# AAF - Groupe PIN
# ISO 16363: principles and status report

Dr David Giaretta
Director of PTAB
david@giaretta.org
http://www.iso16363.org and http://www.giaretta.org

# Outline

- What are the challenges of digital preservation?
  - Lessons learned from audits
- ISO 16363
  - Relationship to other standards
  - ISO certification
    - ISO audit process
- Is ISO 16363 certification **impossibly difficult** as some claim?
- Who can audit?
- What about a Maturity Model?
- What next?

# What are the Challenges for Digital Preservation and ISO 16363 in particular?

- 1110100100 could mean anything
- Everything changes
- We forget what may change
- We forget how quickly details can be forgotten
- Lack of clarity about what is being preserved and for whom
- Not recognising limitations of solutions
  - thinking what works for one case will work for every case
- Deciding which organisations can be trusted to preserve
  - And for how long can they be trusted?
- How to audit

# What is Digital Preservation?

- Preservation of information encoded in bits, with evidence of authenticity
- NOT just bit preservation (which is relatively easy)
- NOT just format (a great deal of which can be captured automatically)
- MUST include **semantics** (which are more difficult and cannot be captured automatically)
- Is likely to include software (which will have many options)
- Because otherwise……

- Information will be lost

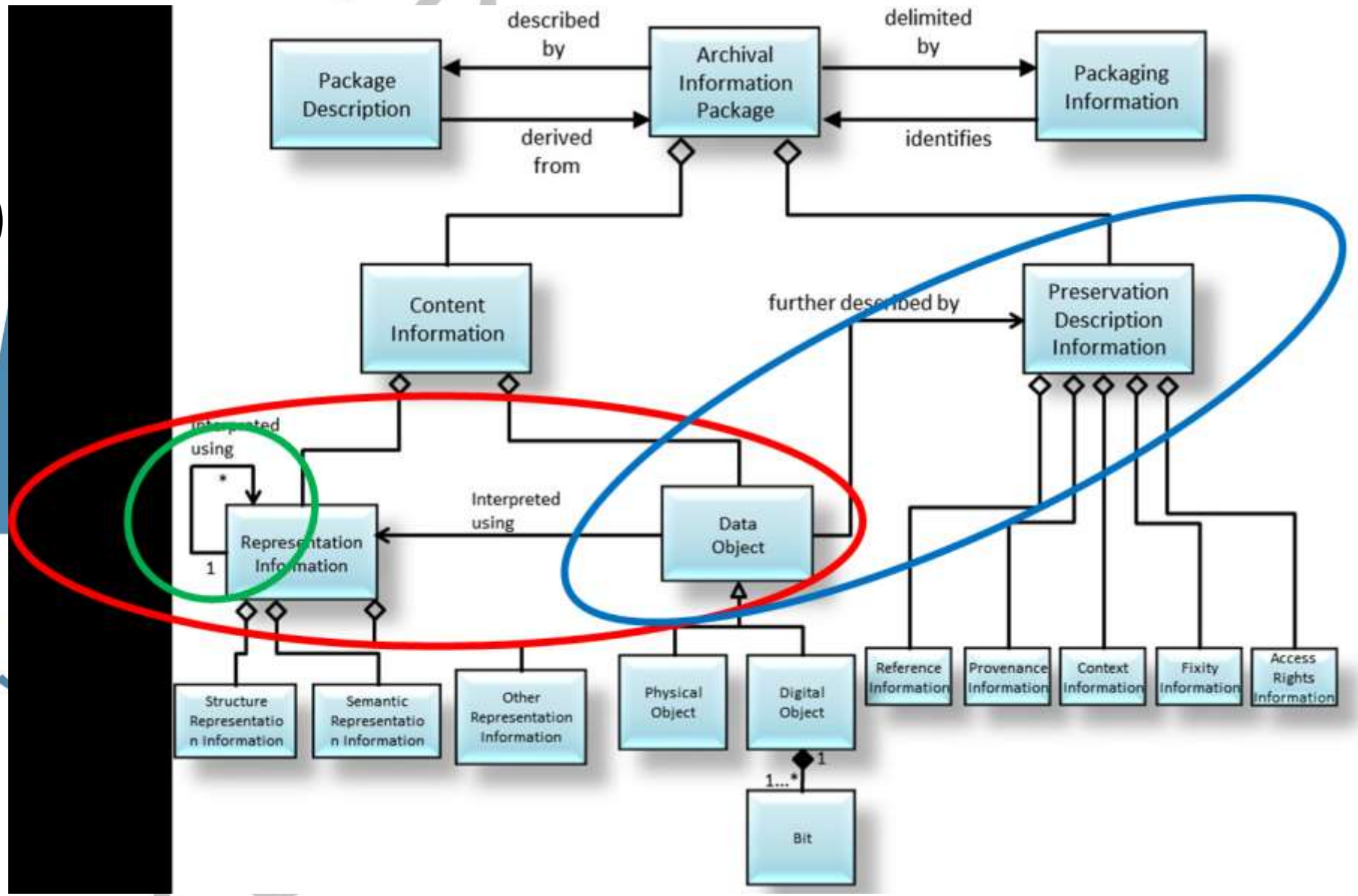
# What is involved in preservation?

