Purdue University PLM Center of Excellence

Spring 2016 Meeting – March 23, 2016

# Distilling ISO 16363 for PLM and the Supply Chain

Michael Witt

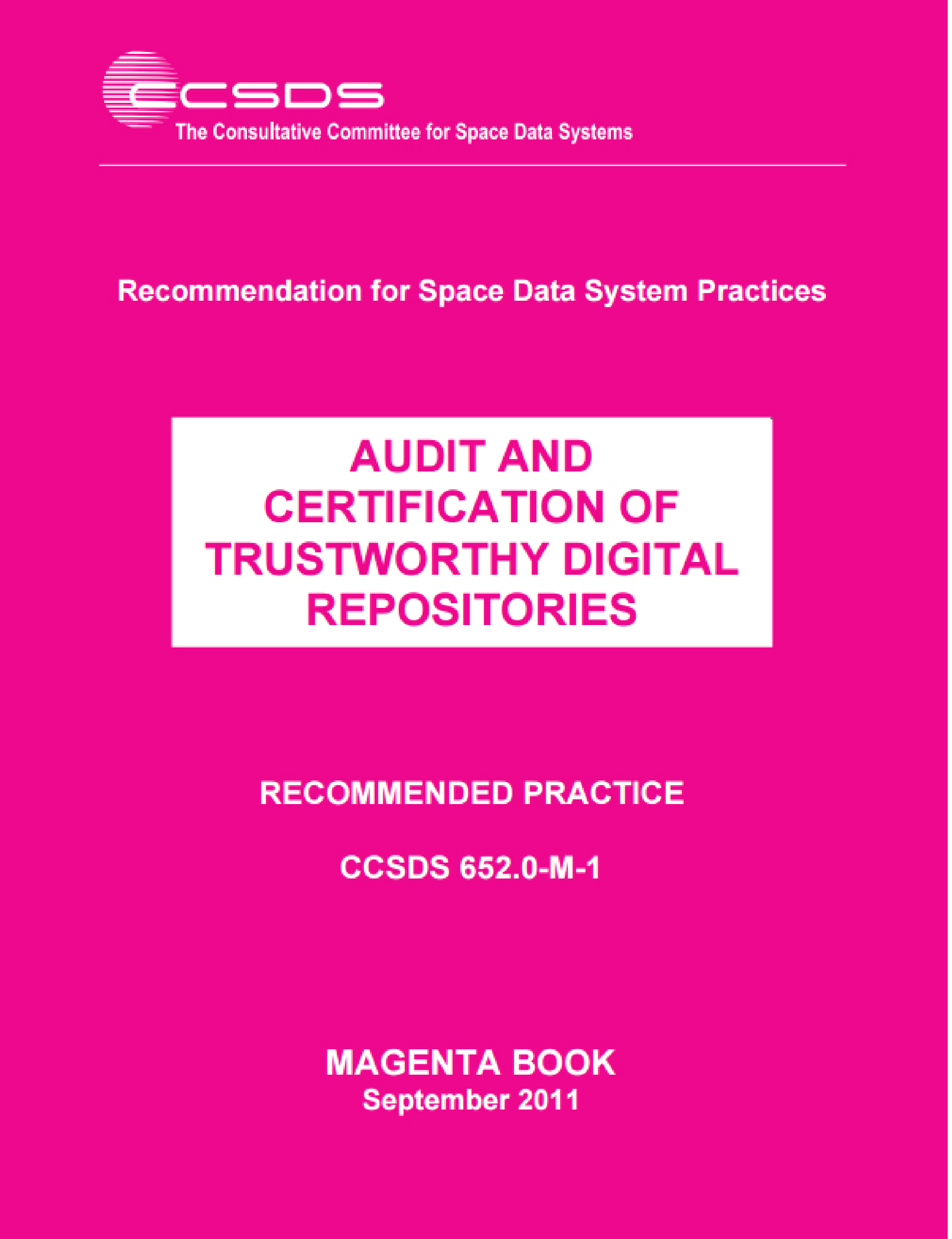
Faculty Fellow, PLM Center

Associate Professor of Library Science

Purdue University

mwitt@purdue.edu

# ISO 16363: Audit and certification of trustworthy digital repositories



CCSDS
The Consultative Committee for Space Data Systems

Recommendation for Space Data System Practices

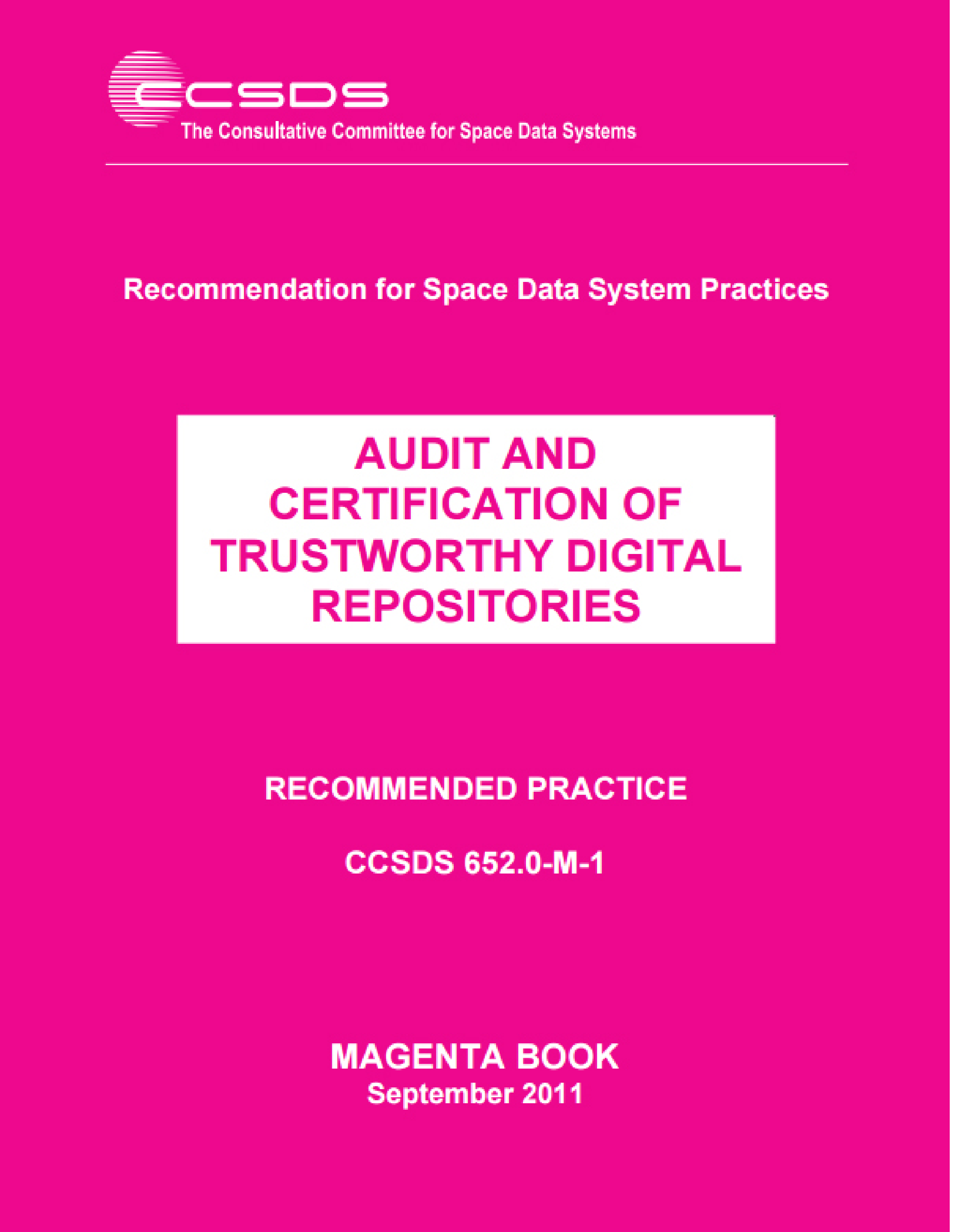
AUDIT AND CERTIFICATION OF TRUSTWORTHY DIGITAL REPOSITORIES

RECOMMENDED PRACTICE

CCSDS 652.0-M-1

MAGENTA BOOK
September 2011

- A repository is a system/service that enables secure and long-term management, preservation, and access to digital data
- Context is libraries and archives but many systems that manage data for PLM and supply chain are repository-like
- The role and importance of trust as a critical element in any context
- Organizations that manage repositories can’t simply identify themselves as trustworthy: objective measures are needed
- ISO 16363 provides a set of criteria that a repository can demonstrate meeting through evidence that is evaluated and certified by a third party auditor



