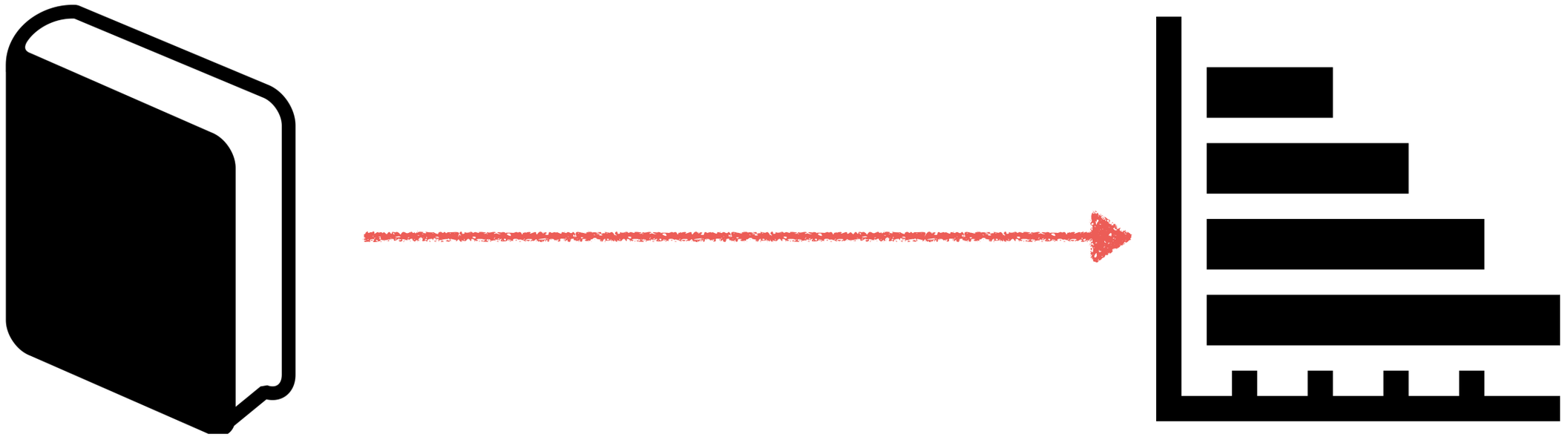


MAPPING STANDARDS FOR RICHER ASSESSMENTS

Bertram Lyons | AVPreserve

Digital Preservation 2014 | Washington, DC

NDSA Levels of Digital Preservation

Matrix (Version 1)

ISO 16363:2012

Audit & Certification of Trustworthy Digital Repositories

	Level 1 (Protect)	Level 2 (Know)	Level 3 (Monitor)	Level 4 (Repair)
Storage and Geographic Location	- Two complete copies that are not collocated - For data on heterogeneous media (optical discs, hard drives, etc.) get the content off the medium and into your storage system	- At least three complete copies - At least one copy in a different geographic location - Document your storage system(s) and storage media and what you need to use them	- At least one copy in a geographic location with a different disaster threat - Obsolescence monitoring process for your storage system(s) and media	- At least three copies in geographic locations with different disaster threats - Have a comprehensive plan in place that will keep files and metadata on currently accessible media or systems
File Fixity and Data Integrity	- Check file fixity on ingest if it has been provided with the content - Create fixity info if it wasn't provided with the content	- Check fixity on all ingests - Use write-blockers when working with original media - Virus-check high risk content	- Check fixity of content at fixed intervals - Maintain logs of fixity info; supply audit on demand - Ability to detect corrupt data - Virus-check all content	- Check fixity of all content in response to specific events or activities - Ability to replace/repair corrupted data - Ensure no one person has write access to all copies
Information Security	- Identify who has read, write, move and delete authorization to individual files - Restrict who has those authorizations to individual files	- Document access restrictions for content	- Maintain logs of who performed what actions on files, including deletions and preservation actions	- Perform audit of logs
Metadata	- Inventory of content and its storage location - Ensure backup and non-collocation of inventory	- Store administrative metadata - Store transformative metadata and log events	- Store standard technical and descriptive metadata	- Store standard preservation metadata
File Formats	- When you can give input into the creation of digital files encourage use of a limited set of known open formats and codecs	- Inventory of file formats in use	- Monitor file format obsolescence issues	- Perform format migrations, emulation and similar activities as needed

