICATION DOCUMENTS

The requirements from ISO/IEC 17021:2006, Clause 8.2 apply. In addition, the following TDR-specific requirements and guidance apply.

8.2.1 TDR 8.2 TDR CERTIFICATION DOCUMENTS

Comment [mc54]: Why do we need this?

The certification body shall provide to each of its client organizations whose TDR digital repository is certified, certification documents such as a letter or a certificate signed by an officer who has been assigned such responsibility. For the client organization and each of its information systems covered by the certification, these documents shall identify the scope of the certification granted and the TDR standard <ISO XXXXX - RAC Document> to which the TDR is certified. In addition, the certificate should include a reference to the specific version of the Statement of Applicability.

Comment [mc55]: What is this?

8.3 DIRECTORY OF CERTIFIED CLIENTS

The requirements from ISO/IEC 17021:2006, Clause 8.3 apply.

8.4 REFERENCE TO CERTIFICATION AND USE OF MARKS

The requirements from ISO/IEC 17021:2006, Clause 8.4 apply. In addition, the following TDR-specific requirements and guidance applies.

8.4.1 TDR 8.4 CONTROL OF CERTIFICATION MARKS

Comment [mc56]: Why is this necessary?

The certification body shall exercise proper control over ownership, use and display of its TDR certification marks. If the certification body confers the right to use a mark to indicate certification of a TDR, the certification body should ensure that the client organization uses the specified mark only as authorized in writing by the certification body. The certification body shall not entitle the client organization to use this mark on a product, or in a way that may be interpreted as denoting product conformity.

8.5 CONFIDENTIALITY

The requirements from ISO/IEC 17021:2006, Clause 8.5 apply. In addition, the following TDR-specific requirements and guidance applies.

8.5.1 TDR 8.5 ACCESS TO ORGANIZATIONAL RECORDS

Before the certification audit, the certification body shall ask the client organization to report if any TDR-digital repository records cannot be made available for review by the audit team because they contain confidential or sensitive information. The certification body shall determine whether the TDR-digital repository can be adequately audited in the absence of these records. If the certification body concludes that it is not possible to adequately audit the TDR-digital repository without reviewing the identified confidential or sensitive records, it shall advise the client organization that the certification audit cannot take place until appropriate access arrangements are granted.

8.6 INFORMATION EXCHANGE BETWEEN A CERTIFICATION BODY AND ITS CLIENTS

The requirements from ISO/IEC 17021:2006, Clause 8.6 apply.

9 PROCESS REQUIREMENTS

Comment [SCL57]: This is the key section where most reworking may be needed.

9.1 9.1 GENERAL REQUIREMENTS

The requirements from ISO/IEC 17021:2006, Clause 9.1 apply. In addition, the following TDR-specific requirements and guidance apply.

Comment [mc58]: This means that we accept the timetable for audits in 17021. (i.e., The audit programme shall include a two-stage initial audit, surveillance audits in the first and second years, and a recertification audit in the third year prior to expiration of certification. The three-year certification cycle begins with the certification or recertification decision.

9.1.1 TDR 9.1.1 GENERAL TDR AUDIT REQUIREMENTS

9.1.1.1 Certification audit criteria

The criteria against which the TDR digital repository of a client are audited shall be those outlined in the standard <ISO XXXXX - RAC Document> and other documents required for certification relevant to the function performed. If an explanation is required as to the application of these documents to a specific certification program, then such an explanation shall be given by a relevant and impartial committee or persons possessing the necessary technical competence and published by the certification body.

Comment [mc59]: What does this mean? Why do we need 9.1.1.1?

Comment [mc60]: Why is this necessary?

9.1.1.2 Policies and procedures

The documentation of the certification body shall include the policy and procedures for implementing the certification process, including checks of the use and application of documents used in certification of TDRs and the procedures for auditing and certifying the client organization's TDR.

Comment [mc61]: Why do we need this? It is already covered in 17021.

9.1.1.3 Audit team

The audit team shall be formally appointed and provided with the appropriate working documents. The plan for and the date of the audit shall be agreed to with the client organization. The mandate given to the audit team shall be clearly defined and made known to the client organization, and shall require the audit team to examine the structure, policies and procedures of the client organization, and confirm that these meet all the requirements relevant to the scope of certification and that the procedures are implemented and are such as to give confidence in the TDR of the client organization.

