# APPLYING DP **STANDARDS** FOR ASSESSMENT & PLANNING

Bertram Lyons | @bertramlyons
AVPreserve | @avpreserve
PASIG 2016 | Prague

# ISO 16363:2012

Audit & Certification of Trustworthy Digital Repositories

Defines a recommended practice for assessing the trustworthiness of digital repositories. It is applicable to the entire range of digital repositories.

# Who Is Using ISO 16363?

This document is meant primarily for those responsible for auditing digital repositories and also for those who work in or are responsible for digital repositories seeking objective measurement of the trustworthiness of their repository.

**Some institutions may also choose to use these metrics during a design or redesign process for their digital repository.**

**- ISO 16363: Audit and certification of trustworthy digital repositories**

certification

VS.

assessment

# self-assessment

PTAB website: http://www.iso16363.org/preparing-for-an-audit/

# external assessment

Partner with trusted third-party group to evaluate current performance

Paramount
A VIACOM COMPANY

Smithsonian
Institution

MoMA
The Museum of Modern Art

New York
Public
Library

VIAA


Discover
interviews
documentation
demonstration
evidence
Analyze
Plan
Improve

Organizational Infrastructure

Digital Object Management

Infrastructure & Security

avps

3.1 Governance and Organizational Viability

3.2 Organizational Structure and Staffing

3.3 Procedural and Policy Framework

3.4 Financial Stability

3.5 Contracts, Licenses, and Liabilities

# ORGANIZATIONAL INFRASTRUCTURE

# 3.1 Governance and Organizational Viability

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. Without one, it is unclear what is in collection scope. Also, it becomes more difficult to say no to out of scope content when you don't have a policy to point to.

(To score well in this metric, a policy both exists and is documented.)

ORGANIZATIONAL INFRASTRUCTURE

# DIGITAL OBJECT MANAGEMENT

4.1 Ingest: Acquisition of Content (SIPs)

4.2 Ingest: Creation of AIPs

4.3 Preservation Planning

4.4 AIP Preservation

4.5 Information Management

4.6 Access Management

# DIGITAL OBJECT MANAGEMENT

## 4.2 Ingest: Creation of AIPs

4.2.2 The repository shall have a description of how AIPs are constructed from SIPs. Organizations are ingesting AIPs all the time, but is the process documented in such a way that all changes occur as expected when SIPs are produced based on delivery requirements? Is the AIP to SIP relationship 1:1? Does normalization happen? Are these difference documented and logged? Does it happen consistently with all assets?

# TECH INFRASTRUCTURE & SECURITY RISK MANAGEMENT

5.1 Technical Infrastructure Risk Management

5.2 Security Risk Management

# TECH INFRASTRUCTURE & SECURITY RISK MANAGEMENT

5.2.4 The repository shall have a suitable written disaster preparedness and recovery plan, including at least one off-site backup of all preserved information together with an off-site copy of the recovery plan. This metric speaks to having a plan in place, but also to making sure it is well documented and communicated and that the technology is disaster-prepared, but so is the organization administratively.

5.2 Security Risk Management

*criteria per category*

**ISO 16363 Audit & Certification of TDRs**

| | |
|---|---|
| Organizational Infrastructure | 25 |
| Digital Object Management | 60 |
| Tech Infrast. & Security Risk Mgmt. | 24 |

*109 total criteria*

*3 categories*

4.2.2 The repository shall have a description of how AIPs are constructed from SIPs.

> “There is a clear understanding of any changes that take place to the files during the ingest process because changes are logged throughout. Submitted files must conform to delivery requirements so that a systematic ingest process can be applied to all files, which includes, for example, renaming files to conform to a documented structure and recording folder hierarchies.“

Supported by interviews, demonstrations of the ongoing logging actions of the repository system, and documentation in the way of workflow guides.

0 ***non-compliant or not started:*** The repository has not yet addressed the requirement.

1 ***slightly compliant:*** The repository has something in place, but has a lot of work to do in addressing the requirement.

2 ***half compliant:*** The repository has partially addressed the requirement and has significant work remaining to fully address the requirement.

3 ***mostly compliant:*** The repository can demonstrate that it has mostly addressed the requirement and is working on full compliance.

4 ***fully compliant:*** The repository can demonstrate that it has comprehensively addressed the requirement.