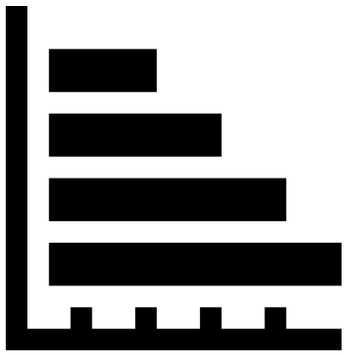
criteria per category

NDSA Levels of Digital Preservation Matrix

Storage and Geographic Location	9
File Fixity and Data Integrity	12
Information Security	5
Metadata	6
File Formats	4

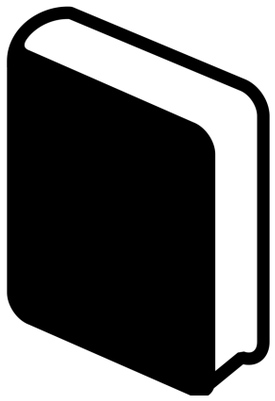
5 categories

36 total criteria



	Level 1 (Protect)	Level 2 (Know)	Level 3 (Monitor)	Level 4 (Repair)
Storage and Geographic Location	**- Two complete copies that are not collocated** **- For data on heterogeneous media (optical discs, hard drives, etc.) get the content off the medium and into your storage system**	**- At least three complete copies** **- At least one copy in a different geographic location** **- Document your storage system(s) and storage media and what you need to use them**	**- At least one copy in a geographic location with a different disaster threat** - Obsolescence monitoring process for your storage system(s) and media	- At least three copies in geographic locations with different disaster threats - Have a comprehensive plan in place that will keep files and metadata on currently accessible media or systems
File Fixity and Data Integrity	**- Check file fixity on ingest if it has been provided with the content** **- Create fixity info if it wasn't provided with the content**	**- Check fixity on all ingests** **- Use write-blockers when working with original media** **- Virus-check high risk content**	**- Check fixity of content at fixed intervals** **- Maintain logs of fixity info; supply audit on demand** **- Ability to detect corrupt data** **- Virus-check all content**	- Check fixity of all content in response to specific events or activities - Ability to replace/repair corrupted data - Ensure no one person has write access to all copies
Information Security	**- Identify who has read, write, move and delete authorization to individual files** **- Restrict who has those authorizations to individual files**	**- Document access restrictions for content**	- **Maintain logs** of who performed what actions on files, including deletions and preservation actions	- Perform audit of logs
Metadata	**- Inventory of content and its storage location** **- Ensure backup and non-collocation of inventory**	**- Store administrative metadata** **- Store transformative metadata and log events**	**- Store standard technical and descriptive metadata**	- **Store standard preservation metadata**
File Formats	**- When you can give input into the creation of digital files encourage use of a limited set of known open formats and codecs**	**- Inventory of file formats in use**	**- Monitor file format obsolescence issues**	- Perform format migrations, emulation and similar activities as needed

	Level 1	Level 2	Level 3	Level 4
Storage & Geographic Location				
File Fixity & Data Integrity				
Information Security				
Metadata				
File Formats				

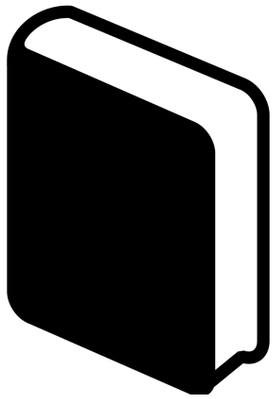


criteria per category

[ISO 16363 Audit & Certification of TDRs](#)	
Organizational Infrastructure	25
Digital Object Management	60
Information & Security Risk Mgmt.	24

