



# Digital Preservation 101: First Steps (and Next Steps)

## Part 2

Lauren Goodley, MSIS, CA, DAS



# DPOE

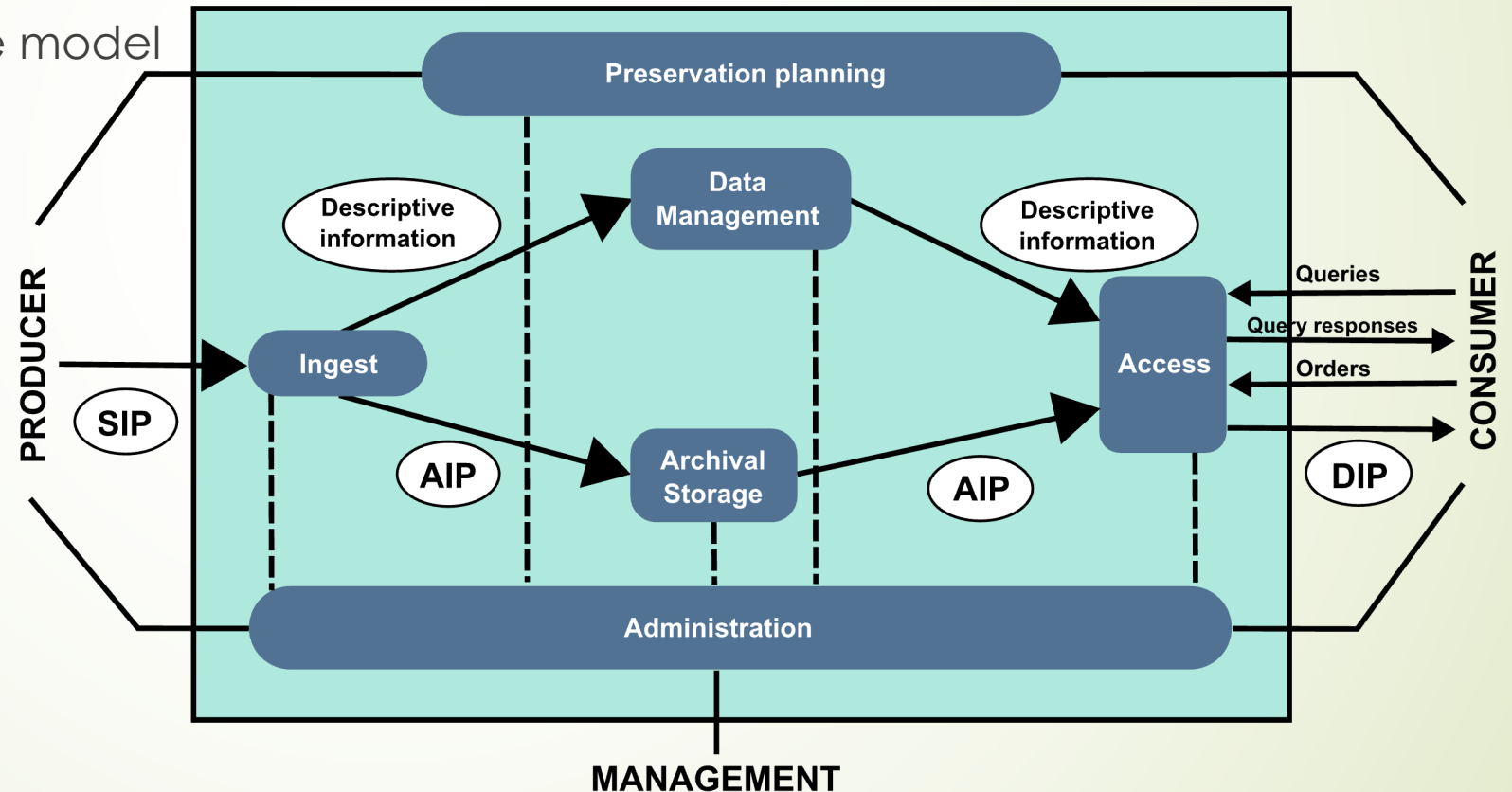
## Digital Preservation Outreach and Education

- **Identify** – what digital content do you have?
- **Select**—what portion of that content is your responsibility to preserve?
- **Store**—how can you store digital content for the long term?
- **Protect**—what steps can you take to protect this digital content?
- **Provide**—how can digital content be made available?
- **Manage**—what provisions can you make for long term management?

