The Consultative Committee for Space Data Systems

Recommendation for Space Data System Practices

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

RECOMMENDED PRACTICE

CCSDS 652.1-M-2

MAGENTA BOOK

March 2014

The Consultative Committee for Space Data Systems

Recommendation for Space Data System Practices

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

RECOMMENDED PRACTICE

CCSDS 652.1-M-2

MAGENTA BOOK

March 2014

AUTHORITY

Issue:	Recommended Practice, Issue 2
Date:	March 2014
Location:	Washington, DC, USA

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 *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-3), 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

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 in themselves considered binding on any Agency.

CCSDS Recommendations take two forms: **Recommended Standards** that are prescriptive and are the formal vehicles by which CCSDS Agencies create the standards that specify how elements of their space mission support infrastructure shall operate and interoperate with others; and **Recommended Practices** that are more descriptive in nature and are intended to provide general guidance about how to approach a particular problem associated with space mission support. This **Recommended Practice** is issued by, and represents the consensus of, the CCSDS members. Endorsement of this **Recommended Practice** is entirely voluntary and does not imply a commitment by any Agency or organization to implement its recommendations in a prescriptive sense.

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.

FOREWORD

This document is a technical Recommended Practice 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 *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-3). 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.

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

Member Agencies

- Agenzia Spaziale Italiana (ASI)/Italy.
- 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 (DLR)/Germany.
- European Space Agency (ESA)/Europe.
- Federal Space Agency (FSA)/Russian Federation.
- Instituto Nacional de Pesquisas Espaciais (INPE)/Brazil.
- Japan Aerospace Exploration Agency (JAXA)/Japan.
- National Aeronautics and Space Administration (NASA)/USA.
- UK Space Agency/United Kingdom.

Observer Agencies

- Austrian Space Agency (ASA)/Austria.
- Belgian Federal Science Policy Office (BFSPO)/Belgium.
- Central Research Institute of Machine Building (TsNIIMash)/Russian Federation.
- China Satellite Launch and Tracking Control General, Beijing Institute of Tracking and Telecommunications Technology (CLTC/BITTT)/China.
- 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.
- Departamento de Ciência e Tecnologia Aeroespacial (DCTA)/Brazil.
- European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)/Europe.
- European Telecommunications Satellite Organization (EUTELSAT)/Europe.
- Geo-Informatics and Space Technology Development Agency (GISTDA)/Thailand.
- 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.
- Ministry of Communications (MOC)/Israel.
- National Institute of Information and Communications Technology (NICT)/Japan.
- National Oceanic and Atmospheric Administration (NOAA)/USA.
- National Space Agency of the Republic of Kazakhstan (NSARK)/Kazakhstan.
- National Space Organization (NSPO)/Chinese Taipei.
- Naval Center for Space Technology (NCST)/USA.
- Scientific and Technological Research Council of Turkey (TUBITAK)/Turkey.
- South African National Space Agency (SANSA)/Republic of South Africa.
- Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
- Swedish Space Corporation (SSC)/Sweden.
- Swiss Space Office (SSO)/Switzerland.
- United States Geological Survey (USGS)/USA.

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS 652.1-M-1	Requirements for Bodies Providing Audit and Certification of Candidate Trustworthy Digital Repositories, Recommended Practice, Issue 1	November 2011	Original issue, superseded
CCSDS 652.1-M-2	Requirements for Bodies Providing Audit and Certification of Candidate Trustworthy Digital Repositories, Recommended Practice, Issue 2	March 2014	Current issue

CONTENTS

CONTENTS (continued)

1 INTRODUCTION

1.1 PURPOSE

The main purpose of this document is to define a CCSDS Recommended Practice (and ISO standard) on which to base the operations of the organization(s) which assess the trustworthiness of digital repositories using ISO 16363 (reference [1]) and provide the appropriate certification. This document specifies requirements for bodies providing audit and certification of digital repositories, based on the metrics contained within ISO/IEC 17021 (reference [4]) and CCSDS 652.0-M-1/ISO 16363 (reference [1]). It is primarily intended to support the accreditation of bodies providing such certification.

ISO/IEC 17021 provides the bulk of the requirements on bodies offering audit and certification for general types of management systems. However, for each specific type of system, specific additional requirements will be needed, for example, to specify the standard against which the audit is to be made and the qualifications which auditors require.

This document provides the (small number of) specific additions required for bodies providing audit and certification of candidate trustworthy digital repositories. Trustworthy here means that they can be trusted to maintain, over the long-term, the understandability and usability of digitally encoded information placed into their safekeeping.