109 total criteria

3 categories



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

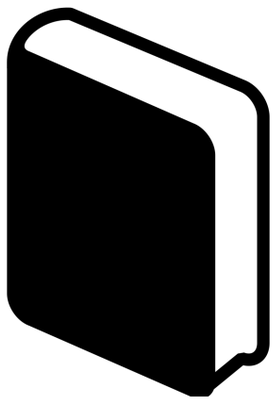
2.86

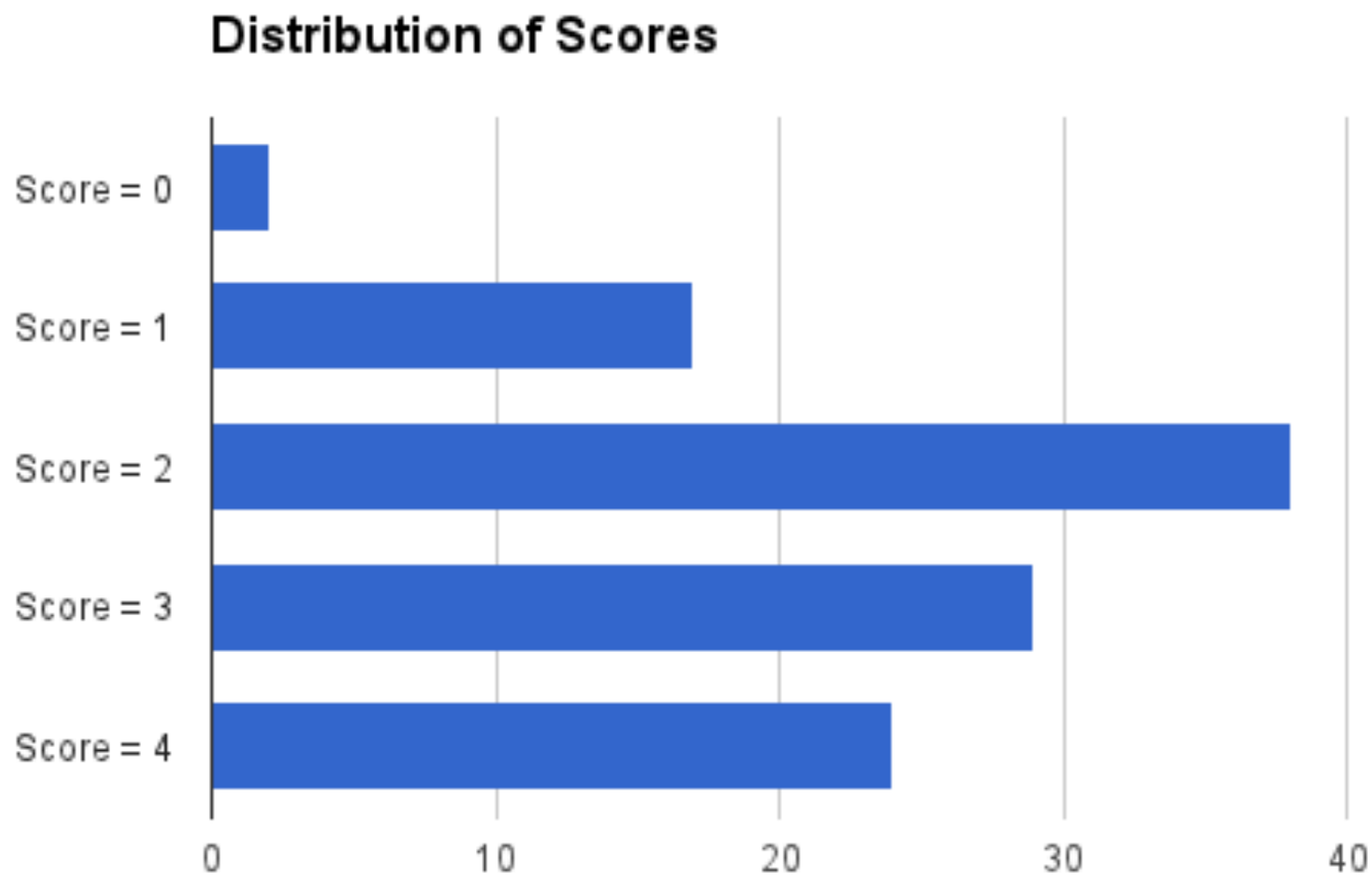
3.67

2.67

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

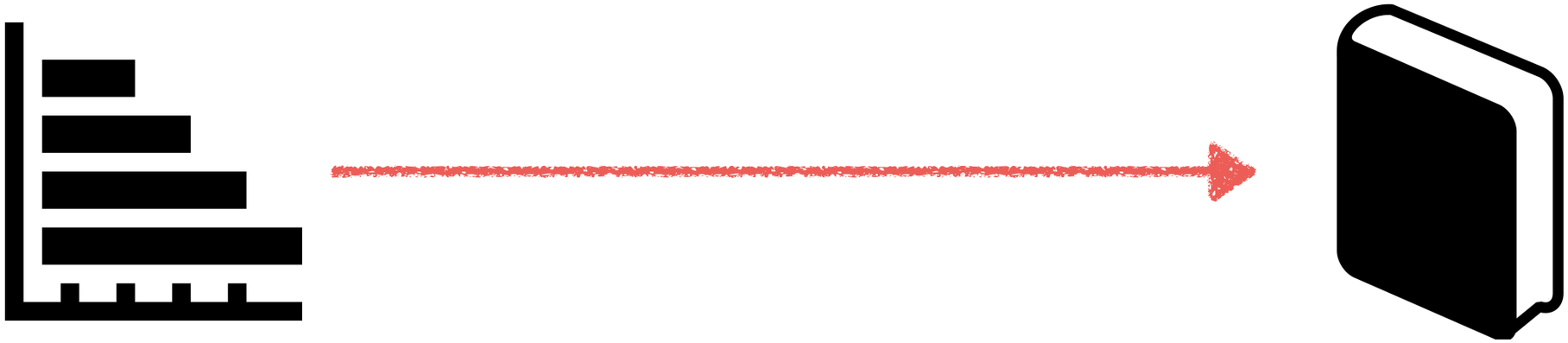
3.00