9.1.2 TDR 9.1.2 SCOPE OF CERTIFICATION

The audit team shall audit the TDR digital repository of the client organization covered by the defined scope against all applicable certification requirements. The certification body shall ensure that the scope and boundaries of the TDR digital repository of the client organization are clearly defined in terms of the characteristics of the business, the organization, its location, assets and technology. The certification body shall confirm, in the scope of their TDR audit, that client organizations address the requirements stated in Clause 1.2 of <ISO XXXXX - RAC Document>.

Comment [mc62]: This clause is about the applicability of the RAC document. Why do we need this bullet?

DRAFT CCSDS RECOMMENDED PRACTICE FOR REQUIREMENTS FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF CANDIDATE TRUSTWORTHY DIGITAL REPOSITORIES~~(SUBJECT)~~

Certification bodies shall ensure that the client organization's digital preservation risk assessment and risk treatment properly reflects its activities and extends to the boundaries of its activities as defined in the TDR standard <ISO XXXXX - RAC Document>. Certification bodies shall confirm that this is reflected in the client organization's scope of their TDR digital repository and Statement of Applicability.

Comment [mc63]: How is this relevant?

Certification bodies shall ensure that interfaces with services or activities that are not completely within the scope of the TDR are addressed within the TDR digital repository subject to certification and are included in the client organization's digital preservation risk assessment. An example of such a situation is the sharing of facilities (e.g. IT systems, databases and telecommunication systems) with other organizations.

Comment [mc64]: audit?

Comment [mc65]: Why is this needed?
See 17021 9.1.4.

9.1.3 TDR 9.1.3 AUDIT TIME

Certification bodies shall allow auditors sufficient time to undertake all activities relating to an initial audit, surveillance audit or recertification audit. The time allocated should be based on factors such as

- a) the size of the TDR scope (e.g. number of information systems used, number of employees);
- b) complexity of the TDR (e.g. criticality of information systems, risk situation of the TDR), see also Annex A;
- c) the type(s) of business performed within scope of the TDR digital repository;
- d) extent and diversity of technology utilized in the implementation of the various components of the TDR
- e) (such as the implemented controls, documentation and/or process control, corrective/preventive action, etc);
- f) number of sites;
- g) previously demonstrated performance of the TDR;
- h) extent of outsourcing and third party arrangements used within the scope of the TDR;

Comment [mc66]: There is no Annex A.

Annex C provides guidance on Audit Time. The certification body shall be prepared to substantiate or justify the amount of time used in any initial audit, surveillance audits and recertification audit.

Comment [mc67]: There is no Annex C.

9.1.4 TDR 9.1.4 MULTIPLE SITES

Comment [mc68]: Why is this necessary? All it does is tie the certification body's hands.

9.1.4.1 Multiple site sampling decisions in the area of TDR certification are more complex than the same decisions are for quality management systems. Where a client organization has a number of sites meeting the criteria from a) to c) below, certification bodies may consider using a sample-based approach to multiple-site certification audit:

- a) all sites are operating under the same TDRdigital repository, which is centrally administered and audited and subject to
- b) central management review;
- c) all sites are included within the client organization's internal TDR audit program;
- d) all sites are included within the client organization's TDR management review program.

9.1.4.2 The certification body wishing to use a sample-based approach shall have procedures in place to ensure the following.

- a) The initial contract review identifies, to the greatest extent possible, the difference between sites such that an adequate level of sampling is determined.
- b) A representative number of sites have been sampled by the certification body, taking into account
 - 1. the results of internal audits of head office and the sites,
 - 2. the results of management review,
 - 3. variations in the size of the sites,
 - 4. variations in the business purpose of the sites,
 - 5. complexity of the TDRdigital repository,
 - 6. complexity of the information systems at the different sites,
 - 7. variations in working practices,
 - 8. variations in activities undertaken,
 - 9. potential interaction with critical information systems or information systems processing sensitive information,
 - 10. any differing legal requirements.