CCSDS
The Consultative Committee for Space Data Systems

Recommendation for Space Data System Practices

AUDIT AND CERTIFICATION OF TRUSTWORTHY DIGITAL REPOSITORIES

RECOMMENDED PRACTICE

CCSDS 652.0-M-1

MAGENTA BOOK
September 2011

- Originated in the libraries and archives community as the Trustworthy Repository Audit Checklist from RLG, OCLC, and NARA (2007)
- Further developed into a standard by the Consultative Committee for Space Data Systems and published as ISO 16363 (2012)
- Builds on work done on ISO 14721 - the Open Archival Information Systems (OAIS) reference model
- Is considered the “gold” standard for repository certification in libraries and archives, other standards exist such as nestor, WDS, and DSA
- Complementary ISO 16919 defines a standard for certification of auditors and audit process
- Still emerging: first audits completed were in the last two years
- Many more using it as a tool for self-assessment

# A trustworthy digital repository

- Mandate to provide reliable, long-term access to managed digital resources to its user, now and into the future
- Understands & mitigates threats and risks
- Constant monitoring, planning, maintenance
- Conscious actions and implemented strategy for digital preservation
- Communicates service to users and demonstrates integrity, sustainability, and support
- Certification is not a one-time accomplishment but a regular cycle

*ISO 16363*

# 109 criteria in three main sections:

- Organizational infrastructure
  - Governance and organizational viability
  - Organizational structure and staffing
  - Procedural accountability and framework
  - Financial sustainability
  - Contracts, licenses, and liabilities
- Digital object management
  - Acquisition of data
  - Creation of Archival Information Package (AIP)
  - Preservation planning
  - AIP preservation
  - Information management
  - Access management
- Infrastructure and security risk management
  - Technical infrastructure risk management
  - Security risk management

*ISO 16363*

# 109 criteria in three main sections:

- **Organizational infrastructure**
  - **Governance and organizational viability**
  - **Organizational structure and staffing**
  - **Procedural accountability and framework**
  - Financial sustainability
  - Contracts, licenses, and liabilities
- Digital object management
  - Acquisition of data
  - **Creation of Archival Information Package (AIP)**
  - **Preservation planning**
  - AIP preservation
  - Information management
  - Access management
- **Infrastructure and security risk management**
  - **Technical infrastructure risk management**
  - **Security risk management**

*ISO 16363*

# Example ISO 16363 criterion

**5.2.1 The repository shall maintain a systematic analysis of security risk factors associated with data, systems, and physical plant**

**Supporting text**: This is necessary to ensure ongoing and uninterrupted service to the Designated Community.

**Examples of Ways the Repository Can Demonstrate It Is Meeting This Requirement**: Repository employs the codes of practice found in the ISO 27000 series of standard system control list; risk, threat, or control analysis

**Discussion**: The repository should conduct regular risk assessments and maintain adequate security protection in order to provide the expected/contracted levels of service, following codes of practice such as ISO 27000. ‘System’ here refers to more than IT systems, such as hardware, software, communications equipment, and firewalls. Fire protection and flood detection systems are also significant, as are means to assess personnel, management, and administrative procedures …

# For PLM/supply chain consideration

1. Content in an archive should be managed
2. Plan for long-term digital archiving that goes beyond backups
3. Documentation and policies that clearly communicate scope of archive and what services it provides
4. Define designated community (users) and use cases for archive
5. Trained staff, responsibilities clearly defined and supported by the company
6. Define in explicit terms what is being archived and how (include metadata, provenance, documentation, etc.)
7. Monitoring and reporting, especially to verify the integrity of data
8. Access policies (ISO 16363 insufficient here)
9. Risk assessment, disaster and recovery plan/s
10. Adequately maintained and secure technology (software, hardware)

# Closing thoughts

- ISO 16363 has a strong bias towards open access and the scholarly (not corporate) environment; some parts are more appropriate than others when it comes to data in PLM/supply chain
- Value for a company in thinking more like an archive when it comes to data that must be kept for the long term, e.g., product data, and the cost when data and/or trust are lost
- Like PLM, archiving is a continuum – nothing is static, and all processes, systems, policies, training, assessments, and such should be continually revisited and updated
- If you currently maintain an archive, review ISO 16363 (77 pages) and consider self-assessment using appropriate criteria

# Links

Audit and Certification of Trustworthy Digital Repositories, Recommended Practice: CCSDS 652.0-M-1 (Magenta Book – free download):

http://public.ccsds.org/publications/archive/652x0m1.pdf

ISO 16363:2012--Space Data and Information Transfer Systems--Audit and Certification of Trustworthy Digital Repositories (~$200)

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56510