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

Total Average Score:
2.51

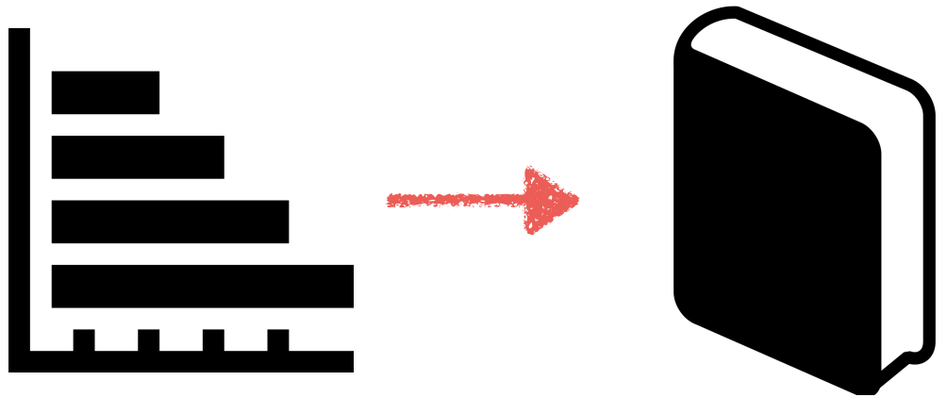


NDSA Levels of Digital Preservation

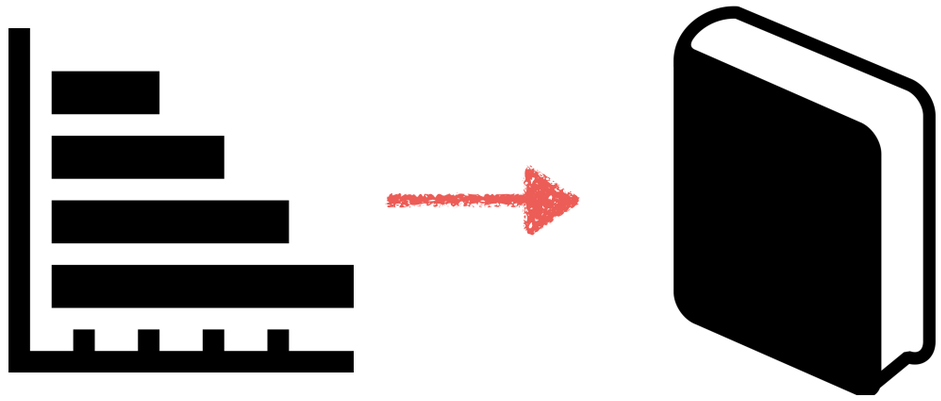
Matrix (Version 1)

ISO 16363:2012

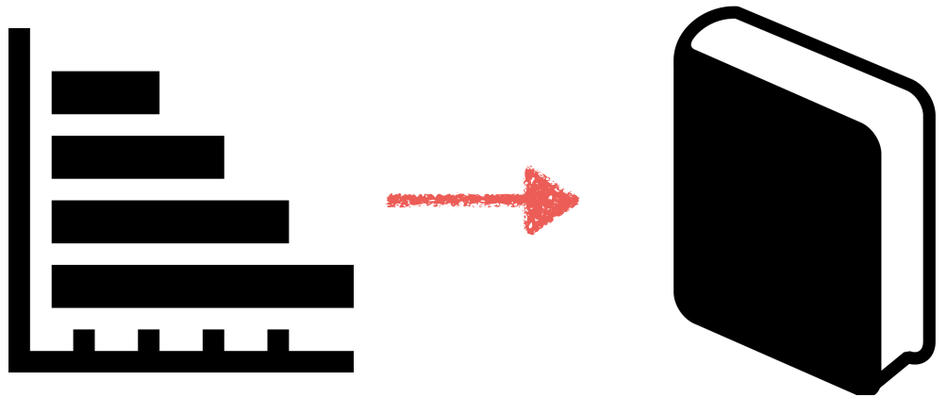
Audit & Certification of Trustworthy Digital Repositories