- Resources including
  - Money
  - People
- Commitment
- Organisation
- Processes
- Software Systems
- Hardware Systems

**ALL CHANGE**

# OAIS conformance requires support for

- OAIS Information Model (version 3)
- OAIS Mandatory responsibilities



# Why are AIPs important?

- To ensure that the archive has everything needed for preserving the information of interest (target of preservation)
  - Easy to check
  - Must also preserve those Extra components such as provenance.
    - PREMIS – but what vocabulary is being used
    - OPM – what schema
    - Home grown – what format, semantics, software?
    - NOTE that the collection of provenance does not stop on hand-over to the archive – what is the archive doing for preservation, who is responsible, how has it been checked .....etc ?
      - ....and how has that information been encoded and preserved.... Probably not the original way.
- Must be able to export (logically) complete AIPs into new system.
  - Does NOT need to be a single file.

# TEST claims – everyone lies ( or misleads)

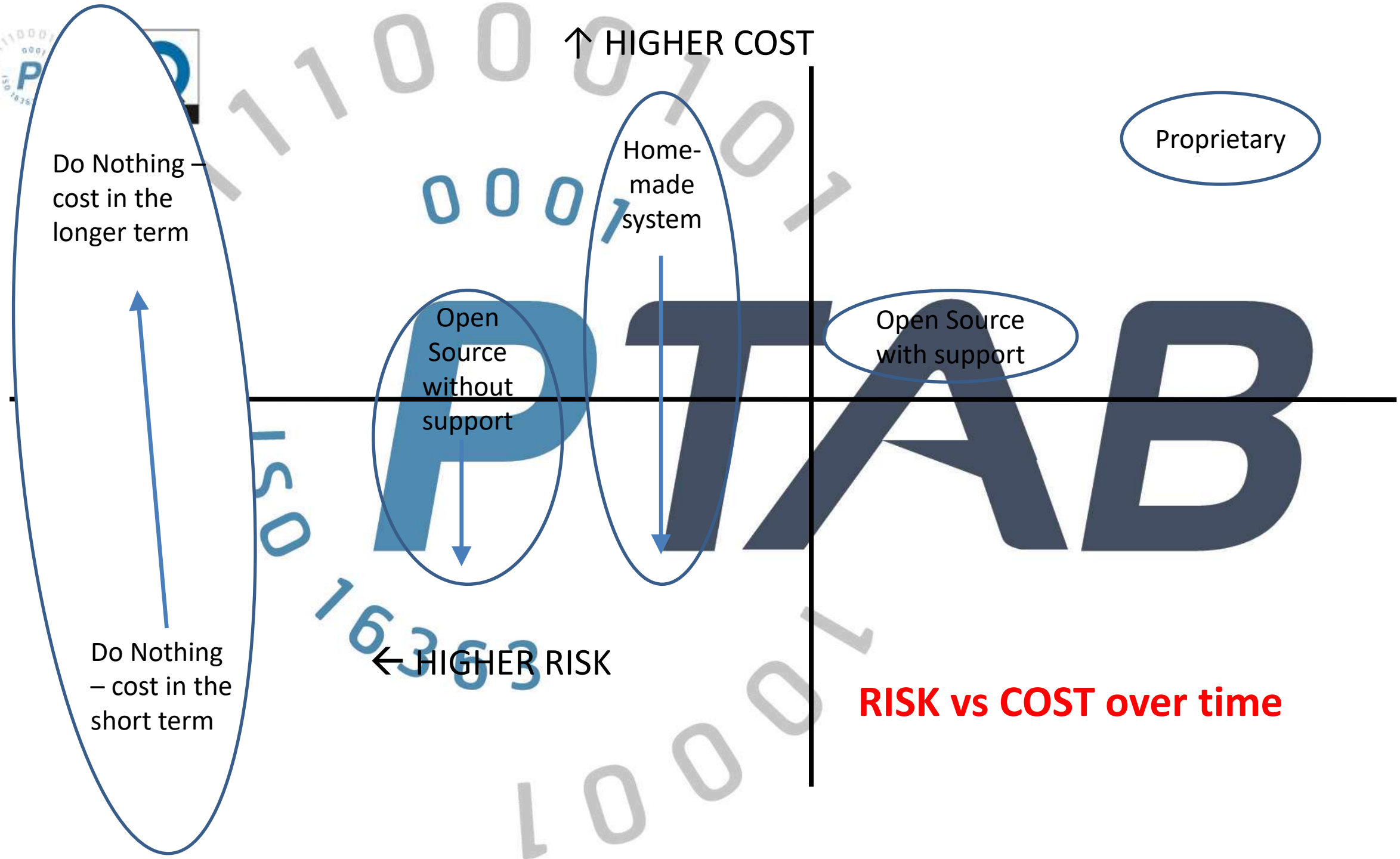
- Are AIPs complete?
  - E-ARK AIP cannot be complete – a simple check will verify this
  - What most systems CLAIM is a AIP -- actually is **NOT an OAIS AIP**
    - Check it yourselved – it is pretty simple – just ask the questions by looking at the diagram in OAIS:
      1. Where is the Semantics?
      2. Where is the software?
      3. Is there enough detail about even the FORMAT??
         1. PRONOM is essentially **useless** **(** e.g. ".txt" file)
         2. LINUX "file" command is much better
- The real OAIS AIP is what the vendor/developer claims is an OAIS AIP – PLUS the missing information