DRAFT CCSDS RECOMMENDED PRACTICE FOR REQUIREMENTS FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF CANDIDATE TRUSTWORTHY DIGITAL REPOSITORIES~~(SUBJECT)~~

- c) A representative sample is selected from all sites within the scope of the client organization's TDR digital repository; this selection should be based upon judgmental choice to reflect the factors presented in item b) above as well as a random element.
- d) Every site included in the TDR digital repository which is subject to significant risks is audited by the certification body prior to certification.
- e) The surveillance program has been designed in the light of the above requirements and covers all sites of the client organization or within the scope of the TDR certification within a reasonable time.
- f) In the case of a nonconformity being observed, either at the head office or at a single site, the corrective action procedure applies to the head office and all sites covered by the certificate.

The audit described in TDR 9.1.5 below shall address the client organization's head office activities to ensure that a single TDR applies to all sites and delivers central management at the operational level. The audit shall address all the issues outlined above.

Comment [mc69]: audit?

9.1.5 TDR 9.1.5 AUDIT METHODOLOGY

The certification body shall have procedures, which require the client organization to be able to demonstrate that the internal TDR audits are scheduled, and the program and procedures are operational and can be shown to be operational.

Comment [mc70]: Why is this necessary?

Comment [mc71]: What does this mean?

The certification body's procedures should not presuppose a particular manner of implementation of a TDR or a particular format for documentation and records. Certification procedures shall focus on establishing that a client organization's TDR digital repository meets the requirements of the <ISO XXXXX - RAC Document> standard and the policies and objectives of the client organization.

The audit plan should identify the network-assisted auditing techniques that will be utilized during the audit, as appropriate.

NOTE Network assisted auditing techniques may include, for example, teleconferencing, web meeting, interactive web based communications and remote electronic access to the TDR documentation and/or TDR processes. The focus of such techniques should be to enhance audit effectiveness and efficiency, and should support the integrity of the audit process.

9.1.6 TDR 9.1.6 CERTIFICATION AUDIT REPORT

9.1.6.1 The certification body may adopt reporting procedures that suit its needs but as a minimum these procedures shall ensure that

Comment [mc72]: Why is this necessary?

- a) a meeting takes place between the audit team and the client organization's management prior to leaving

DRAFT CCSDS RECOMMENDED PRACTICE FOR REQUIREMENTS FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF CANDIDATE TRUSTWORTHY DIGITAL REPOSITORIES~~{SUBJECT}~~

- b) the client organization's premises at which the audit team provides
 - 1. a written or oral indication regarding the conformity of the client organization's TDR with the particular certification requirements,
 - 2. an opportunity for the client organization to ask questions about the findings and their basis;
- c) the audit team provides the certification body with an audit report of its findings as to the conformity of the client organization's TDR with all of the certification requirements.

9.1.6.2 The audit report should provide the following information:

- a) an account of the audit including a summary of the document review;
- b) an account of the certification audit of the client organization's digital preservation risk analysis;
- c) total audit time used and detailed specification of time spent on document review, assessment of risk analysis, on-site audit, and audit reporting;
- d) audit enquiries which have been followed, rationale for their selection, and the methodology employed.

9.1.6.3 The audit report of findings provided to the certification body shall be of sufficient detail to facilitate and support a certification decision and shall contain

- a) areas covered by the audit (e.g. the certification requirements and the sites that were audited), including significant audit trails followed and audit methodologies utilized (see TDR 9.1.5);
- b) observations made, both positive (e.g. noteworthy features) and negative (e.g. potential nonconformities);
- c) details of any nonconformities identified, supported by objective evidence and a reference of these nonconformities to the requirements of the TDR standard <ISO XXXXX - RAC Document> or other documents required for certification;
- d) comments on the conformity of the client organization's TDR with the certification requirements with a clear statement of nonconformity, a reference to the version of the Statement of Applicability, and, where applicable, any useful comparison with the results of previous certification audits of the client organization.

Completed questionnaires, checklists, observations, logs, or auditor notes might form an integral part of the audit report. If these methods are used, these

DRAFT CCSDS RECOMMENDED PRACTICE FOR REQUIREMENTS FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF CANDIDATE TRUSTWORTHY DIGITAL REPOSITORIES~~(SUBJECT)~~

documents shall be submitted to the certification body as evidence to support the certification decision. Information about the samples evaluated during the audit should be included in the audit report, or in other certification documentation.