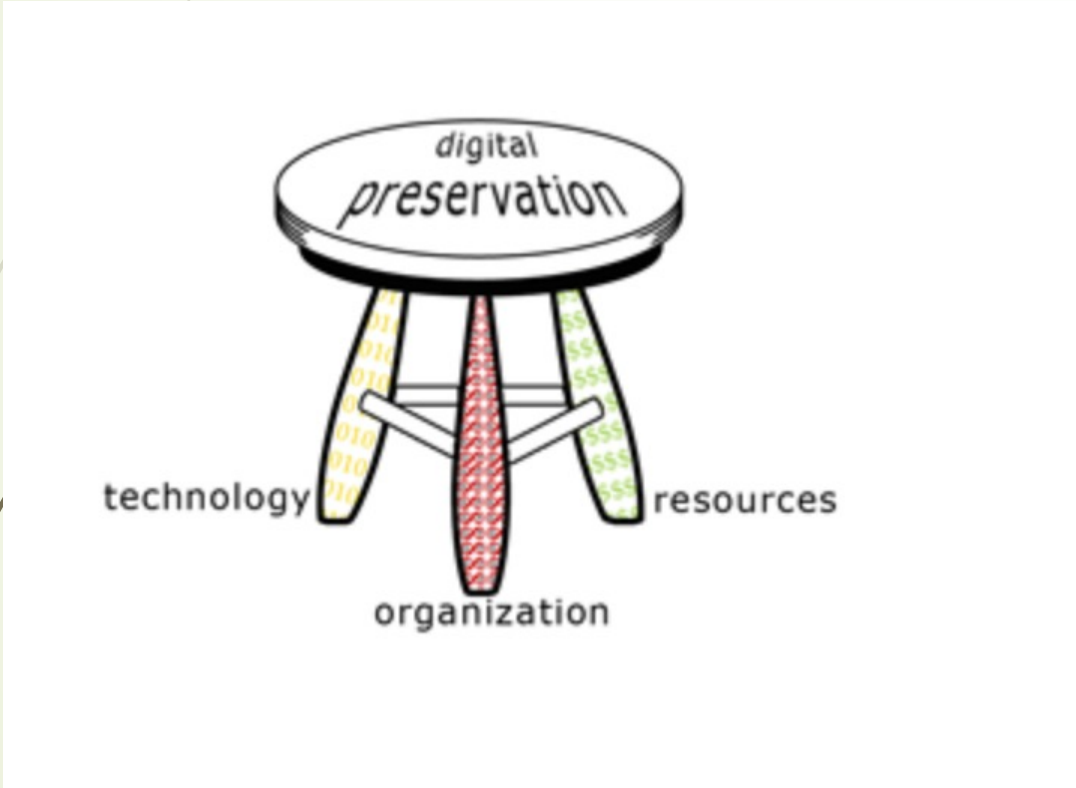
# OAIS

## Open Archival Information System

- ISO Standard
- Reference model



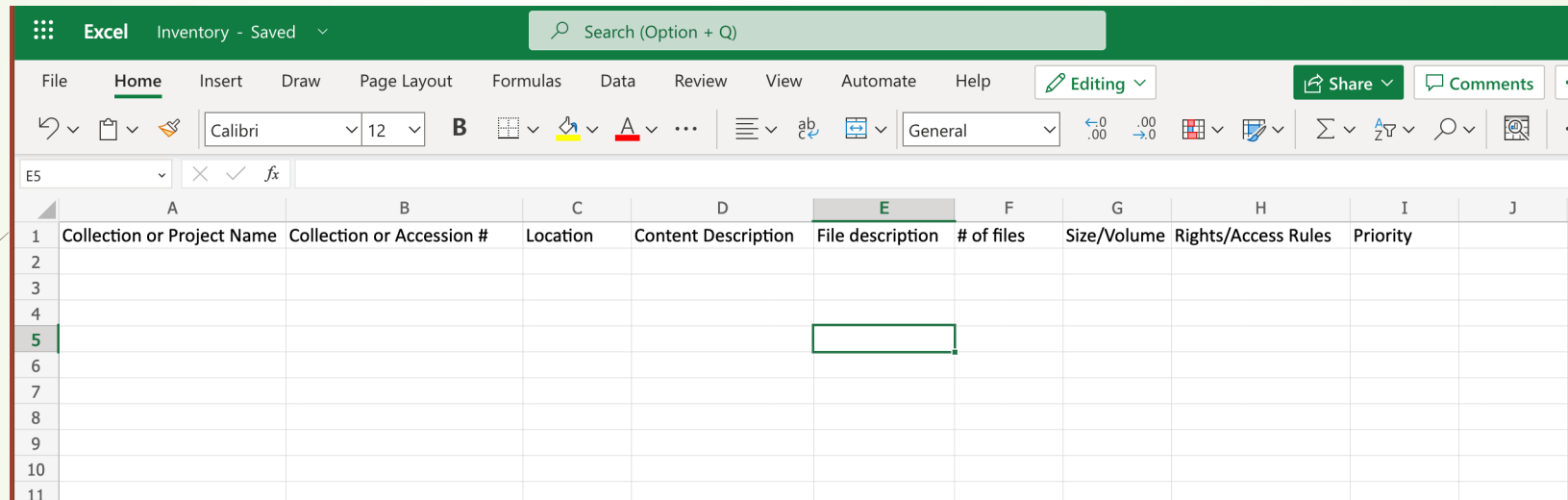
# Digital Preservation Management Workshop