**DOCUMENTATION**
records of policy, procedure, and outcomes of activities

**POLICY**
the definition of approaches and protocol for repository functions and procedures

**PROCEDURE**
specification of preservation and infrastructure management activities

**SOFTWARE DEVELOPMENT/CONFIGURATION**
development or configuration of preservation systems

**INFRASTRUCTURE**
procurement, monitoring, and management of hardware infrastructure

**OPERATIONS**
organizational infrastructure including funding, staffing, and strategy

# SHORT

**0-1 YEARS**

# MEDIUM

**1-2 YEARS**

# SUSTAIN

**REVISIT IN 2 YEARS**

# SHORT

*immediate needs*

**First**

**Second**

**Third**

# MEDIUM

**First**

**Second**

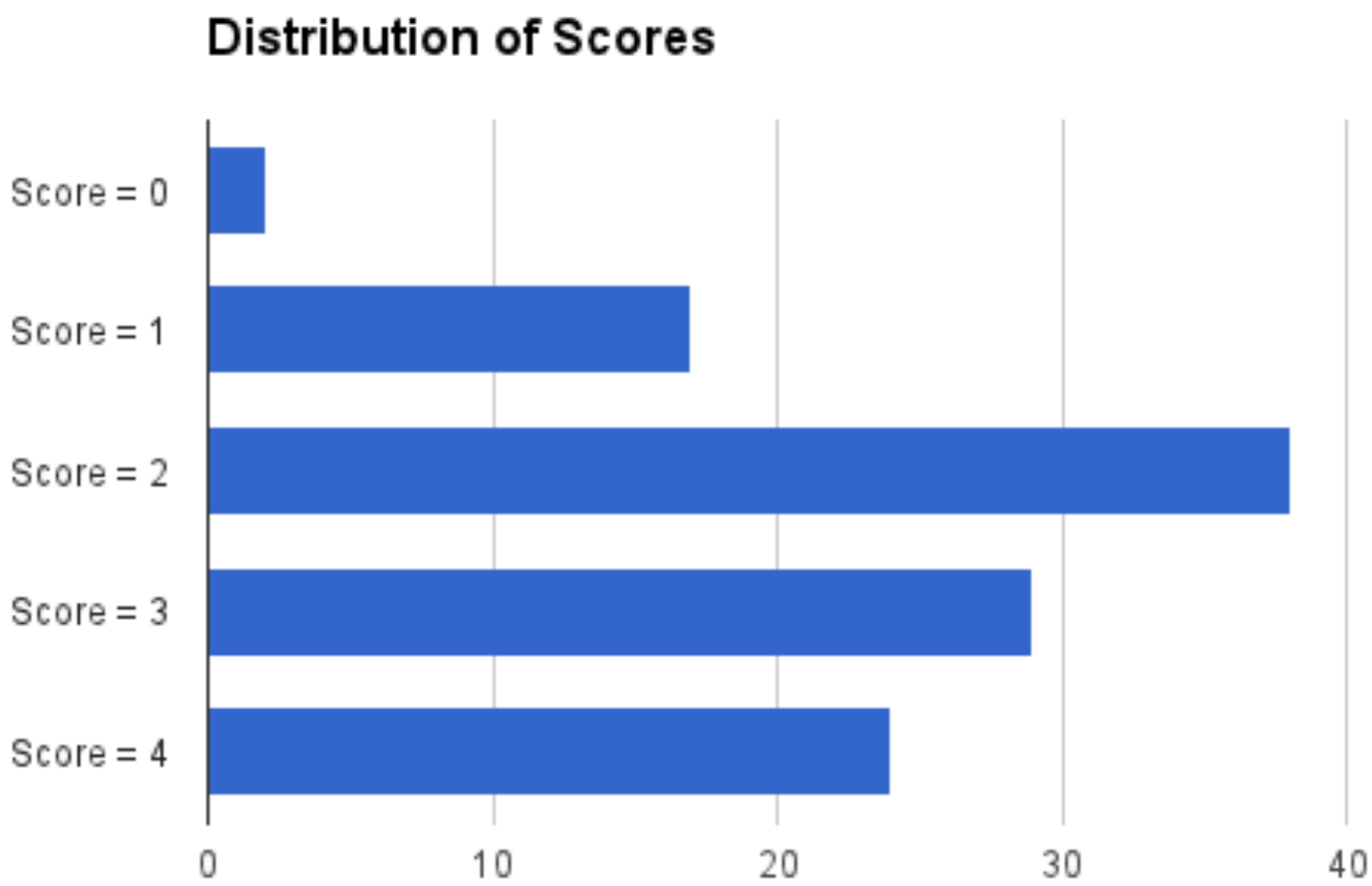
**Third**

*less pressing needs*

## 4.2.6.3 Ensure PDI is persistently associated with relevant CI.

> “In most cases, the PDI is persistently associated with the content information in the repository system. The only exception [a related system ID] number. It was assumed that this ID was being captured and stored in the repository system, however, during the visit it was discovered that this value has not been captured. We recommend that this ID be added to the repository system records as intended to ensure persistent association between original physical objects and digitized counterparts.”

Score of 3, timeframe of short second, type=software




key:
4 = fully compliant
3 = mostly compliant
2 = half compliant
1 = slightly compliant
0 = non-compliant

Total Average Score:
**2.51**

| 3 | Organizational Infrastructure | Score |
|---|---|---|
| 3.1 | **Governance and Organizational Viability** | |
| 3.1.1 | Mission Statement | 4 |
| 3.1.2 | Preservation Strategic Plan | 4 |
| 3.1.2.1 | Succession Plan / Escrow | 3 |
| 3.1.2.2 | Monitoring for Succession/Contingency | 2 |