The report shall consider the adequacy of the internal organization and procedures adopted by the client organization to give confidence in the TDR.

In addition to the requirements for reporting in ISO/IEC 17021:2006, Clause 9.1.10, the report should cover

- the degree of reliance that can be placed on the internal TDR audits and management reviews;
- a summary of the most important observations, positive as well as negative, regarding the implementation and effectiveness of the TDR;
- the audit team's recommendation as to whether the client organization's TDR should be certified or not, with information to substantiate this recommendation.

9.2 INITIAL AUDIT AND CERTIFICATION

The requirements from ISO/IEC 17021:2006, Clause 9.2 apply.

~~In addition, the following TDR specific requirements and guidance apply:~~

~~9.2.1 TDR 9.2.1 Audit team competence~~

~~The following requirements apply to certification assessment, in addition to the requirements that are listed in Clause 7.2. For surveillance activities only those requirements which are relevant to the scheduled surveillance activity apply.~~

~~The following requirements apply to the audit team as a whole:~~

~~a) In each of the following areas at least one audit team member shall satisfy the certification body's criteria for taking responsibility within the team~~

- ~~1. managing the team,~~
- ~~2. management systems and process applicable to TDR,~~
- ~~3. knowledge of the legislative and regulatory requirements in the particular digital preservation field,~~
- ~~4. identifying digital preservation related threats and incident trends,~~
- ~~5. identifying the vulnerabilities of the client organization and understanding the likelihood of their exploitation, their impact and their mitigation and control,~~
- ~~6. knowledge of TDR controls and their implementation,~~
- ~~7. knowledge of TDR effectiveness review and measurement of controls,~~
- ~~8. related and/or relevant TDR standards, industry best practices, preservation policies and procedures,~~
- ~~9. knowledge of incident handling methods and business continuity,~~
- ~~10. knowledge about tangible and intangible information assets and impact analysis,~~
- ~~11. knowledge of the current technology where preservation might be relevant or an issue,~~
- ~~12. knowledge of risk management processes and methods.~~

Formatted: Normal, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Comment [SCL73]: List needs amending for TDR context.

Formatted: Justified, Space Before: 12 pt, Line spacing: At least 14 pt, No bullets or numbering

DRAFT CCSDS RECOMMENDED PRACTICE FOR REQUIREMENTS FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF CANDIDATE TRUSTWORTHY DIGITAL REPOSITORIES~~(SUBJECT)~~

~~b) The audit team shall be competent to trace indications of preservation incidents in the client organization's TDR back to the appropriate elements of the TDR.~~

~~e) The audit team shall have appropriate work experience and practical application of the items above (this does not mean that an auditor needs a complete range of experience of all areas of digital preservation, but the audit team as whole should have enough appreciation and experience to cover the TDR scope being audited).~~

~~An audit team may consist of one person provided that the person meets all the criteria set out in a) above.~~

9.2.1.1 ~~TDR 9.2.1.1 Demonstration of auditor competence~~

~~Auditors shall be able to demonstrate their knowledge and experience, as outlined above, for example through~~

- ~~a) recognized TDR-specific qualifications;~~
- ~~b) registration as auditor;~~
- ~~c) approved TDR training courses;~~
- ~~d) up to date continuous professional development records;~~
- ~~e) practical demonstration through witnessing auditors going through the TDR audit process on real client systems.~~

Formatted: Normal, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Justified, Space Before: 12 pt, Line spacing: At least 14 pt, No bullets or numbering

Comment [DG74]: As agreed 20100222

9.2.2.1 TDR 9.2.2 GENERAL PREPARATIONS FOR THE INITIAL AUDIT

The certification body shall require that a client organization makes all necessary arrangements for the conduct of the certification audit, including provision for examining documentation and the access to all areas, records (including internal audit reports and reports of independent reviews of digital preservation) and personnel for the purposes of certification audit, recertification audit and resolution of complaints.

At least the following information shall be provided by the client prior to the onsite certification audit:

- a) general information concerning the TDR and the activities it covers;
- b) a copy of the TDR documentation required in <ISO XXXXX - RAC Document>, Clause 4.3.1 and, where required, associated documentation.

