NATIONAL DIGITAL STEWARDSHIP ALLIANCE

Putting the NDSA Levels of Digital Preservation to Work for your Organization

Digital Preservation 2013
Washington, DC

Jefferson Bailey, Metropolitan New York Library Council (METRO)
Andrea Goethals, Harvard Library
Trevor Owens, Library of Congress
Megan Phillips, National Archives and Records Administration

First off… show of hands: How many people have read the Levels?

Second… Has anybody here tried to use them for your organization?

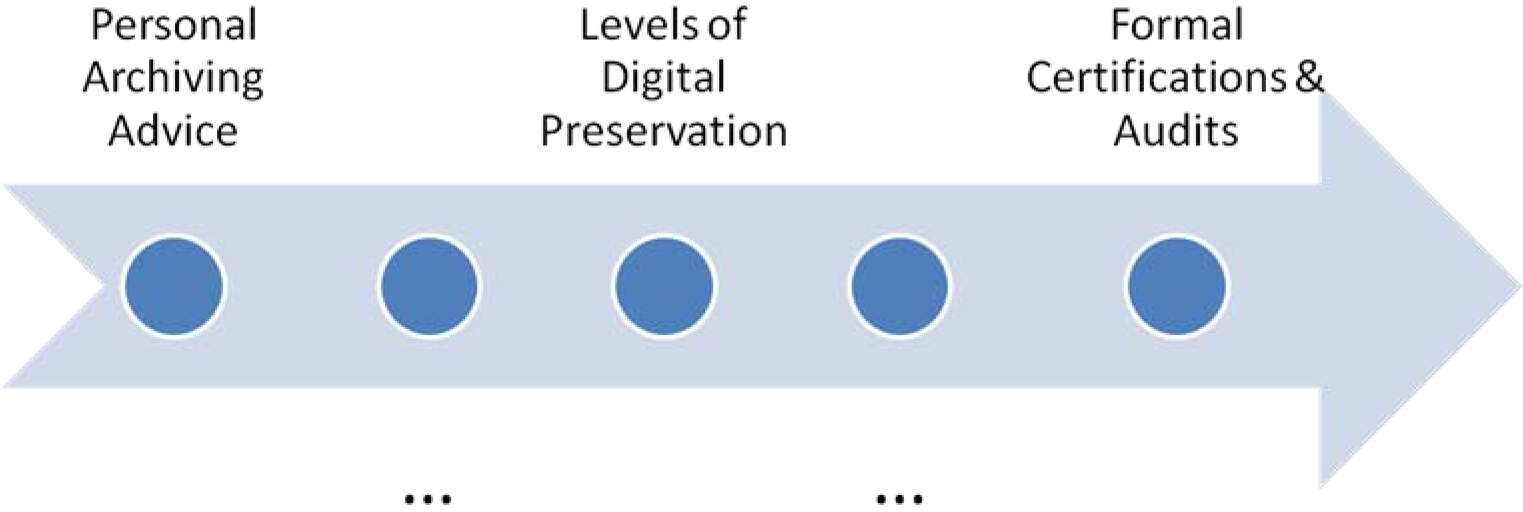
Overview

- Version One of the Levels, Review
- Use Examples
- Discussion of uses

Common Need

- Simple, practical, documented levels of preservation services reflecting best practices, **broadly useful**
  - For those just starting out & those with mature programs
  - Independent of formats, storage systems
  - Useful to educators & implementers

Niche



Personal Archiving Advice

…

Levels of Digital Preservation

…

Formal Certifications & Audits

NATIONAL DIGITAL STEWARDSHIP ALLIANCE

Levels of Digital Preservation, v1

	Level 1 ↓	Level 2 ↓	Level 3 ↓	Level 4 ↓
Category 1 →				
Category 2 →				
Category 3 →				
Category 4 →				
Category 5 →				