In order improve readability the section numbers are kept consistent with those of ISO/IEC 17021. Some subsections are applicable as they stand, and these are simply enumerated; otherwise additions to subsections are explicitly given. In the former case the sections may consist of just a few sentences. As a result this document must be read in conjunction with ISO/IEC 17021.

1.2 SCOPE

The requirements contained in this CCSDS Recommended Practice need to be demonstrated in terms of competence and reliability by any organization or body providing certification of digital repositories.

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.

1.4 RATIONALE

There is a hierarchy of standards concerned with good auditing practice (references [3]-[5]). This document is positioned within this hierarchy in order to ensure that these good practices can be applied to the evaluation of the trustworthiness of digital repositories.

ISO/IEC 17021 *Conformity assessment — Requirements for bodies providing audit and certification of management systems* (reference [5]) 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 candidate trustworthy digital repositories in accordance with CCSDS 652.0-M-1/ISO 16363 (reference [1]), some requirements that are additional to ISO/IEC 17021 are necessary. These are provided by this document.

The text in sections 4 to 10 in this document follows the structure of ISO/IEC 17021, with specific additions on the application of ISO/IEC 17021 for certification of candidate trustworthy digital repositories.

1.5 STRUCTURE OF THIS DOCUMENT

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

Sections 1-2 of this document 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. These are normative.
- Section 2 provides an overview of auditing practices. This is informative.
- Section 3 is reserved for future use.
- Section 4 states the principles that apply.
- Sections 5 to 10 provide the normative rules against which an organization providing audit and certification of candidate trustworthy digital repositories may be judged, based on ISO/IEC 17021 (reference [4]).
- Annex A specifies the trusted digital repository management system competencies for certification body personnel for specific certification functions.
- Annex B is a CCSDS-required informative discussion of the security implications of applying this CCSDS Recommended Practice.

1.6 DEFINITIONS

1.6.1 ACRONYMS AND ABBREVIATIONS

CAB	conformity assessment body
CCSDS	Consultative Committee for Space Data Systems
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
OAIS	Open Archival Information System
TDR	trustworthy digital repository
TDRMS	trustworthy digital repository management system

1.6.2 TERMINOLOGY

1.6.2.1 General

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 Open Archival Information System (OAIS) Reference Model (reference [2]). One of the great strengths of the OAIS Reference Model 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 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, and is used to denote any type of digital repository; it may be a Trustworthy Digital Repository (TDR), a candidate TDR, a lapsed TDR, or one not seeking certification. 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.

1.6.2.2 Glossary

For the purposes of this document, the terms and definitions given in ISO/IEC 17021 (reference [4]), CCSDS 650.0-B-1/ISO 14721 (reference [2]), CCSDS 652.0-M-1/ISO 16363 (reference [1]), ISO 9000:2005 (reference [3]) and the following apply.

trustworthy digital repository, TDR: A repository which has a current certification.

1.6.3 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.

1.7 CONFORMANCE

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

1.8 REFERENCES

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

[1] *Audit and Certification of Trustworthy Digital Repositories*. Issue 1. Recommendation for Space Data System Practices (Magenta Book), CCSDS 652.0-M-1. Washington, D.C.: CCSDS, September 2011. [Equivalent to ISO 16363:2012]

[2] *Reference Model for an Open Archival Information System (OAIS)*. Issue 1. Recommendation for Space Data System Standards (Blue Book), CCSDS 650.0-B-1. Washington, D.C.: CCSDS, January 2002. [Equivalent to ISO 14721:2003]

[3] *Quality Management Systems—Fundamentals and Vocabulary*. 3rd ed. International Standard, ISO 9000:2005. Geneva: ISO, 2005.

[4] *Conformity Assessment—Requirements for Bodies Providing Audit and Certification of Management Systems*. 2nd ed. International Standard, ISO/IEC 17021:2011. Geneva: ISO, 2011.

[5] *Conformity Assessment—Vocabulary and General Principles*. International Standard, ISO/IEC 17000:2004. Geneva: ISO, 2004.

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 the body providing such third party certification can inspire this confidence. It does this by building on the more general specifications of references [3]-[5].

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 in 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 specifies how complaints are dealt with.

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

3 RESERVED

This section is reserved for future use.

4 PRINCIPLES

The principles from ISO/IEC 17021:2011, Clause 4 apply.

The term ‘management system’ used in ISO/IEC 17021 shall be replaced by ‘trusted digital repository management system’ in the context of this document.

5 GENERAL REQUIREMENTS

5.1 LEGAL AND CONTRACTUAL MATTERS

All the requirements from ISO/IEC 17021:2011, Clause 5.1 apply.