# Commercial solutions – costs and benefits

- 300TB, 2 extra copies in cool storage, approx US$ 100K per year.
- Benefits
  - Able to cope with large, frequent ingests using Cloud
  - Security checks on software – penetration tests (in some cases)
  - Support and updates
- Downsides:
  - Almost NONE support the OAIS Information Model
  - Almost NONE can help a respository fulfil its mandatory responsibilities
  - BOTH these are needed for the repository to be OAIS conformance
    - In which archives using this software CANNOT be ISO 16363 certified
    - Unless something is added – may be something quite simple

# Open source solutions

- Do many useful things
- Cheaper than the commercial software
- BUT, they do not support the OAIS Information Model
  - Although may be configurable if done with care
  - Or may need additional software


↑ HIGHER COST
Do Nothing – cost in the longer term
Home-made system
Proprietary
Open Source without support
Open Source with support
Do Nothing – cost in the short term
← HIGHER RISK
RISK vs COST over time

# 3 Fundamental Preservation Methods

New draft makes the various techniques explicit: the Content Information being preserved may be

- kept by the Archive but may be changed or
- kept by the Archive unchanged or
- not kept by the Archive, but instead be handed on to another Archive

Each of these three imply the following:

- In case (1) the Archive may Transform the Content Data Object
- In case (2) the Archive may add Representation Information to ensure the Content Information is Independently Understandable
- In case (3) the Archive may hand over the complete AIP which contains the Content Information