| 3.1.3 | Collection Policy | 4 |
| 3.2 | **Organizational Structure and Staffing** | |
| 3.2.1 | Staff and Structure are well-documented | 3 |
| 3.2.1.1 | Well-documented duties necessary to be TDR | 3 |
| 3.2.1.2 | Appropriate # of staff | 3 |
| 3.2.1.3 | Active professional development program | 2 |
| 3.3 | **Procedural Accountability and Preservation Policy Framework** | |
| 3.3.1 | Defined designated community | 3 |
| 3.3.2 | Preservation policies in place | 3 |
| 3.3.2.1 | Mechanisms to review and update preservation policies | 2 |
| 3.3.3 | Documented history of changes to operations, procedures, software, hardware | 2 |
| 3.3.4 | Demonstrated commitment to transparency and accountability | 3 |
| 3.3.5 | Define, collect, track information integrity measurements | 4 |
| 3.3.6 | Commitment to regular schedule of self-assessment and certification | 3 |
| 3.4 | **Financial Sustainability** | |
| 3.4.1 | Short and long-term business planning in place | 4 |
| 3.4.2 | Sound legal financial practices | 4 |
| 3.4.3 | Commitment to analyze and report on financial risk, benefit, investment, expenditure | 3 |
| 3.5 | **Contracts, License, and Liabilities** | |
| 3.5.1 | Contracts or deposit agreements for digital materials in collection | 4 |
| 3.5.1.1 | Contracts must specify preservation rights | 2 |
| 3.5.1.2 | Specify aspects of acquisition, maintenance, access, withdrawal with all depository | 2 |
| 3.5.1.2 | Clarify when repository accepts preservation duties for a SIP | 2 |
| 3.5.1.4 | Policies that address liability and challenges to rights/ownership | 3 |
| 3.5.2 | Track,act on, and verify rights restrictions related to use of digital objects in repository | 3 |

3.40

2.75

2.86

3.67

2.67

3.00

key:
4 = fully compliant
3 = mostly compliant
2 = half compliant
1 = slightly compliant
0 = non-compliant