DRAFT CCSDS RECOMMENDED PRACTICE FOR REQUIREMENTS FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF CANDIDATE TRUSTWORTHY DIGITAL REPOSITORIES{SUBJECT}

9.2.3.2.2 TDR 9.2.3 INITIAL CERTIFICATION AUDIT

9.2.3.19.2.2.1 TDR 9.2.3.1 Stage 1 audit

In this stage of the audit, the certification body shall obtain documentation on the design of the TDR covering the documentation required in **Clause 4.3.1** of <ISO XXXXX - RAC Document>.

The objective of the stage 1 audit is to provide a focus for planning the stage 2 audit by gaining an understanding of the TDR in the context of the client organization's TDR policy and objectives, and, in particular, of the client organization's state of preparedness for the audit.

The stage 1 audit includes, but should not be restricted to, the document review. The certification body shall agree with the client organization when and where the document review is conducted. In every case, the document review shall be completed prior to the commencement of the stage 2 audit.

The results of the stage 1 audit shall be documented in a written report. The certification body shall review the stage 1 audit report before deciding on proceeding with the stage 2 audit and for selecting the stage 2 audit team members with the necessary competence.

The certification body shall make the client organization aware of the further types of information and records that may be required for detailed examination during the stage 2 audit.

9.2.3.29.2.2.2 TDR 9.2.3.2 Stage 2 audit

9.2.3.2.19.2.2.2.1 The stage 2 audit always takes place at the site(s) of the client organization; **at least two members of the audit team will be physically present, other members of the team may take part remotely as long as they can have access to the relevant materials.** On the basis of findings documented in the stage 1 audit report, the certification body drafts an audit plan for the conduct of the stage 2 audit. The objectives of the stage 2 audit are

- a) to confirm that the client organization adheres to its own policies, objectives and procedures;
- b) to confirm that the TDR conforms to all the requirements of the normative TDR standard <ISO XXXXX - RAC Document> and is achieving the client organization's policy objectives.

9.2.3.2.29.2.2.2.2 **To do this, the audit shall focus on the client organization's**

- a) assessment of digital preservation related risks, and that the assessments produce comparable and reproducible results;

Comment [SCL75]: Amend list for TDR context.

DRAFT CCSDS RECOMMENDED PRACTICE FOR REQUIREMENTS FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF CANDIDATE TRUSTWORTHY DIGITAL REPOSITORIES~~(SUBJECT)~~

- b) documentation requirements listed in Clause 4.3.1 of <ISO XXXXX - RAC Document>;
- c) selection of control objectives and controls based on the risk assessment and risk treatment processes;
- d) reviews of the effectiveness of the TDR and measurements of the effectiveness of the digital preservation controls, reporting and reviewing against the TDR objectives;
- e) internal TDR audits and management reviews;
- f) management responsibility for the digital preservation policy;
- g) correspondence between the selected and implemented controls, the Statement of Applicability, and the results of the risk assessment and risk treatment process, and the TDR policy and objectives;
- h) implementation of controls (see Annex D), taking into account the organization's measurements of effectiveness of controls [see d) above], to determine whether controls are implemented and effective to achieve the stated objectives;
- i) programs, processes, procedures, records, internal audits, and reviews of the TDR effectiveness to ensure that these are traceable to management decisions and the TDR policy and objectives.

~~9.2.3.3~~ 9.2.2.3 **TDR 9.2.3.3 Specific elements of the TDR audit**

Comment [SCL76]: Update for TDR context.

The role of the certification body is to establish that client organizations are consistent in establishing and maintaining procedures for the identification, examination and evaluation of digital preservation related threats to assets, vulnerabilities and impacts on the client organization. Certification bodies shall

- a) require the client organization to demonstrate that the analysis of preservation related threats is relevant and adequate for the operation of the client organization and its custodianship of its digital holdings;

NOTE The client organization is responsible for defining criteria by which digital preservation related risks of the client organization are identified as significant, and to develop procedure(s) for doing this.

- b) establish whether the client organization's procedures for the identification, examination and evaluation of digital preservation related threats to assets, vulnerabilities and impacts and the results of their application are consistent with the client organization's policy, objectives and targets.