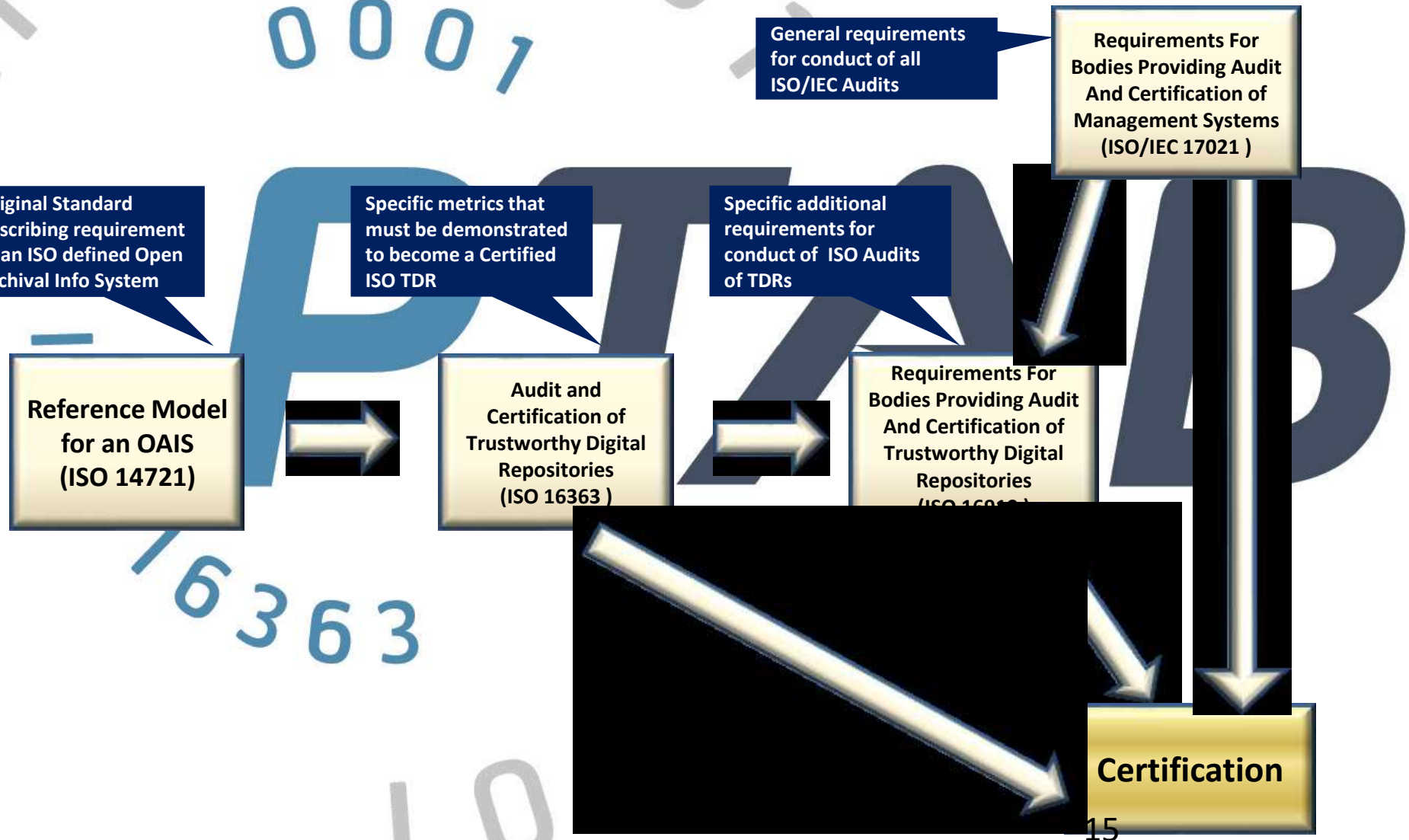
# Suggested Handover timescale checks

- Need enough time to create and hand over all the AIPs
  - Time to collect all the components needed
  - For example:
    - every 6 months the time remaining in the guaranteed funding envelope should be compared with the estimated time needed to export the AIPs. If it appears that there is a risk that the funding would run out in twice the time that the AIPs can be exported then the AIPs should all be created and made ready for transfer if or when the succession plan is to be implemented

# Designated Community

- Must be carefully defined by the archive
- Determines how much Representation Information is needed
- Can be tested

# Relationship between standards



# Why ISO?

- ISO audits are used across the World and in vast numbers of areas on which our lives depend.
- The ISO process ensures international consistency of certification and their international recognition
- Everyone at every level is tested/evaluated every year

# ISO 17021

…specifies **requirements for bodies providing audit and certification of management systems**. It gives **generic requirements** for such bodies performing audit and certification in the field of quality, the environment and other types of management systems. Such bodies are referred to as certification bodies. **Observance of these requirements is intended to ensure that certification bodies operate management system certification in a competent, consistent and impartial manner**, thereby **facilitating the recognition of such bodies and the acceptance of their certifications on a national and international basis**. This part of ISO/IEC 17021 serves as a foundation for **facilitating the recognition of management system certification in the interests of international trade**.