5.2 MANAGEMENT OF IMPARTIALITY

5.2.1 GENERAL

The requirements from ISO/IEC 17021:2011, Clause 5.2 apply. In addition, the following TDR audit and certification specific requirements and guidance apply.

5.2.2 CONFLICTS OF INTEREST

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

a) 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 b) below;

b) 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. However, the certification body shall be independent from the body or bodies (including any individuals) which provide the internal self-assessment of the client organization’s repository subject to certification.

5.3 LIABILITY AND FINANCING

The requirements from ISO/IEC 17021:2011, Clause 5.3 apply.

6 STRUCTURAL REQUIREMENTS

All the requirements from ISO/IEC 17021:2011, Clause 6 apply.

7 RESOURCE REQUIREMENTS

7.1 COMPETENCE OF MANAGEMENT AND PERSONNEL

7.1.1 GENERAL CONSIDERATIONS

All the requirements given in 7.1.1 of ISO/IEC 17021:2011 apply.

7.1.2 DETERMINATION OF COMPETENCE CRITERIA

All the requirements given in 7.1.2 of ISO/IEC 17021:2011 apply.

The competence criteria included in annex A of this document shall form the basis for the criteria developed. Competence criteria can include generic and specific criteria. The competence criteria in Annex A of ISO/IEC 17021 would be considered to be generic.

In determining competence criteria for auditors and audit teams the certification body shall clearly identify those competencies that auditors are required to have to be signed off as auditors, and those competencies that could be provided by other team members acting as Technical Experts in a particular technical area.

NOTE – Qualifications and experience can be used as part of the criteria; however, they are not by themselves guarantees of competencies. The competencies must be evaluated explicitly.

7.1.3 EVALUATION PROCESSES

All the requirements given in 7.1.3 of ISO/IEC 17021:2011 apply.

7.1.4 OTHER CONSIDERATIONS

All the requirements given in 7.1.4 of ISO/IEC 17021:2011 apply.

7.2 PERSONNEL INVOLVED IN THE CERTIFICATION ACTIVITIES

All the requirements from ISO/IEC 17021:2011, Clause 7.2 apply.

7.3 USE OF INDIVIDUAL EXTERNAL AUDITORS AND EXTERNAL TECHNICAL EXPERTS

All the requirements from ISO/IEC 17021:2011, Clause 7.3 apply.

7.4 PERSONNEL RECORDS

All the requirements from ISO/IEC 17021:2011, Clause 7.4 apply.

7.5 OUTSOURCING

All the requirements from ISO/IEC 17021:2011, Clause 7.5 apply.

8 INFORMATION REQUIREMENTS

8.1 PUBLICLY ACCESSIBLE INFORMATION

The requirements from ISO/IEC 17021:2011, Clause 8.1 apply.

8.2 CERTIFICATION DOCUMENTS

The requirements from ISO/IEC 17021:2011, Clause 8.2 apply.

8.3 DIRECTORY OF CERTIFIED CLIENTS

The requirements from ISO/IEC 17021:2011, Clause 8.3 apply.

8.4 REFERENCE TO CERTIFICATION AND USE OF MARKS

The requirements from ISO/IEC 17021:2011, Clause 8.4 apply.

8.5 CONFIDENTIALITY

The requirements from ISO/IEC 17021:2011, Clause 8.5 apply. In addition, the following TDR audit and certification specific requirements apply.

Before the certification audit, the certification body shall ask the client organization to report if any digital repository information cannot be made available for review by the audit team because they contain confidential or sensitive information. The certification body shall determine whether the 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 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 17021:2011, Clause 8.6 apply.

9 PROCESS REQUIREMENTS

The requirements from ISO/IEC 17021:2011, Clause 9 apply. In addition, the following TDR audit and certification specific requirements apply.

The criteria against which the candidate trustworthy digital repository of a client are audited shall be those outlined in the CCSDS Recommended Practice CCSDS 652.0-M-1/ISO 16363 (reference [1]) and other documents required for certification relevant to the function performed.

For on-site audits of the client organization at least two members of the audit team shall be physically present; other members of the team may take part remotely as long as they can have access to the relevant materials.

10 MANAGEMENT SYSTEM REQUIREMENTS FOR CERTIFICATION BODIES

The requirements from ISO/IEC 17021:2011, Clause 10 apply.

ANNEX A

REQUIRED TRUSTED DIGITAL REPOSITORY MANAGEMENT SYSTEM (TDRMS) COMPETENCIES

(NORMATIVE)

The following table specifies the trusted digital repository management system competencies for certification body personnel for specific certification functions. These specific competencies are additional to the generic competencies identified in ISO/IEC 17021:2011 Annex A Table A.1.

