ACADEMIC
PRESERVATION TRUST

Bradley J. Daigle, University of Virginia

Scott Turnbull, University of Virginia

DLF Forum 2014
29 October 2014

ACADEMIC PRESERVATION TRUST

Columbia University
Indiana University
North Carolina State University
Johns Hopkins University
Penn State University
Syracuse University
U of Chicago
U of Cincinnati
U of Connecticut
U of Maryland
U of Miami
U of Michigan
U of North Carolina
U of Notre Dame
U of Virginia
Virginia Tech

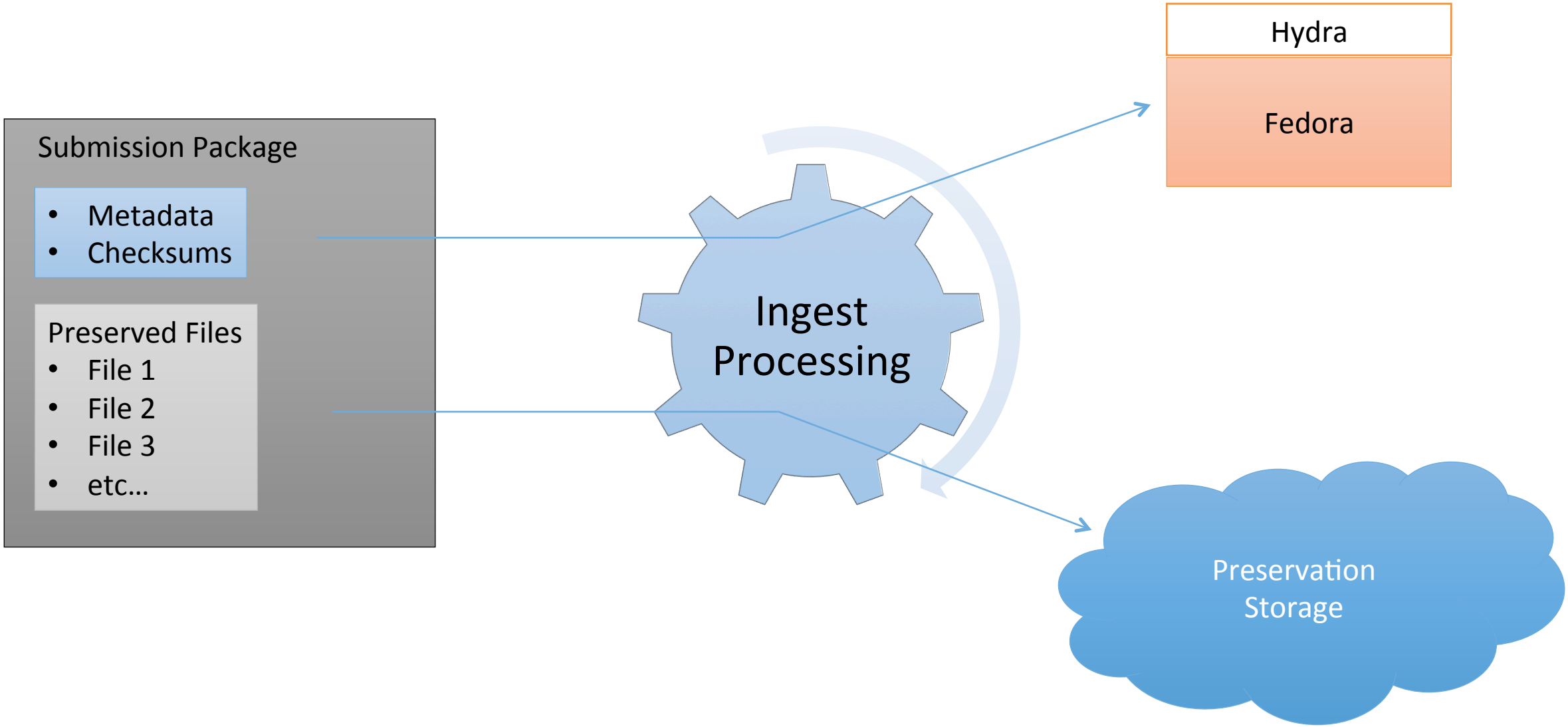
ACADEMIC
PRESERVATION TRUST

Committed to the creation and management of a sustainable environment for digital preservation