**Certification of a management system provides independent demonstration that the management system of the organization**:

a) conforms to specified requirements;

b) is capable of consistently achieving its stated policy and objectives;

c) is effectively implemented.

Conformity assessment, such as the certification of a management system, thereby **provides value to the organization, its customers and interested parties**.

# ISO 17021 Principles for inspiring confidence include

- impartiality;
- competence;
- responsibility;
- openness;
- confidentiality;
- responsiveness to complaints;
- risk-based approach.

# Risk-based approach

Certification bodies need to take into account the risks associated with providing competent, consistent and impartial certification. Risks may include, but are not limited to, those associated with:

- the objectives of the audit;
- the sampling used in the audit process;
- real and perceived impartiality;
- legal, regulatory and liability issues;
- the client organization being audited and its operating environment;
- impact of the audit on the client and its activities;
- health and safety of the audit teams;
- perception of interested parties;
- misleading statements by the certified client;
- use of marks.

# ISO 16363

# Audit and Certification of Trusted Digital Repositories

Designed for audit – self audit and independent auditors

- Hierarchy of metrics – to make the auditor look at more and more specific details when required
- Metrics and their structure:
  - Statement of requirement
  - Supporting text
  - Examples of Ways the Repository can Demonstrate it is Meeting this Requirement
  - Discussion
- NUMBER of metrics at each level

| Metrics→ | Top level X | Metric X.X | Sub-metric X.X.X | Sub-sub metric X.X.X.X | Sub-sub-sub metric X.X.X.X.X |
|---|---|---|---|---|---|
| Organisational Infrastructure | 1 | 6 | 21 | 31 | 31 |
| Digital Object Management | 1 | 7 | 36 | 62 | 67 |
| Infrastructure and Security Risk Management | 1 | 3 | 9 | 16 | 27 |
| TOTAL | 3 | 16 | 66 | 109 | 125 |

## 3 ORGANIZATIONAL INFRASTRUCTURE

### 3.1 GOVERNANCE AND ORGANIZATIONAL VIABILITY

3.1.1 The repository shall have a mission statement that reflects a commitment to the preservation of, long term retention of, management of, and access to digital information.

3.1.2 The repository shall have a Preservation Strategic Plan that defines the approach the repository will take in the long-term support of its mission.

3.1.2.1 The repository shall have an appropriate succession plan, contingency plans, and/or escrow arrangements in place in case the repository ceases to operate or the governing or funding institution substantially changes its scope.

3.1.2.2 The repository shall monitor its organizational environment to determine when to execute its succession plan, contingency plans, and/or escrow arrangements.

3.1.3 The repository shall have a Collection Policy or other document that specifies the type of information it will preserve, retain, manage, and provide access to.

### 3.2 ORGANIZATIONAL STRUCTURE AND STAFFING

3.2.1 The repository shall have identified and established the duties that it needs to perform and shall have appointed staff with adequate skills and experience to fulfill these duties.

3.2.1.1 The repository shall have identified and established the duties that it needs to perform.

3.2.1.2 The repository shall have the appropriate number of staff to support all functions and services.

3.2.1.3 The repository shall have in place an active professional development program that provides staff with skills and expertise development opportunities.

### 3.3 PROCEDURAL ACCOUNTABILITY AND PRESERVATION POLICY FRAMEWORK

3.3.1 The repository shall have defined its Designated Community and associated knowledge base(s) and shall have these definitions appropriately accessible.

3.3.2 The repository shall have Preservation Policies in place to ensure its Preservation Strategic Plan will be met.

3.3.2.1 The repository shall have mechanisms for review, update, and ongoing development of its Preservation Policies as the repository grows and as technology and community practice evolve.