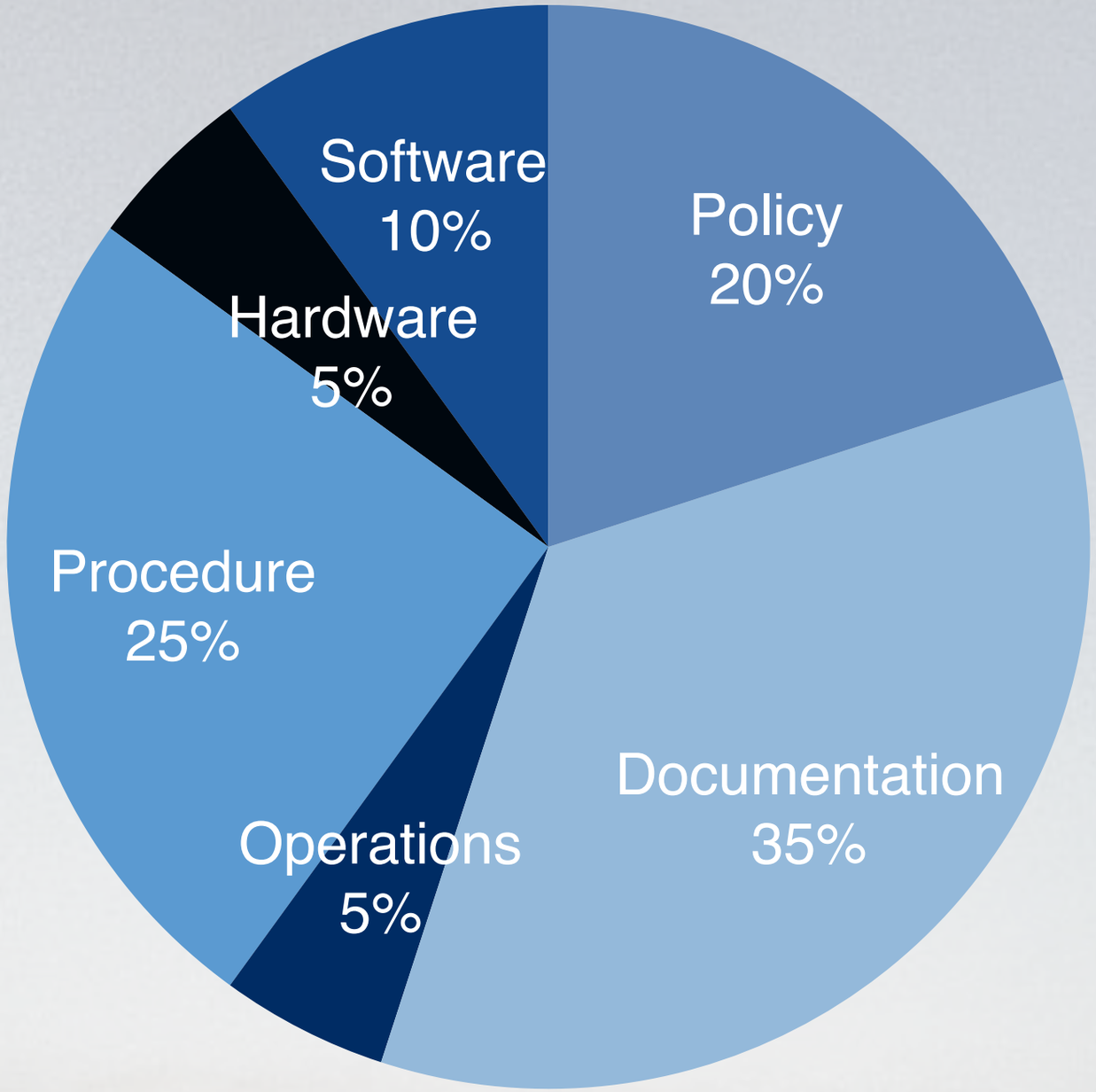
# Areas to Sustain

| ISO 16363 Section | # Metrics Scored 4 | # Metrics Scored |
|---|---|---|
| Organizational Infrastructure | 7 | 20 |
| Digital Object Management | 22 | 37 |
| Infrastructure and Security Risk Management | 19 | 21 |
| Totals | 48 | 78 |

# Areas to Improve

| ISO 16363 Section | # Metrics Scored 3 | # Metrics Scored 2 | # Metrics Scored 1 | # Metrics Scored 0 |
|---|---|---|---|---|
| Organizational Infrastructure | 5 | 4 | 2 | 2 |
| Digital Object Management | 10 | 5 | 0 | 0 |
| Infrastructure and Security Risk Management | 1 | 1 | 0 | 0 |
| Totals | 16 | 10 | 2 | 2 |

