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-1

MAGENTA BOOK

November 2011

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-1

## MAGENTA BOOK

**November 2011**

# AUTHORITY

| | |
|---|---|
| Issue: | Recommended Practice, Issue 1 |
| Date: | November 2011 |
| 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 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 e.V. (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.
- CSIR Satellite Applications Centre (CSIR)/Republic of South Africa.
- 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.
- Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
- Swedish Space Corporation (SSC)/Sweden.
- 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 |

# 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 performs ISO audits for assessing the trustworthiness of digital repositories using reference [1] and provides the appropriate 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

This document specifies requirements and provides guidance for bodies providing audit and certification of digital repositories, based on the metrics contained within ISO/IEC 17021 (reference [5]) and CCSDS 652.0-M-1/ISO 16363 (reference [1]). It is primarily intended to support the accreditation of bodies providing such certification.

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]-[6]). 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 digital repositories in accordance with CCSDS 652.0-M-1/ISO 16363 (reference [1]), some requirements and guidance 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 and guidance on the application of ISO/IEC 17021 for certification of 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 describes the Primary Trustworthy Digital Repository (TDR) Authorisation Body (PTAB).
- Sections 4 to 10 provide the normative rules against which an organization providing audit and certification of digital repositories may be judged, based on ISO/IEC 17021 (reference [5]).
- Annex A is a CCSDS required discussion of the security implications of applying this CCSDS Recommended Practice.

## 1.6 DEFINITIONS

### 1.6.1 ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| **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 |

### 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 [5]), 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.

**Certification Body:** third party that assesses and certifies the digital repository of a client organization.

**Primary TDR Authorisation Body (PTAB)**: The Primary TDR Authorisation Body will consist of internationally recognized experts in digital preservation, the membership building on members of the authors of CCSDS 652.0-M-1/ISO 16363 (reference [1]).

**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 documents contain provisions which, through reference in this text, constitute provisions of this Recommended Practice. 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 documents.

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

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

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

[4] *Guidelines for Quality and/or Environmental Management Systems Auditing*. International Standard, ISO 19011:2002. Geneva: ISO, 2002.

[5] *Conformity Assessment—Requirements for Bodies Providing Audit and Certification of Management Systems*. International Standard, ISO/IEC 17021:2006. Geneva: ISO, 2006.

[6] *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 standards (references [4]-[6]).

Section 3 describes the Primary TDR Authorisation Body (PTAB).

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.

Annex A is a CCSDS required discussion of the security implications of applying this CCSDS Recommended Practice.

# 3 PRIMARY TDR AUTHORISATION BODY (PTAB)

The Primary TDR Authorisation Body is a special body which provides audit and certification of candidate TDRs and also has the responsibility of accrediting training courses for auditors. The PTAB will also accredit other certification bodies. It will consist of internationally recognized experts in digital preservation, the membership including members of the CCSDS Digital Repository Audit and Certification Working Group, who produced CCSDS 652.0-M-1/ISO 16363 (reference [1]). It will

- undertake audits;
- make certification decisions;
- certify auditors (see 7.2.2.3);
- accredit auditor qualifications (see 7.2.2.3);
- accredit other TDR certification bodies;
- have a mechanism for adding new members to PTAB from internationally recognised experts in digital preservation.

The PTAB will be ISO 17011 certified as an accrediting body, and will become a member of the International Accreditation Forum (IAF) to provide oversight and transparency.

# 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 MANAGEMENT OF IMPARTIALITY

### 5.2.1 GENERAL

The requirements from ISO/IEC 17021:2006, 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 17021:2006, 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.

## 7.2 PERSONNEL INVOLVED IN THE CERTIFICATION ACTIVITIES

### 7.2.1 GENERAL

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

### 7.2.2 COMPETENCE OF CERTIFICATION BODY PERSONNEL

#### 7.2.2.1 General

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

a) knowledge of CCSDS 652.0-M-1/ISO 16363 (reference [1]) and other relevant normative documents;

b) understanding of digital preservation;

c) understanding of risk assessment and risk management of digitally encoded information;

d) technical knowledge of the digital preservation aspects which apply to the activity to be audited;

e) general knowledge of regulatory requirements relevant to TDRs;

f) knowledge of management systems;

g) understanding of the principles of auditing based on ISO 19011.

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 digital repository 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 digital repository 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 digital repository.

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.

#### 7.2.2.2 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 CCSDS 652.0-M-1/ ISO 16363 (reference [1]).

#### 7.2.2.3 Prerequisite Levels of Education, Work Experience, Auditor Training, and Audit Experience for Auditors Conducting TDR Audits (Except the Primary TDR Authorisation Body)

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

a) have at least four years full time practical workplace experience in data management, libraries, archives, or information technology with a focus on digital preservation;

b) have successfully completed five days of training in a course approved by the Primary TDR Authorisation Body (PTAB) or its delegate or successor, the scope of which covers TDR audits and audit management;

c) have gained experience in the entire process of assessing the trustworthiness of digital repositories prior to assuming responsibility for performing as an auditor; this experience should have been gained by participation in a minimum of two certification audits for a total of at least 20 days, including review of documentation and risk analysis, implementation assessment, and audit reporting;

d) have experience which is reasonably current, and some familiarity with current research in digital preservation;

e) keep their knowledge and skills in digital preservation and auditing up to date through continual professional development;

f) be certified by the Primary TDR Authorisation Body or its delegate or successor.

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

In addition to these requirements, 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 two complete TDR audits;

c) have demonstrated the capability to communicate effectively, both orally and in writing.

## 7.3 USE OF INDIVIDUAL EXTERNAL AUDITORS AND EXTERNAL TECHNICAL EXPERTS

The requirements from ISO/IEC 17021:2006, Clause 7.3 apply.

## 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.

## 8.2 CERTIFICATION DOCUMENTS

The requirements from ISO/IEC 17021:2006, Clause 8.2 apply.

## 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.

## 8.5 CONFIDENTIALITY

### 8.5.1 GENERAL

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

### 8.5.2 ACCESS TO ORGANIZATIONAL RECORDS

Before the certification audit, the certification body shall ask the client organization to report if any 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 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 17021:2006, Clause 8.6 apply.

# 9 PROCESS REQUIREMENTS

The requirements from ISO/IEC 17021:2006, Clause 9 apply. In addition, the following TDR audit and certification specific-requirements and guidance apply.

The criteria against which the digital repository of a client is audited shall be those outlined in the 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 17021:2006, Clause 10 apply.

# ANNEX A

# SECURITY

# (INFORMATIVE)

## A1 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 maintained by the PTAB.

## A2 SECURITY CONCERNS WITH RESPECT TO THE CCSDS DOCUMENT

### A2.1 DATA PRIVACY

The accreditation records maintained by the PTAB 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 volume, audit records resulting from TDR reviews may also be subject to privacy concerns, and the PTAB (or its designees or replacement) may require privacy controls and management processes for audit organizations to maintain their credentials.

### A2.2 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 both the PTAB and any audit organizations chartered by it 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.

### A2.3 AUTHENTICATION OF COMMUNICATING ENTITIES

Primary communicating entities are the audit organizations, candidate or accredited TDRs, and PTAB. These organizations would be expected to authenticate each other through standard business practices.

### A2.4 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.

## A2.5 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, including the PTAB, is outside the scope of this document.

## A2.6 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.

## A3 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 the PTAB or 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 method of transmission of information which is agreed between the repository and auditor.

## A4 AUDIT BY NON-CONFORMANT BODIES

The purpose of this document is to ensure that bodies which provide audit and certification services 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.