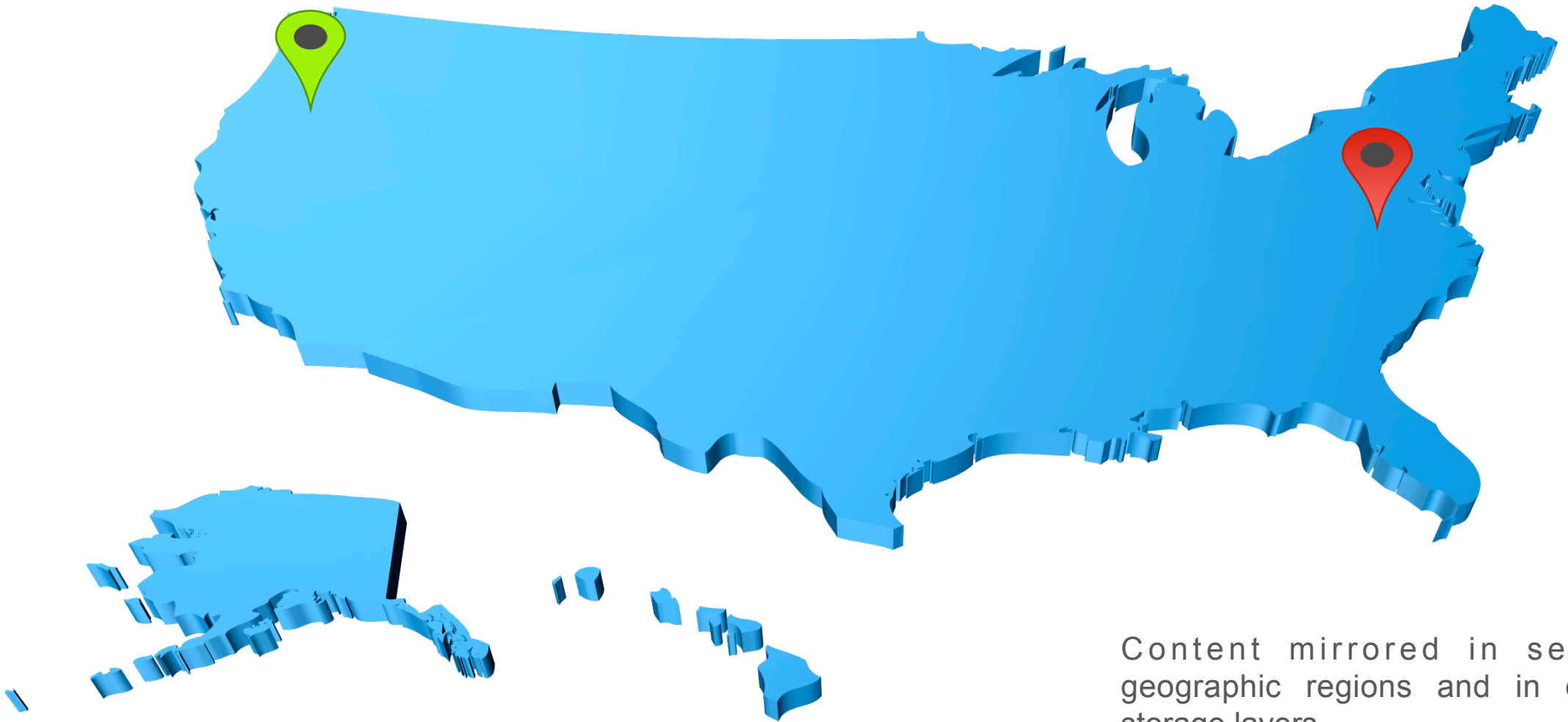
Aggregation Repository

Replicating Node for DPN

Suite of Preservation Services


Hydra
Fedora
Submission Package
• Metadata
• Checksums
Preserved Files
• File 1
• File 2
• File 3
• etc…
Ingest Processing
Preservation Storage

Geographic Content Distribution



Content mirrored in separate geographic regions and in different storage layers

Observations So Far

Challenges

- Remaining Agnostic
- Parallel submission pipelines
- Scaling of processing content
- Complexity of dealing with concurrent asyncronous and high latency processes

Advantages

- Aggregating content allows discovery or discussion of common practices
- Resilience of distributed systems
- Components allow for flexible growth