NDSA Levels of Digital Preservation - Categories	Quantity of related ISO 16363 Criterion
Storage and Geographic Location	34
File Fixity and Data Integrity	29
Information Security	22
Metadata	50
File Formats	32



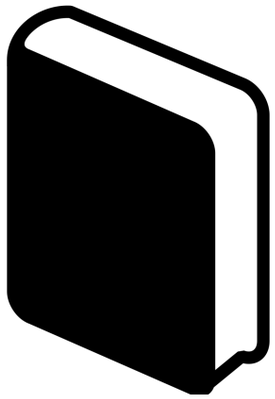
NDSA Levels of Digital Preservation - Categories	Quantity of related ISO 16363 Criterion	Quantity of NDSA LoDP Criterion
Storage and Geographic Location	34	9
File Fixity and Data Integrity	29	12
Information Security	22	5
Metadata	50	6
File Formats	32	4



Organizational Infrastructure

23 | not-mappable

NDSA Levels of Digital Preservation - Categories	Quantity of related ISO 16363 Criterion	Quantity of NDSA LoDP Criterion
Storage and Geographic Location	34	9
File Fixity and Data Integrity	29	12
Information Security	22	5
Metadata	50	6
File Formats	32	4



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

3.40

2.75

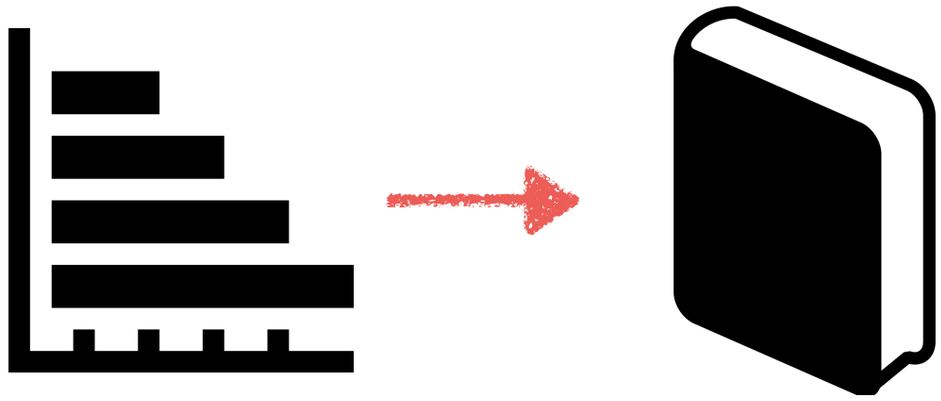
2.86

3.67

2.67

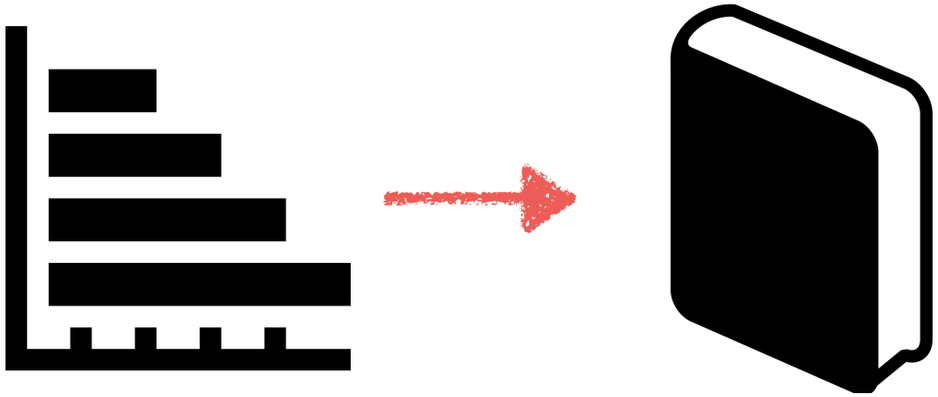
key:
4 = fully compliant
3 = mostly compliant
2 = half compliant
1 = slightly compliant
0 = non-compliant