3.3.3 The repository shall have a documented history of the changes to its operations, procedures, software, and hardware.

3.3.4 The repository shall commit to transparency and accountability in all actions supporting the operation and management of the repository that affect the preservation of digital content over time.

3.3.5 The repository shall define, collect, track, and appropriately provide its information integrity measurements.

3.3.6 The repository shall commit to a regular schedule of self-assessment and external certification.

### 3.4 FINANCIAL SUSTAINABILITY

3.4.1 The repository shall have short- and long-term business planning processes in place to sustain the repository over time.

3.4.2 The repository shall have financial practices and procedures which are transparent, compliant with relevant accounting standards and practices, and audited by third parties in accordance with territorial legal requirements.

3.4.3 The repository shall have an ongoing commitment to analyze and report on financial risk, benefit, investment, and expenditure (including assets, licenses, and liabilities).

### 3.5 CONTRACTS, LICENSES, AND LIABILITIES

3.5.1 The repository shall have and maintain appropriate contracts or deposit agreements for digital materials that it manages, preserves, and/or to which it provides access.

3.5.1.1 The repository shall have contracts or deposit agreements which specify and transfer all necessary preservation rights, and those rights transferred shall be documented.

3.5.1.2 The repository shall have specified all appropriate aspects of acquisition, maintenance, access, and withdrawal in written agreements with depositors and other relevant parties.

3.5.1.3 The repository shall have written policies that indicate when it accepts preservation responsibility for contents of each set of submitted data objects.

3.5.1.4 The repository shall have policies in place to address liability and challenges to ownership/rights.

3.5.2 The repository shall track and manage intellectual property rights and restrictions on use of repository content as required by deposit agreement, contract, or license.

# Who can evaluate repositories?

- Me?
- You?
- Anyone?

# ISO Standards – who can audit?

| METRIC | STANDARD FOR REQUIREMENTS FOR AUDITORS |
| --- | --- |
| • OAIS – ISO 14721 | • None |
| • ISO 16363 | • ISO 16919 |
| • ISO 27001 | • ISO 19896 |
| • ISO 15489 | • None |