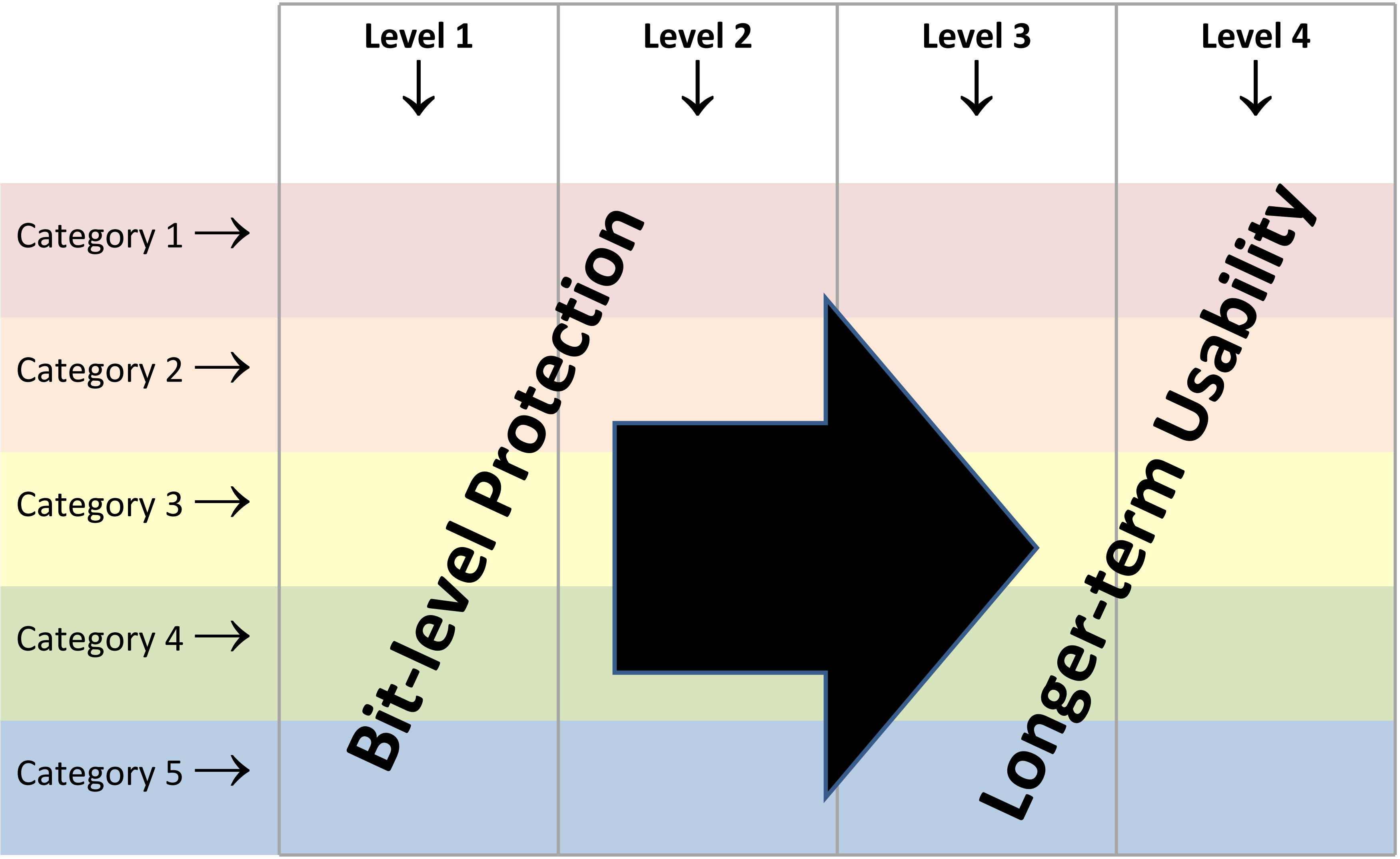
NATIONAL DIGITAL STEWARDSHIP ALLIANCE

Levels of Digital Preservation, v1

	Level 1 ↓	**Level 2** ↓	**Level 3** ↓	**Level 4** ↓
Category 1 →	Level 1 Actions for Category 1	Level 2 Actions for Category 1	…	…
Category 2 →	Level 1 Actions for Category 2	Level 2 Actions for Category 2	…	…
Category 3 →	…	…	…	…
Category 4 →	…	…	…	…
Category 5 →	…	…	…	…

NATIONAL DIGITAL STEWARDSHIP ALLIANCE

Levels of Digital Preservation, v1



Level 1

Level 2

Level 3

Level 4

Category 1 →

Category 2 →

Category 3 →

Category 4 →

Category 5 →

Bit-level Protection

Longer-term Usability

NATIONAL DIGITAL STEWARDSHIP ALLIANCE

Levels of Digital Preservation, v1

	Level 1 (Protect your data)	Level 2 (Know your data)	Level 3 (Monitor your data)	Level 4 (Repair your data)
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

Storage and Geographic Location

Level 1 Protect your data	Level 2 Know your data	Level 3 Monitor your data	Level 4 Repair your data
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 systems(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 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

Level 1 **Protect your data**	**Level 2** **Know your data**	**Level 3** **Monitor your data**	**Level 4** **Repair your data**
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

Level 1 Protect your data	Level 2 Know your data	Level 3 Monitor your data	Level 4 Repair your data
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

Level 1 Protect your data	Level 2 Know your data	Level 3 Monitor your data	Level 4 Repair your data
Inventory of content and its storage location Ensure backup and non-collocation of inventory	Store administrative metadata Store transformative metadata and log events	Store standards technical and descriptive metadata	Store standard preservation metadata

File Formats

Level 1 Protect your data	Level 2 Know your data	Level 3 Monitor your data	Level 4 Repair your data
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

Usage Contexts

- **Inform Local Guidelines Development:** Educate and develop guidelines for content creators and contributors **USGS**
- **Self Assessments** – how do we compare with best practices? What should we improve next? Where do we excel? How will we improve after project X? How have we improved over time? **Harvard & ARTstor**
- **Developing requirements** for third-party preservation service providers

Self-assessment example

🟩	= satisfied with implementation	🟨	= implemented but could be improved
▨	= will be satisfied with implementation after current enhancement project	🟥	= not implemented

	Level One	Level Two	Level Three	Level Four
Storage & Geographic Location	🟩	🟨	🟥	🟥
File Fixity and Data Integrity	🟩	▨	▨	🟩
Information Security	🟨	🟨	▨	▨
Metadata	▨	▨	▨	▨
File Formats	🟩	🟩	🟨	🟥