The certification body shall also establish whether the procedures employed in analysis of significance are sound and properly implemented. If a digital

DRAFT CCSDS RECOMMENDED PRACTICE FOR REQUIREMENTS FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF CANDIDATE TRUSTWORTHY DIGITAL REPOSITORIES~~{SUBJECT}~~

preservation related threat to assets, a vulnerability, or an impact on the client organization is identified as being significant, it shall be managed within the TDR.

9.2.3.3.19.2.2.3.1 **9.2.3.3.1 Legal and regulatory compliance**

The maintenance and evaluation of legal and regulatory compliance is the responsibility of the client organization. The certification body shall restrict itself to checks and samples in order to establish confidence that the TDR functions in this regard. The certification body shall verify that the client organization has a management system to achieve legal and regulatory compliance applicable to the digital preservation risks and impacts.

9.2.3.3.29.2.2.3.2 **9.2.3.3.2 Integration of TDR documentation with that for other management systems**

The client organization can combine the documentation for TDR and other management systems (such as quality, health and safety, and environment) as long as the TDR can be clearly identified together with the appropriate interfaces to the other systems.

9.2.3.3.39.2.2.3.3 **9.2.3.3.3 Combining management system audits**

A certification body may offer other management system certification linked with the TDR certification, or may offer TDR certification only.

The TDR audit can be combined with audits of other management systems. This combination is possible provided it can be demonstrated that the audit satisfies all requirements for certification of the TDR. All the elements important to a TDR shall appear clearly, and be readily identifiable, in the audit reports. The quality of the audit shall not be adversely affected by the combination of the audits.

NOTE ISO 19011 provides guidance for carrying out combined management system audits.

9.2.49.2.3 **TDR 9.2.4 INFORMATION FOR GRANTING INITIAL CERTIFICATION**

In order to provide a basis for the certification decision, the certification body shall require clear reports, which provide sufficient information to make this decision.

Reports from the audit team to the certification body are required at various stages in the certification audit process. In combination with information held on file, these reports should at least contain the information required in TDR 9.1.6.

9.2.59.2.4 **TDR 9.2.5 CERTIFICATION DECISION**

The entity, which may be an individual, which takes the decision on granting/withdrawing a certification within the certification body, should incorporate

DRAFT CCSDS RECOMMENDED PRACTICE FOR REQUIREMENTS FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF CANDIDATE TRUSTWORTHY DIGITAL REPOSITORIES~~(SUBJECT)~~

a level of knowledge and experience in all areas which is sufficient to evaluate the audit processes and associated recommendations made by the audit team.

The decision whether or not to certify a client organization's TDR shall be taken by the certification body on the basis of the information gathered during the certification process and any other relevant information.

Those who make the certification decision shall not have participated in the audit. This decision shall be based upon the findings and certification recommendation of the audit team as provided in their certification audit report (see TDR 9.1.6) and any other relevant information available to the certification body.

The entity which takes the decision on granting certification should not normally overturn a negative recommendation of the audit team. If such a situation does arise, the certification body shall document and justify the basis for the decision to overturn the recommendation.

On the subject of deciding on certification, ISO/IEC 17021 does not mention a specific period in which at least one complete internal TDR audit and one management review of the client organization's TDR shall have taken place. The certification body may specify such a period. Irrespective of whether the certification body has chosen to specify a minimum frequency, measures shall be established by the certification body to ensure the effectiveness of the client organization's management review and internal TDR audit processes.

Certification shall not be granted to the client organization until there is sufficient evidence to demonstrate that the arrangements for management reviews and internal TDR audits have been implemented, are effective, and will be maintained.

9.3 9.3 SURVEILLANCE ACTIVITIES

The requirements from ISO/IEC 17021:2006, Clause 9.3 apply. In addition, the following TDR-specific requirements and guidance apply.

9.3.1 TDR 9.3 SURVEILLANCE AUDITS

9.3.1.1 Surveillance audit procedures shall be consistent with those concerning the certification audit of the client organization's TDR as described in this standard.