# Example Gaps: Short Term Priorities by Type



| ISO 16363 | | Score | TImeframe | Priority | Type |
|---|---|---|---|---|---|
| 3.1.1 | Mission Statement (preservation of, long term retention of, management of, and access to digital information) | 1 | Short | first | policy documentation |
| 3.1.2 | Preservation Strategic Plan | 0 | Short | first | policy documentation |
| 3.1.3 | Collection Policy | 2 | Short | first | policy documentation |
| 3.2.1.1 | Well-documented duties | 3 | Short | first | documentation operations |
| 3.2.1.2 | Appropriate levels of staff and skills | 3 | Short | first | operations |
| 3.3.1 | Defined designated community | 3 | Short | first | documentation |
| 3.3.5 | Define, collect, track information integrity measurements | 3 | Short | first | policy procedure documentation |
| 3.5.1 | Contracts or deposit agreements for digital materials in collection | 0 | Short | first | policy procedure documentation |
| 4.4.1.2 | Actively monitor the integrity of AIPs | 3 | Short | first | procedure documentation |
| 4.5.1 | Minimum information requirements to enable DC to discover/identify content | 3 | Short | first | documentation |
| 5.1.1.6.1 | Documented CM process identifies changes to ciritical processes above | 3 | Short | first | procedure documentation |
| 5.2.4 | Written disaster preparedness and recovery plans | 2 | Short | first | procedure documentation |
| 4.1.1 | Identify Content Information (CI) and Information Properties (IP) to be preserved | 2 | Short | second | policy procedure documentation |
| 4.2.1 | Must have clear definition of AIP or AIP classes, adequate for parsing/fit for long-term | 2 | Short | second | policy documentation |
| 4.2.5 | Access to tools and resources to provide authoritative Representation Information (RI) for all objects | 3 | Short | second | procedure documentation software |
| 3.3.2 | Preservation policies in place | 2 | Short | third | policy documentation |
| 3.3.2.1 | Mechanisms to review and update preservation policies | 2 | Short | third | procedure |
| 4.1.5 | Ingest process that verifes each SIP for completeness and correctness | 3 | Short | third | procedure documentation software |
| 4.2.2 | Description of how AIPs are constructed from SIPs | 3 | Short | third | documentation |
| 4.2.4.1 | Uniquely identify each AIP in repository | 2 | Short | third | policy procedure documentation |
| 4.3.1 | Documented preservation strategies relevant to holdings | 2 | Short | third | documentation |
| 4.3.3 | Mechanisms to change preservation plans as a result of monitoring activities | 3 | Short | third | procedure documentation |
| 4.4.2.1 | Procedures for all actions taken on AIPs | 3 | Short | third | documentation |
| 4.2.7 | Ensure CI of AIPs is understandable for DC at time of creation of AIPs | 3 | Medium | first | procedure documentation |
| 4.2.8 | Verify each AIP for completeness and correctness at point of creation | 2 | Medium | first | procedure documentation software |
| 3.3.6 | Commitment to regular schedule of self-assessment and certification | 3 | Medium | second | policy documentation |
| 4.4.2.2 | Demonstrate any actions taken on AIPs compliant with specs of those actions | 3 | Medium | second | procedure documentation |
| 3.1.2.1 | Succession Plan / Escrow | 1 | Medium | third | policy procedure documentation |

# Action Plan

## Year 1

### 1-6 Months

- Define and ratify the Organization's Mission Statement
- Document a formal Collection Policy
- Document the Organization's Designated Community
- Develop and document a Preservation Strategic Plan
- Increase staffing levels
- Specify and document preservation procedures: Integrity Monitoring
- Generate and sign agreements between the Organization and units
- Make explicit the Organization's responsibility regarding descriptive information
- Involve units in testing changes to system

### 7-12 Months

- Specify and document all preservation procedures: Disaster Recovery
- Complete definition of AIP specifications for all accepted AIP classes based on Mission Statement, Collection Policy, Designated Community, and Preservation Strategic Plan
- Define the Organization-wide AIP identifier schema that supports unique identification of all AIP classes
- Complete definition of required contents of SIPs based on updates to AIPs
- Document procedures for transformation of SIPs to AIPs for all classes of AIP

## Year 2

### 13-18 Months

- Formalize the Organization as a continuing system within the Parent Organization
- Specify and document all preservation procedures that will be used to manage all classes of AIP: AIP Quality Assurance
- Generate evidence to demonstrate compliance with defined preservation activities

### 19-24 Months

- Specify and document all preservation procedures that will be used to manage all classes of AIP: Format Audit Procedures
- Demonstrate commitment to regular schedule of repository assessment by planning for self-assessment or third-party audit

# Děkuji!

Bertram Lyons | @bertramlyons
AVPreserve | @avpreserve
PASIG 2016 | Prague