The certification body shall identify specific knowledge consistent with the general competencies identified in the table. 'X' does not have the same meaning as ISO/IEC 17021. In this table it is used only to identify which of the competencies are relevant; the letter X has no specific meaning.

Competency \ Function	Application Review	Audit Team Selection	Audit Planning Activities	Auditing Activities	Certification Decision	Auditor Evaluation
Possesses the knowledge of and ability to apply the application review requirements in ISO/IEC 17021, this document, and specific scheme rules and certification body procedures, including: – audit duration requirements and their application.	X		X	X	X	
Possesses the knowledge of and ability to identify the competencies required for the audit team and required additional technical expertise, in accordance with this table and CAB procedures, including things specific to a repository: – local language; – applicable legal framework, including any specific national or regional factors; – types of digital objects being preserved.		X	X			

Competency \ Function	Application Review	Audit Team Selection	Audit Planning Activities	Auditing Activities	Certification Decision	Auditor Evaluation
Possesses the knowledge of and ability to develop an audit plan that ensures: – audit team members audit those products and processes that they are technically competent to audit; – the audit team includes members with knowledge required to assess all necessary repository components; – audit time is optimised; and – audit objectives defined in ISO 16363 can be realized.			X	X		X
Possesses the knowledge of the TDRMS principles as enumerated in ISO 16363, and the ability to apply these principles including: – establishment of acceptable limits with respect to evidence which should be inspected; – validation methodologies for assessing the evidence presented by the repository.		X	X	X	X	X
Possesses the knowledge of and ability to apply the requirements for reporting in ISO/IEC 17021, this document, and any CAB.			X	X	X	X
Possesses the knowledge of and ability to evaluate organizational governance and organizational viability as far as it affects long-term preservation of digitally encoded information, including: – evaluate an organization's commitment to preservation; – recognize whether enough detail is specified in a collection's policy; – evaluate long term business plans; – evaluate sustainability plans (i.e., what will happen to the content if the repository closes?).				X	X	X

Competency \ Function	Application Review	Audit Team Selection	Audit Planning Activities	Auditing Activities	Certification Decision	Auditor Evaluation
Possesses the knowledge and ability to evaluate an organization's capacity to undertake digital preservation according to ISO 16363 in terms of – Staffing: • whether adequate staffing levels and expertise are in place; • organizational charts, job descriptions, and staff competencies; • training requirements for repository staff; • plans for professional development and training; – Financial stability: • mitigation of financial risks and other risks; • business plans, budgets, and contingency plans; • risk management plans; – Contracts, licenses, and liabilities: • contracts, licenses, agreements, and permissions statements; • permissions documents and licenses.				X	X	X
Possesses knowledge of the TDRMS principles with respect to procedural accountability and the associated preservation policy framework including its ability to: – evaluate the process by which a designated community is defined; – determine whether system documentation is adequate for all aspect of the TDRMS; – determine whether preservation plans are adequate and match the preservation policies; – determine if preservation policies are accurately captured in system workflows; – determine if workflows are adequately documented; – recognise whether an adequate level of detail has been recorded about system changes; – evaluate the organisation's commitment to transparency and accountability.		X		X		X

Competency \ Function	Application Review	Audit Team Selection	Audit Planning Activities	Auditing Activities	Certification Decision	Auditor Evaluation
Possesses the knowledge to assess the TDRMS's procedures and processes when acquiring content, including its ability to: – identify Information Properties that are important for preserving the repository's digital content; – information that needs to be associated with the content information (e.g., contextual metadata); – specify Submission Information Packages (SIPs) and understand how they are processed; – assess mechanisms to capture provenance; – understand legislative constraints and rights over digital objects; – understand agreements between the repository and depositors.		X		X		X
Possesses the knowledge to assess the TDRMS's procedures and processes when creating Archival Information Packages (AIPs), and its ability to: – assess the level of detail to which an AIP should be described; – determine the functions of the various components of an AIP and how they may be implemented; – identify the range of provenance information that should be collected; – identify the difference between SIP and AIP and ways in which the former may be converted to the latter; – identify and assess workflows and whether they reliably achieve what they purport to do; – assess the relationship between the various identifiers used within a repository; – assess ways of defining Designated Communities and how the appropriate amount of Representation Information may be obtained; – identify (or assess) possible changes in the Designated Community and its knowledge base and impacts on understandability; – assess the risks to the integrity of digital holdings in various circumstances, both technical and non-technical.		X		X		X