The purpose of surveillance is to verify that the approved TDR continues to be implemented, to consider the implications of changes to that system initiated as a result of changes in the client organization's operation and to confirm continued compliance with certification requirements. Surveillance programs should normally cover

- a) the system maintenance elements which are internal TDR audit, management review and preventive and corrective action;
- b) communications from external parties as required by the TDR standard <ISO XXXXX - RAC Document> and other documents required for certification;
- c) changes to the documented system;
- d) areas subject to change;
- e) selected elements of <ISO XXXXX - RAC Document>;
- f) other selected areas as appropriate.

9.3.1.2 As a minimum, surveillance by the certification body shall review the following:

- a) the effectiveness of the TDR with regard to achieving the objectives of the client organization's digital preservation policy;
- b) the functioning of procedures for the periodic evaluation and review of compliance with relevant digital preservation legislation and regulations;
- c) action taken on nonconformities identified during the last audit.

DRAFT CCSDS RECOMMENDED PRACTICE FOR REQUIREMENTS FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF CANDIDATE TRUSTWORTHY DIGITAL REPOSITORIES~~(SUBJECT)~~

9.3.1.3 Surveillance by the certification body should at least cover the points required for surveillance audit in ISO/IEC 17021. In addition, the following issues should be considered.

- a) The certification body should be able to adapt its surveillance program to the digital preservation issues related threats to assets, vulnerabilities and impacts on to the client organization and justify this program.
- b) The surveillance program of the certification body should be determined by the certification body. Specific dates for visits may be agreed with the certified client organization.
- c) Surveillance audits may be combined with audits of other management systems. The reporting shall clearly indicate the aspects relevant to each management system.
- d) The certification body is required to supervise the appropriate use of the certificate.

During surveillance audits, certification bodies shall check the records of appeals and complaints brought before the certification body and, where any nonconformity or failure to meet the requirements of certification is revealed, that the client organization has investigated its own TDR and procedures and taken appropriate corrective action.

A surveillance report shall contain, in particular, information on clearing of nonconformities revealed previously.

As a minimum, the reports arising from surveillance should build up to cover in totality the requirement of point a) above.

9.4 RECERTIFICATION

The requirements from ISO/IEC 17021:2006, Clause 9.4 apply. In addition, the following TDR-specific requirements and guidance apply.

9.4.1 TDR 9.4 RECERTIFICATION AUDITS

Recertification audit procedures shall be consistent with those concerning the certification audit of the client organization's TDR as described in this International Standard.

Certification bodies shall have clear procedures laying down the circumstances and conditions in which certifications will be maintained. If on surveillance or recertification audit, nonconformities are found to exist, such nonconformities shall be effectively corrected within a time agreed by the certification body. If correction is not made within the time agreed the scope of certification shall be reduced, or the certificate suspended or withdrawn. The time allowed to implement corrective action

DRAFT CCSDS RECOMMENDED PRACTICE FOR REQUIREMENTS FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF CANDIDATE TRUSTWORTHY DIGITAL REPOSITORIES~~{SUBJECT}~~

should be consistent with the severity of the nonconformity and the risk to the assurance of products or services of the client organization meeting specified requirements.

9.5 9.5 SPECIAL AUDITS

The requirements from ISO/IEC 17021:2006, Clause 9.5 apply. In addition, the following TDR-specific requirements and guidance apply.

9.5.1 TDR 9.5 SPECIAL CASES

The surveillance activities shall be subject to special provision if a client organization with a certified TDR makes major modifications to its system or if other changes take place which could affect the basis of its certification.

9.6 SUSPENDING, WITHDRAWING OR REDUCING SCOPE OF CERTIFICATION

The requirements from ISO/IEC 17021:2006, Clause 9.6 apply.

9.7 APPEALS

The requirements from ISO/IEC 17021:2006, Clause 9.7 apply.

9.8 COMPLAINTS

The requirements from ISO/IEC 17021:2006, Clause 9.8 apply. In addition, the following TDR-specific requirements and guidance apply.

9.8.1 TDR 9.8 COMPLAINTS

Complaints represent a source of information as to possible nonconformity. The certification body should require the certified client organization that, on receipt of a complaint, the certified client organization should establish, and where appropriate report on, the cause of the complaint, including any predetermining (or predisposing) factors within the client organization's TDR.