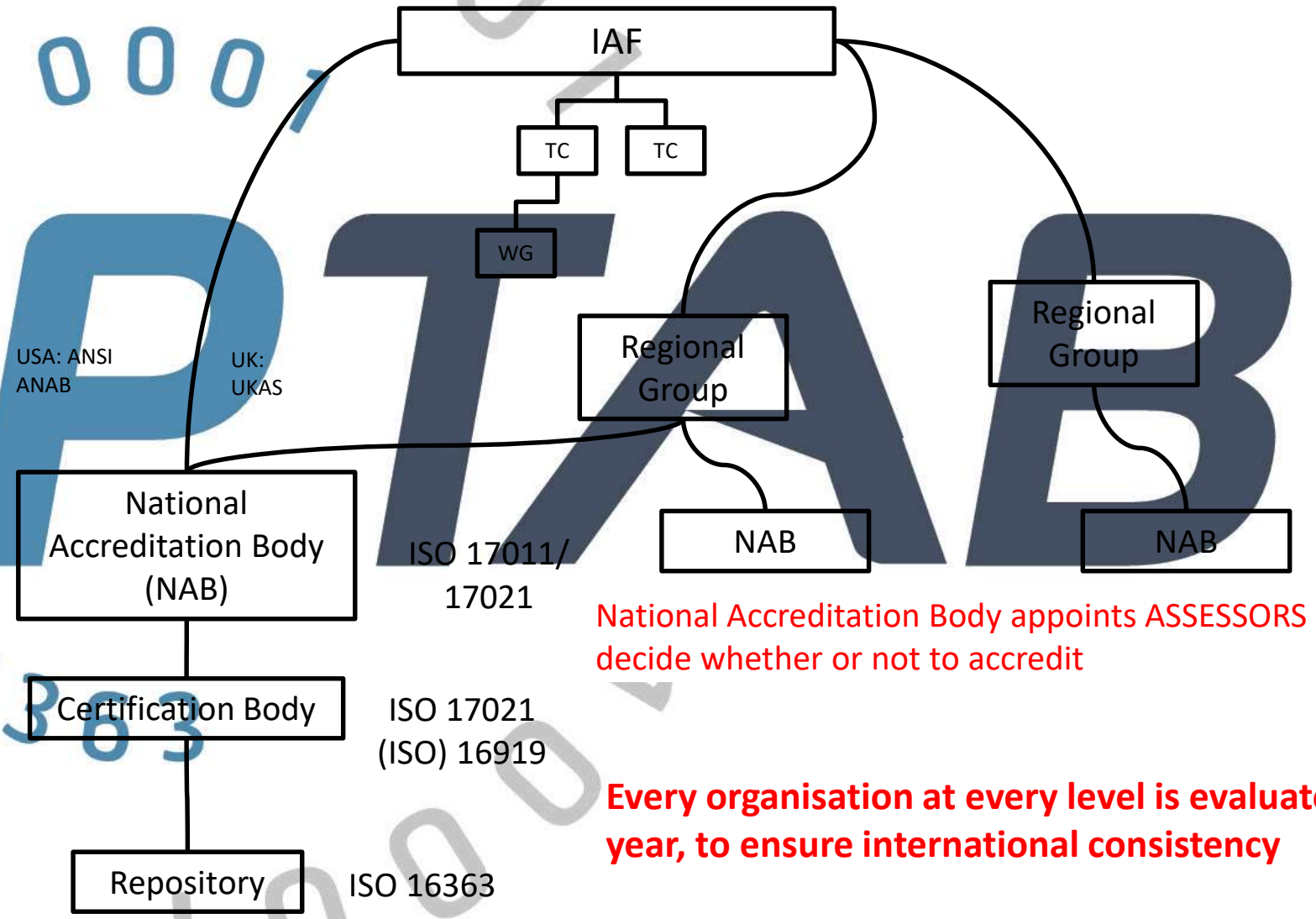
# Auditor behaviour

a) ethical, i.e. fair, truthful, sincere, honest and discreet;
b) open-minded, i.e. willing to consider alternative ideas or points of view;
c) diplomatic, i.e. tactful in dealing with people;
d) collaborative, i.e. effectively interacting with others;
e) observant, i.e. actively aware of physical surroundings and activities;
f) perceptive, i.e. instinctively aware of and able to understand situations;
g) versatile, i.e. adjusts readily to different situations;
h) tenacious, i.e. persistent and focused on achieving objectives;
i) decisive, i.e. reaches timely conclusions based on logical reasoning and analysis;
j) self-reliant, i.e. acts and functions independently;
k) professional, i.e. exhibiting a courteous, conscientious and generally business-like demeanour in the workplace;
l) morally courageous, i.e. willing to act responsibly and ethically even though these actions may not always be popular and may sometimes result in disagreement or confrontation;
m) organized, i.e. exhibiting effective time management, prioritization, planning, and efficiency.

# Example competences from ISO 16919

| 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:<br>– determine a variety of digital preservation strategies and where they should be applied;<br>– identify changes that may endanger preservation, how they may be monitored, and how they may be mitigated;<br>– identify types of evidence that may support claims of effective digital preservation;<br>– understand how the various parts of an AIP should be monitored and preserved against intentional and unintentional change;<br>– identify changes in the preservation system that may be relevant to AIP preservation and responses to them that are appropriate. | | X | | X | | X |

# ISO Accreditation and Certification




**PTAB**

**e.g. GPO**

National Accreditation Body appoints ASSESSORS to help decide whether or not to accredit

**Every organisation at every level is evaluated every year, to ensure international consistency**

# PTAB accreditation

- PTAB created a great deal of documentation and procedures consistent with ISO 17021 and ISO 16919, to ensure consistency between auditors
- Auditors and auditor levels agreed with Assessors

# Evaluating …..

- People and organisations who audit:
  - ISO 16919 list of competences
- Process
  - ISO 17021
    - Two Stages
    - Documentation
    - Complaint etc
- Criteria
  - ISO 16363