Competency \ Function	Application Review	Audit Team Selection	Audit Planning Activities	Auditing Activities	Certification Decision	Auditor Evaluation
Possesses the knowledge to evaluate aspects relevant to a TDRMS's preservation planning and preservation activities and its ability to: – determine a variety of digital preservation strategies and where they should be applied; – identify changes that may endanger preservation, how they may be monitored, and how they may be mitigated; – identify types of evidence that may support claims of effective digital preservation; – understand how the various parts of an AIP should be monitored and preserved against intentional and unintentional change; – identify changes in the preservation system that may be relevant to AIP preservation and responses to them that are appropriate.		X		X		X
Possesses the knowledge to evaluate policies, procedures, and processes relevant to a TDRMS's information management and information access activities, and its ability to: – provide mechanisms by which digital material in a repository may be discovered; – store and make available descriptive information for discovering and retrieving AIPs, or parts of AIPs; – ensure the correctness of linkages between the AIPs and descriptive data; – use and enforce appropriate policies, practices, and procedures.				X		X

Competency \ Function	Application Review	Audit Team Selection	Audit Planning Activities	Auditing Activities	Certification Decision	Auditor Evaluation
Possesses the knowledge to evaluate policies, procedures, and processes relevant to a TDRMS's technical infrastructure and security risk management activities, and its ability to: – understand computing and storage technologies sufficiently so as to be able to identify and assess baseline engineering changes for impacts or risks to AIPs; – understand enterprise overall risk management practices well enough to identify and validate enterprise risks which are pertinent to technical infrastructure as well as infrastructure risks that have been appropriately registered at the enterprise level; – identify classes of risks that are specific to storage and processing technologies and verify mitigation plans for those classes of risks; – identify security risk factors and threats for managing data, systems, personnel, and the physical plant; – identify the controls and roles to implement changes to address security risk factors; – assess development and implementation of security and risk management plans.		X		X		X

ANNEX B

SECURITY

(INFORMATIVE)

B1 INTRODUCTION

Potential areas of security concern include security risks in the operations of the organization which performs audits, and protection of accreditation, third party proprietary, and audit history records.

B2 SECURITY CONCERNS WITH RESPECT TO THE CCSDS DOCUMENT

B2.1 DATA PRIVACY

Related records must be protected from inadvertent and unauthorized disclosure. However, this document does not prescribe specific technologies or methodologies for recording or storing auditor accreditations and certifications, so privacy is not a direct concern of this document. Audit records resulting from candidate TDR reviews may also be subject to privacy concerns and may require privacy controls and management processes for audit organizations to maintain their credentials.

B2.2 DATA INTEGRITY

As this document does not prescribe any technologies or specific data management solutions, data integrity concerns are limited to those related to records management. While it is expected that any audit organizations must have records management processes in place to maintain the accuracy, credibility, and fixity of those records, the specifics of such processes are outside the scope of this document.

B2.3 AUTHENTICATION OF COMMUNICATING ENTITIES

Primary communicating entities are the Audit organizations, Candidate or certified TDRs. These organizations would be expected to authenticate each other through standard business practices.

B2.4 CONTROL OF ACCESS TO RESOURCES

Primary resources are data and personnel. Except insofar as the data may require protections described under Data Privacy, access controls are expected to be the normal and conventional forms used in business and commerce.

B2.5 AVAILABILITY OF RESOURCES

Data and personnel availability is primarily driven by the funding profiles of the respective organizational entities. Availability/acquisition of sufficient financial resources to carry out the duties of any of the organizations mentioned is outside the scope of this document.

B2.6 AUDITING OF RESOURCE USAGE

While it is expected that resource usage will be audited in accordance with the standard business accounting practices of the country or countries wherein the audit organizations are domiciled, the actual audit practices are outside of the scope of this document.

B3 POTENTIAL THREATS AND ATTACK SCENARIOS

Threats and risks of intentional hostile actions or inadvertent loss of data or personnel are beyond the scope of 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 fake organizations or false auditors must rely on standard business practices of individual audit organizations. Protection against loss of confidential information in the possession of the auditor must be provided by the security system of that auditor and the information transmission method which is agreed between the repository and auditor.

B4 AUDIT BY NON-CONFORMANT BODIES

The purpose of this document is to ensure that bodies which provide audit and certification services for candidate trustworthy digital repositories can inspire confidence that the certification has been performed with

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

A digital repository which is audited and certified by a body not conformant to this CCSDS Recommended Practice could run the risk of having a certificate which does not inspire confidence in its users. It also runs the risk that any confidential data revealed during the audit could be open to misuse.