The certification body should satisfy itself that the client organization is using such investigations to develop remedial / corrective action, which should include measures for

- a) notification to appropriate authorities if required by regulation;
- b) restoring conformity;
- c) preventing recurrence;
- d) evaluating and mitigating any adverse preservation incidents and their associated impacts;
- e) ensuring satisfactory interaction with other components of the TDR;
- f) assessing the effectiveness of the remedial / corrective measures adopted.

The certification body shall require each client organization whose TDR is certified to make available to the certification body, when requested, the records of all complaints and corrective action taken in accordance with the requirements of <ISO XXXXX - RAC Document>.

9.9 RECORDS OF APPLICANTS AND CLIENTS

The requirements from ISO/IEC 17021:2006, Clause 9.9 apply.

10 MANAGEMENT SYSTEM REQUIREMENTS FOR CERTIFICATION BODIES

10.1 OPTIONS

The requirements from ISO/IEC 17021:2006, Clause 10.1 apply.

10.2 OPTION 1 – MANAGEMENT SYSTEM REQUIREMENTS IN ACCORDANCE WITH ISO 9001

The requirements from ISO/IEC 17021:2006, Clause 10.2 apply.

10.3 OPTION 2 – GENERAL MANAGEMENT SYSTEM REQUIREMENTS

The requirements from ISO/IEC 17021:2006, Clause 10.3 apply. In addition, the following TDR-specific requirements and guidance apply.

10.3.1 TDR 10.3 TDR IMPLEMENTATION

It is recommended that certification bodies implement a TDR in accordance with <ISO XXXXX - RAC Document>.

11 SECURITY

11.1 INTRODUCTION

The use of the Audit and Certification standard has several potential areas of security concern.

One security concern is the possibility that the repository is fooled into undergoing an archive-audit by someone unqualified or even malicious.

Another concern involves the possible release of confidential information which is collected as evidence by the auditor.

11.2 SECURITY CONCERNS WITH RESPECT TO THE CCSDS DOCUMENT

The repository may ask someone to perform an audit using this standard. There is a possibility that the person contacted is not in fact the person that the repository believes. Alternatively the correct person may be contacted but in fact another, possibly malicious, person may turn up to perform the audit.

In the process of collecting evidence for the various metrics the auditor may collect information which is confidential or sensitive, for example details of security weaknesses.

There is a danger that such information may fall into the wrong hands and expose the repository to increased risk. Alternatively in the process of collecting evidence the repository system may be damaged.

While these are all valid security concerns, they fall outside the purview of this standard, which applies only to the metrics which an auditor should use for auditing a repository.

11.3 POTENTIAL THREATS AND ATTACK SCENARIOS

Impersonation of an auditor and/or release of confidential information could both result in exposing the repository and its holdings to increased risk and loss of reputation of the repository.

11.4 CONSEQUENCES OF NOT APPLYING SECURITY TO THE TECHNOLOGY

While these security issues are of concern, they are out of scope with respect to this document. This document aims to provide the basis for an audit and certification process for assessing the trustworthiness of digital repositories. Providing protection against false auditors must rely on the repository's identification and authorization systems. Protection against loss of confidential information in the possession of the auditor must be provided by the security system of that auditor and the method of transmission of information which is agreed

DRAFT CCSDS RECOMMENDED PRACTICE FOR REQUIREMENTS FOR BODIES
PROVIDING AUDIT AND CERTIFICATION OF CANDIDATE TRUSTWORTHY DIGITAL
REPOSITORIES~~{SUBJECT}~~

between the repository and auditor. Protection against damage to the repository or its holdings during an audit must rely on the security and safety systems of the repository.

DRAFT CCSDS RECOMMENDED PRACTICE FOR REQUIREMENTS FOR BODIES
PROVIDING AUDIT AND CERTIFICATION OF CANDIDATE TRUSTWORTHY DIGITAL
REPOSITORIES~~(SUBJECT)~~

ANNEX A

[ANNEX TITLE]

[EITHER NORMATIVE OR INFORMATIVE]

[Annexes contain ancillary information. Normative annexes precede informative annexes. Informative references are placed in an informative annex. See CCSDS A20.0-Y-2, *CCSDS Publications Manual* (Yellow Book, Issue 2, June 2005) for discussion of the kinds of material contained in annexes.]