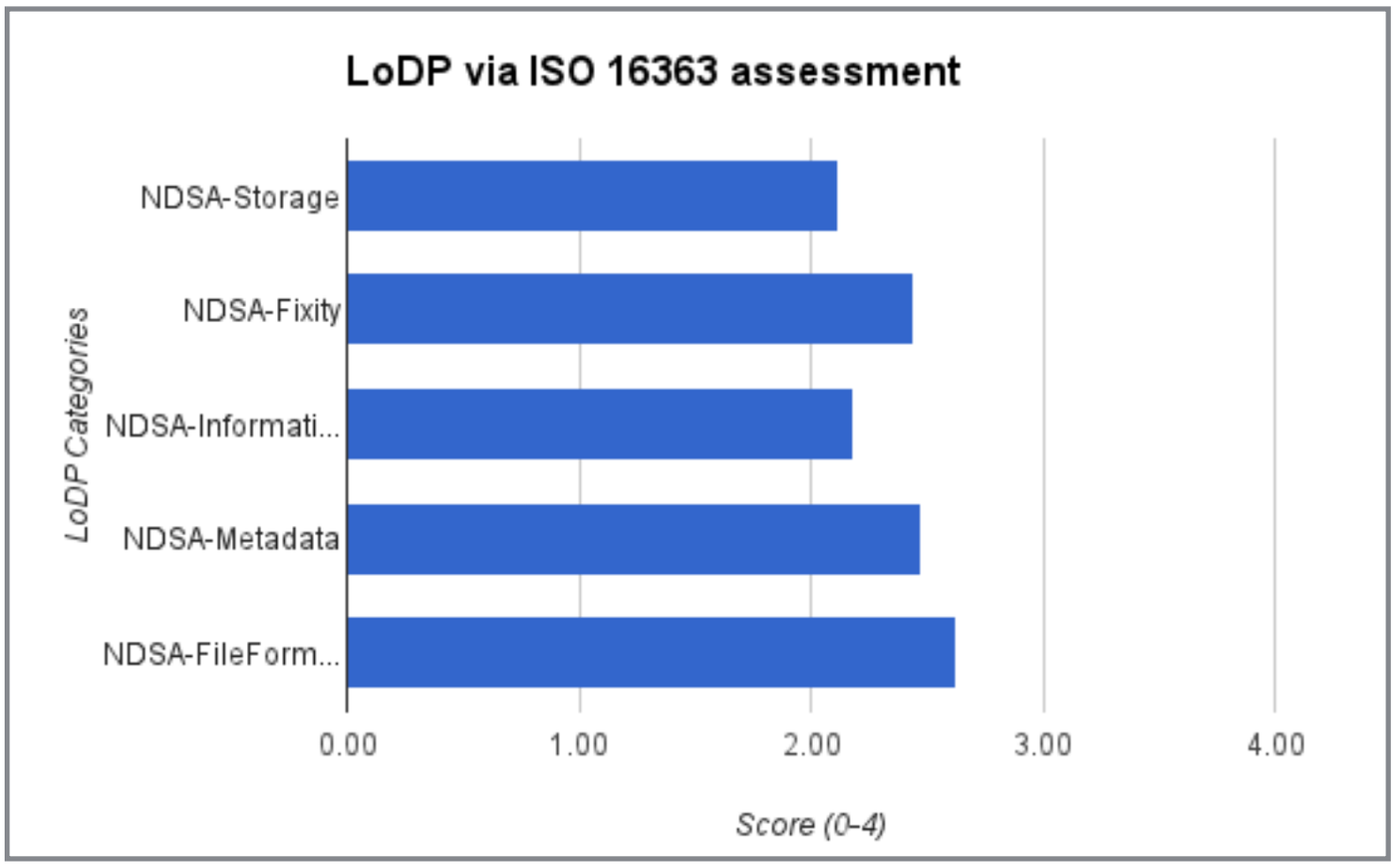
3.00

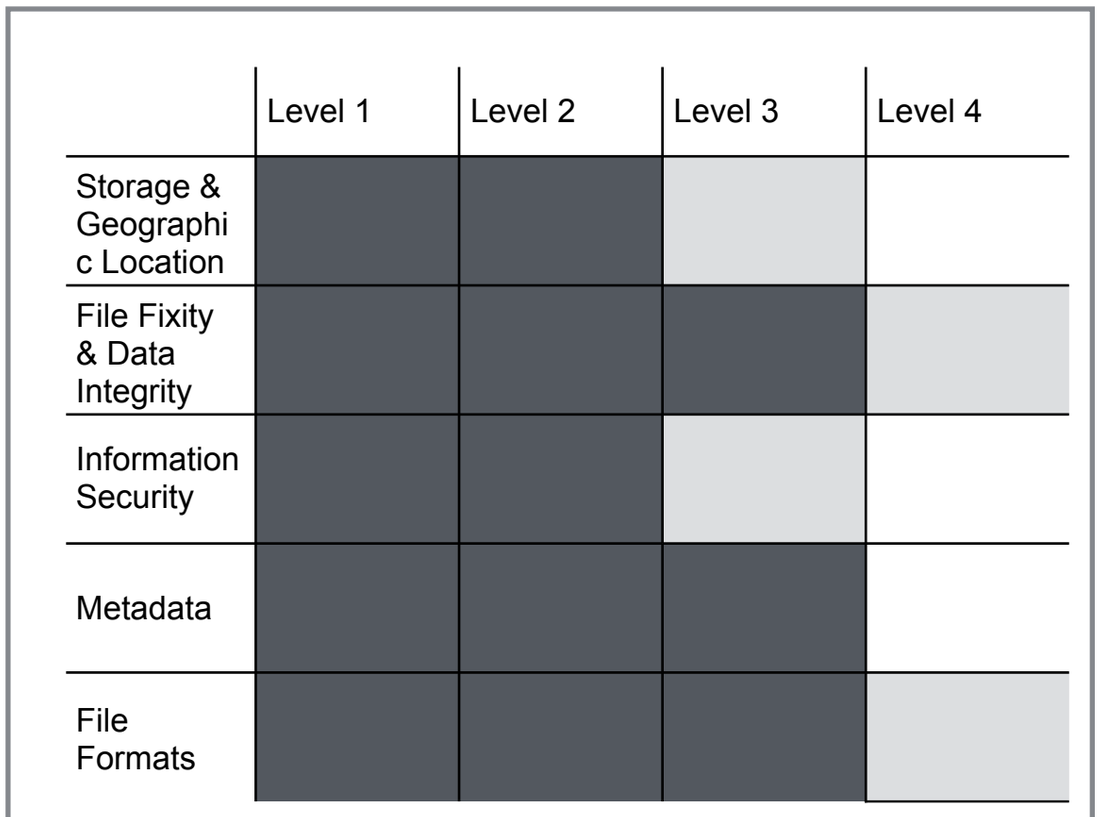


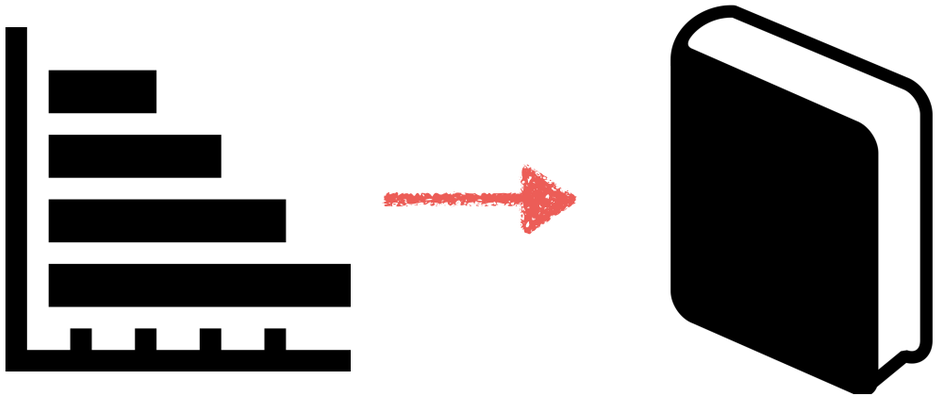
key:
4 = fully compliant
3 = mostly compliant
2 = half compliant
1 = slightly compliant
0 = non-compliant

NDSA Levels of Digital Preservation - Categories	Cumulative Score from ISO 16363 Assessment
Storage and Geographic Location	2.12
File Fixity and Data Integrity	2.45
Information Security	2.18
Metadata	2.48
File Formats	2.63




LoDP via ISO 16363 assessment
NDSA-Storage
NDSA-Fixity
NDSA-Informati...
NDSA-Metadata
NDSA-FileForm...
LoDP Categories
0.00
1.00
2.00
3.00
4.00
Score (0-4)


Level 1
Level 2
Level 3
Level 4
Storage & Geographic Location
File Fixity & Data Integrity
Information Security
Metadata
File Formats