- **Organizational Infrastructure**  
includes the policies, procedures, practices, people
- **Technological Infrastructure**  
consists of the requisite equipment, software, hardware, a secure environment, and skills
- **Resources Framework**  
addresses the requisite startup, ongoing, and contingency funding

# Review Part 1

## Identify and Select



The screenshot shows the Microsoft Excel interface with a spreadsheet titled "Inventory - Saved". The ribbon is set to "Home". The spreadsheet has the following columns: A (Collection or Project Name), B (Collection or Accession #), C (Location), D (Content Description), E (File description), F (# of files), G (Size/Volume), H (Rights/Access Rules), and I (Priority). Row 5 is highlighted, and a green box is drawn around cell E5.

	A	B	C	D	E	F	G	H	I	J
1	Collection or Project Name	Collection or Accession #	Location	Content Description	File description	# of files	Size/Volume	Rights/Access Rules	Priority	
2										
3										
4										
5										
6										
7										
8										
9										
10										
11										

- Identifying metadata
- Descriptive metadata
- Administrative metadata
- Preservation metadata
- Files themselves
- Priorities



# Store & Protect- Considerations

## LOCKSS

- 3 copies, in disparate geographical, administrative, and technological locations
- Spinning disks / server
- Partnerships-consortia
- Permissions (locked doors)
- AIP- METS "wrapper" / directory folder



# Store Protect - AIP

## What are you storing and Protecting?

### Files

- Filetypes – open or standardized
- Preservation files or Use files

### Metadata

PDI – Preservation  
Description Information

- **Reference**  
(Identification)
- **Provenance**  
(Collection/project,  
repository/institution)
- **Context** (Description)
- **Fixity** (Checksum,  
health checks)
- **Access & Rights**





# Provide

## What are you providing access to?


### Files and metadata

- File types
  - Use/Access files
- Metadata
  - Use/Access descriptive metadata
  - Rights/permissions
- Mukurtu, CONTENTdm





# Manage Digital Preservation Policy

- 
1. Purpose
  2. Objectives
  3. Mandate
  4. Scope
  5. Challenges/Incentives
  6. Principles