# ISO Process – the auditor must:

- determine whether it is able to perform the audit. If so, must
- develop the audit programme which must include
  - An initial certification with these components
    - Stage 1 – often an off-site review of documentation - identifying areas of concern that could be classified as a nonconformity during stage 2.
    - Stage 2 – on-site review using a defined process to identify nonconformities
    - Repository resolves issues
    - Certification committee makes decision on whether or not to award certificate
  - Annual surveillance audit in year 1 and year 2 after the initial certification
  - Re-certification audit in year 3, to begin the cycle again

# PTAB Process following ISO 17021

**Start**

Repository wants to be certified Trustworthy according to ISO 16363

Initial discussion between repository and PTAB

Repository completes PTAB application form

PTAB reviews application & may request additional information

PTAB provides audit plan with cost estimate

Repository signs contract and makes initial payment

**Stage 1**

PTAB starts Stage 1 of audit

Repository sends completed self-audit spreadsheet and related docs

PTAB plans Stage 1 audit and selects auditors

PTAB conducts Stage 1 audit

PTAB reports areas of concern found in Stage 1 audit

Repository acts to resolve areas of concern

**Stage 2**

When concerns are resolved, Stage 2 of audit initiated

PTAB plans Stage 2 audit and confirms audit team

PTAB auditors conduct Stage 2 audit on-site

PTAB reports non-conformances & certification recommendation

Repository agrees causes and corrective actions with PTAB

Repository resolves major non-conformances

**Certification**

PTAB certification committee makes certification decision

If PTAB grants certification, certification mark is issued

Repository displays its certification

**Surveillance and re-certification**

Repository wants to maintains ISO 16363 certification

First Surveillance audit

Second Surveillance audit

Re-certification audit

# Is ISO 16363 certification **impossibly difficult** as some claim?

- Any good repository will be doing a lot that is right
- There will be some areas that are weak:
  - Lack of clear definition of Designated Community
  - Lack of Representation Information
    - May not need much right now, but must be able to deal with it later
      - Especially things that are unique to your archive
    - Not just for “target of preservation” but also Provenance, Fixity etc
  - Lack of clear documentation about what “everyone knows”
- BUT….
- Lots of challenges are common and knowledge can be shared
- Budgets cannot be guaranteed forever
  - Just needs to be long enough to be able to prepare for transfer AIPs to a successor archive

Can be fixed with

- make clear decision
- collect RepInfo – just needs clear thinking
- write documentation
- speak to other archives
- Read OAIS, create proper AIPs and make a rough agreement for successor

# Lessons learned (1)

- It is important that audits are carried out annually
  - Allows auditors to look at timescales e.g.
    - what is changing?
    - is there time to prepare for hand over?
  - Budgets do not have to be guaranteed forever
    - Budget determine the timescales to check against

# Lessons learned (2)

- Sampling is essential
- Perfection is not necessary
  - Just has to be good enough

# What about a Maturity Model?

- ISO audits do not work with a maturity model
- The question is whether the archive is able to do what is needed
  - If it is not able to do so then major nonconformities are identified which the archive must fix
- But it does NOT have to be perfect
  - Minor nonconformities that are identified do have to be fixed
  - Other minor nonconformities may be found in subsequent audits
- So the archive can do what is needed if it is certified
- A Maturity Model comes into play when the archive does not want to marked as **unable** to do what it must do.

# What next?

- Improve the preservation capabilities of archives
- Ensure there are enough archives seeking audit/certification to
  - Encourage other organisations to seek accreditation to perform ISO 16363 audits so that the auditing can scale up

# References


- **ISO/IEC 17021-1:2015** Conformity assessment -- Requirements for bodies providing audit and certification of management systems -- Part 1: Requirements, available from http://www.iso.ch
- Audit and Certification of Trustworthy Digital Repositories. Magenta Book. Issue 1. September 2011., available from https://public.ccsds.org/Pubs/652x0m1.pdf also known as **ISO 16363:2012**
- Reference Model for an Open Archival Information System (OAIS). Magenta Book. Issue 2. June 2012, available from https://public.ccsds.org/Pubs/650x0m2.pdf also known as **ISO 14721:2012**,
- Requirements for Bodies Providing Audit and Certification of Candidate Trustworthy Digital Repositories. Magenta Book. Issue 2. March 2014, available from https://public.ccsds.org/Pubs/652x1m2.pdf also known as **ISO 16919:2014**


Thank You
PTAB
ISO 16363