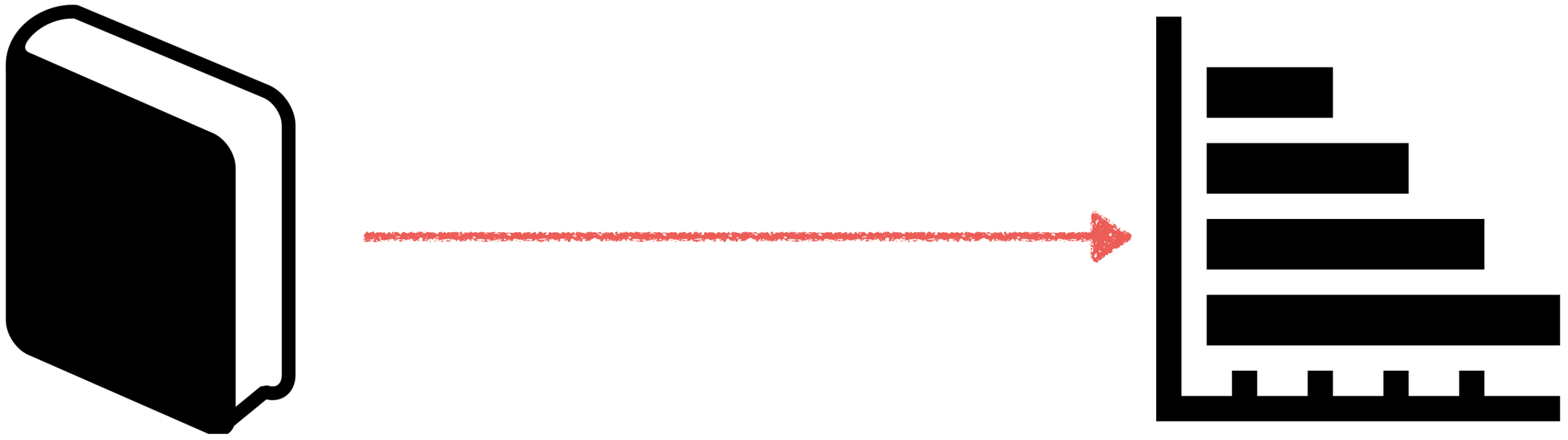
key:
4 = fully compliant
3 = mostly compliant
2 = half compliant
1 = slightly compliant
0 = non-compliant

NDSA Levels of Digital Preservation - Categories	Cumulative Score from ISO 16363 Assessment
Storage and Geographic Location	2.12
File Fixity and Data Integrity	2.45
Information Security	2.18
Metadata	2.48
File Formats	2.63

ISO 16363 via NDSA LoDP

Storage and Geographic Location

ISO 16363	Criterion Description	Score
4.1.6	Obtain sufficient control over DOs to preserve them (physical and legal)	3
4.2.4.2	System of linknig/resolution services in order to find uniquely identified object	2
4.2.5.4	Tools or methods to ensure that RI is presistently associate with relevant DOs	4
4.3.1	Documented preservation strategies relevant to holdings	3
4.3.2	Mechanisms for monitoring preservation environment	2
4.4.1	Specifications for how AIPs are stored down to the bit level	3
4.4.1.1	Preserve CI of AIPs	2
4.4.1.2	Actively monitor the integrity of AIPs	3
4.4.2	Maintain records of actions/admin processes relevant to storage/preservation of AIPs	2
4.4.2.1	Procedures for all actions taken on AIPs	2
4.6.1.1	Log and review all access management failures and anomalies	1
4.6.2	Policies and procedures enable dissemnination of digital objects traceable to originals	3
5.1.1	Identify and manage risks to preservation operations and goals with system	2
5.1.1.1	Employ technology watches or other monitoring notification system	3
5.1.1.1.1	Hardware technologies appropriate to services provided	4
5.1.1.1.2	Procedures to monitor/receive notifications when changes are needed	1
5.1.1.1.3	Procedures to evaluate when changes are needed to hardware	2
5.1.1.1.4	Procedures commitment and funding to replace hardware when needed	3
5.1.1.1.5	Software technologies appropriate to the services provides	4
5.1.1.1.6	Procedures to monitor/receive notifications when changes are needed	0
5.1.1.1.7	Procedures to evaluate when changes are needed to software	1
5.1.1.1.8	Procedures commitment and funding to replace software when needed	0
5.1.1.2	Adequate hardware/software support for backup functions	1
5.1.1.4	Process to record/react to new security updates based on risk-benefit assessment	2
5.1.1.5	Processes for storage media and/or hardware change	4
5.1.1.6	Identify processes that affect ability to comply with mandatory responsibilities	1
5.1.1.6.1	Documented change management process identifies changes to critical processes	2
5.1.1.6.2	Test and evaluate effect of changes to critical processes	1
5.1.1.7	Manage the number and location of copies of all DOs	1
5.1.1.7.1	Mechanisms to ensure any/multiple copies of digital objects are synchronized	0
5.1.2.1	Systematic analysis of security risk factors with data, systems, personnel, plans	1
5.1.2.2	Controls to address each defined security risk	0
5.1.2.3	Delineated roles for staff related to implementing changes within system	1
5.1.2.4	Written disaster preparedness and recovery plans	2



MAPPINGS AVAILABLE FOR COMMENT:

http://bit.ly/1qyfOtP

Bertram Lyons | AVPreserve

Digital Preservation 2014 | Washington, DC