# Manage Digital Preservation Policy (cont)

7. Roles and Responsibilities

8. Cooperation/Collaboration

9. Selection and Acquisition Criteria

10. Access/Use Criteria

11. Definitions

12. References



# Manage NDSA Levels of Preservation

Functional Area	Level			
	Level 1 (Know your content)	Level 2 (Protect your content)	Level 3 (Monitor your content)	Level 4 (Sustain your content)
<b>Storage</b>	Have two complete copies in separate locations  Document all storage media where content is stored  Put content into stable storage	Have three complete copies with at least one copy in a separate geographic location  Document storage and storage media indicating the resources and dependencies they require to function	Have at least one copy in a geographic location with a different disaster threat than the other copies  Have at least one copy on a different storage media type  Track the obsolescence of storage and media	Have at least three copies in geographic locations, each with a different disaster threat  Maximize storage diversification to avoid single points of failure  Have a plan and execute actions to address obsolescence of storage hardware, software, and media
<b>Integrity</b>	Verify integrity information if it has been provided with the content  Generate integrity information if not provided with the content  Virus check all content; isolate content for quarantine as needed	Verify integrity information when moving or copying content  Use write-blockers when working with original media  Back up integrity information and store copy in a separate location from the content	Verify integrity information of content at fixed intervals  Document integrity information verification processes and outcomes  Perform audit of integrity information on demand	Verify integrity information in response to specific events or activities  Replace or repair corrupted content as necessary
<b>Control</b>	Determine the human and software agents that should be authorized to read, write, move, and delete content	Document the human and software agents authorized to read, write, move, and delete content and apply these	Maintain logs and identify the human and software agents that performed actions on content	Perform periodic review of actions/access logs
<b>Metadata</b>	Create inventory of content, also documenting current storage locations  Backup inventory and store at least one copy separately from content	Store enough metadata to know what the content is (this might include some combination of administrative, technical, descriptive, preservation, and structural)	Determine what metadata standards to apply  Find and fill gaps in your metadata to meet those standards	Record preservation actions associated with content and when those actions occur  Implement metadata standards chosen
<b>Content</b>	Document file formats and other essential content characteristics including how and when these were identified	Verify file formats and other essential content characteristics  Build relationships with content creators to encourage sustainable file choices	Monitor for obsolescence, and changes in technologies on which content is dependent	Perform migrations, normalizations, emulation, and similar activities that ensure content can be accessed

# Manage - Digital Readiness Levels- Recollection Wisconsin

## Digital Readiness Levels

The Digital Readiness Levels are a structured roadmap for public history organizations to plan and sustainably grow their digital initiatives in order to improve access to collections.



Focus Area	Bronze	Silver	Gold
Plan and Prioritize	Set goals for digital work that fit the organization's mission and policies. Adopt a digital mission statement or revise existing mission statement to include digital work.	Identify and prioritize potential digital projects. Make a digital project plan that includes roles, activities, required resources, and partners.	Adopt a digital collection development policy or revise existing policy to include digitized and born digital content.
Obtain Permissions	Create and use permission forms and donor agreements that include specific language for the use of digitized and born-digital content or modify existing forms.	Evaluate copyright status of content. Identify items with access restrictions or concerns, including privacy, ethical, or cultural considerations.	Assign standardized rights statements or Creative Commons licenses for collection items. Adopt a takedown policy and, if applicable, a statement on harmful content.
Digitize	Determine standards and procedures to be used to digitize physical materials or process born-digital content.	Using identified standards, undertake digitization or born-digital processing work either in-house or with an appropriate vendor or partner.	Use a quality control checklist to review content and confirm it meets identified standards.
Describe	Adopt a consistent naming convention for digital files. Determine standards to be used to describe digital content.	Using identified standards, create basic descriptive metadata for items.	Develop a data dictionary and use controlled vocabularies to standardize metadata.
Share	Review goals and options for providing access to content. Choose an access platform or system that meets identified needs.	Make items and associated descriptive information available for discovery and repurposing.	Implement techniques to support accessibility of online content, including alt text, transcripts, and other best practices.
Store and Maintain	Create and maintain a collection-level inventory of digital content.	Store at least two, preferably three, copies of each primary file and related metadata, with one copy stored off-site. Check and refresh storage media on a regular schedule.	Plan for future storage needs. Use software tools to check file integrity.
Evaluate	Identify primary users and ways to engage them with digital content.	Collect data and stories about how digital content is used.	Use collected data and stories to inform future collection development, outreach, and programming. Share knowledge with other practitioners to build community around digital work.

Revised June 2022





# Sources

- DPOE  
Digital Preservation Outreach and Education, Library of Congress  
Workshops  
<https://web.archive.org/web/20111128110839/http://www.digitalpreservation.gov/education/index.html#instructor>
- OAIS - Open Archival Information System, ISO standard  
<https://public.ccsds.org/Pubs/650x0m2.pdf>
- Digital Preservation Management Workshop (3-legged stool)  
<https://web.archive.org/web/20220121044830/http://www.dpworkshop.org:80/dpm-eng/conclusion.html>

Lauren Goodley  
lgoodley@txstate.edu

# Resources on Dropbox, <https://bit.ly/3f8mwHs>



- [This presentation](#) (Part 1 and 2, ppt and pdf)
  - Inventory document (excel and pdf)
  - My comments/transcript (pdf)
- OAIS Reference Model (pdf, model on page 44)
- [Digital Preservation Management Workshop](#) (3 legged stool)
  - Action Plan parts 1, 2, 3 (pdf)
  - Dig Pres Policy example (word doc)
- 2 charts
  - [NDSA Levels of Preservation](#) (pdf)
  - Recollection Wisconsin Digital Readiness Levels and [Toolkit](#) (pdf, chart on page 12)