UNIVERSITY OF MIAMI

Preparing for APTrust at the University of Miami

Laura Capell
October 27, 2014

How We Plan to Use APTrust

1. Born digital content in library collections
   - Where the digital file is all we have
   - Disk images of physical media

2. Materials digitized from library collections
   - Analog audio & video
   - Paper-based resources
   - Photographic resources

3. Future uses
   - Research data
   - University-generated resources

The Library's Digital Environment

1. CONTENTdm for access to digital collections

2. Digital Commons for institutional repository

3. File server to store digital masters
   - Administered by Campus IT
   - 50 TB and growing
   - Weekly checksums
   - 6 month tape backup
   - Not a preservation repository

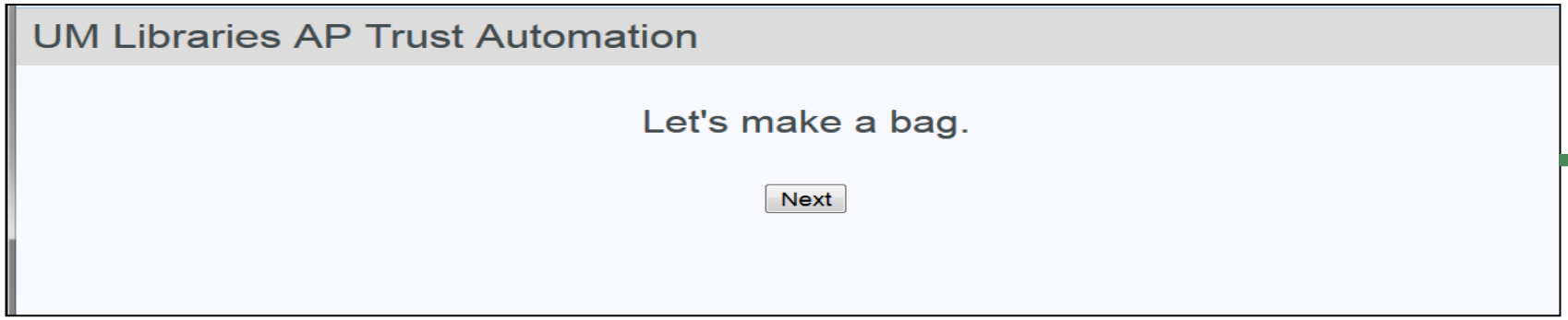
Preparing for APTrust

1. Examine digital content for cleanup & identification

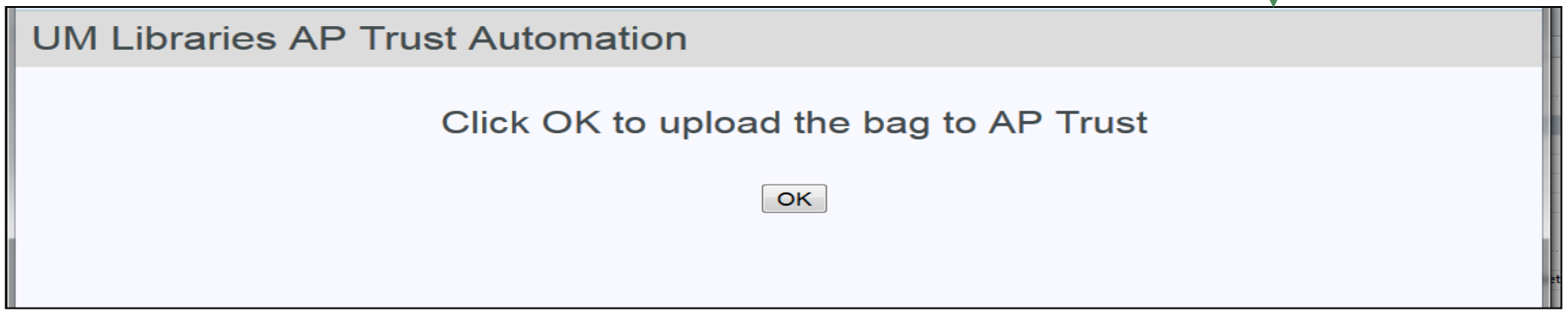
2. Setting priorities
   - Born digital content
   - Scanned content where original is high-risk
   - Cost to reproduce or recreate content
   - Research value
   - Intellectual property rights
   - Uniqueness
   - Ready for ingest

Web Interface for Bagging

Step 1…



Final step

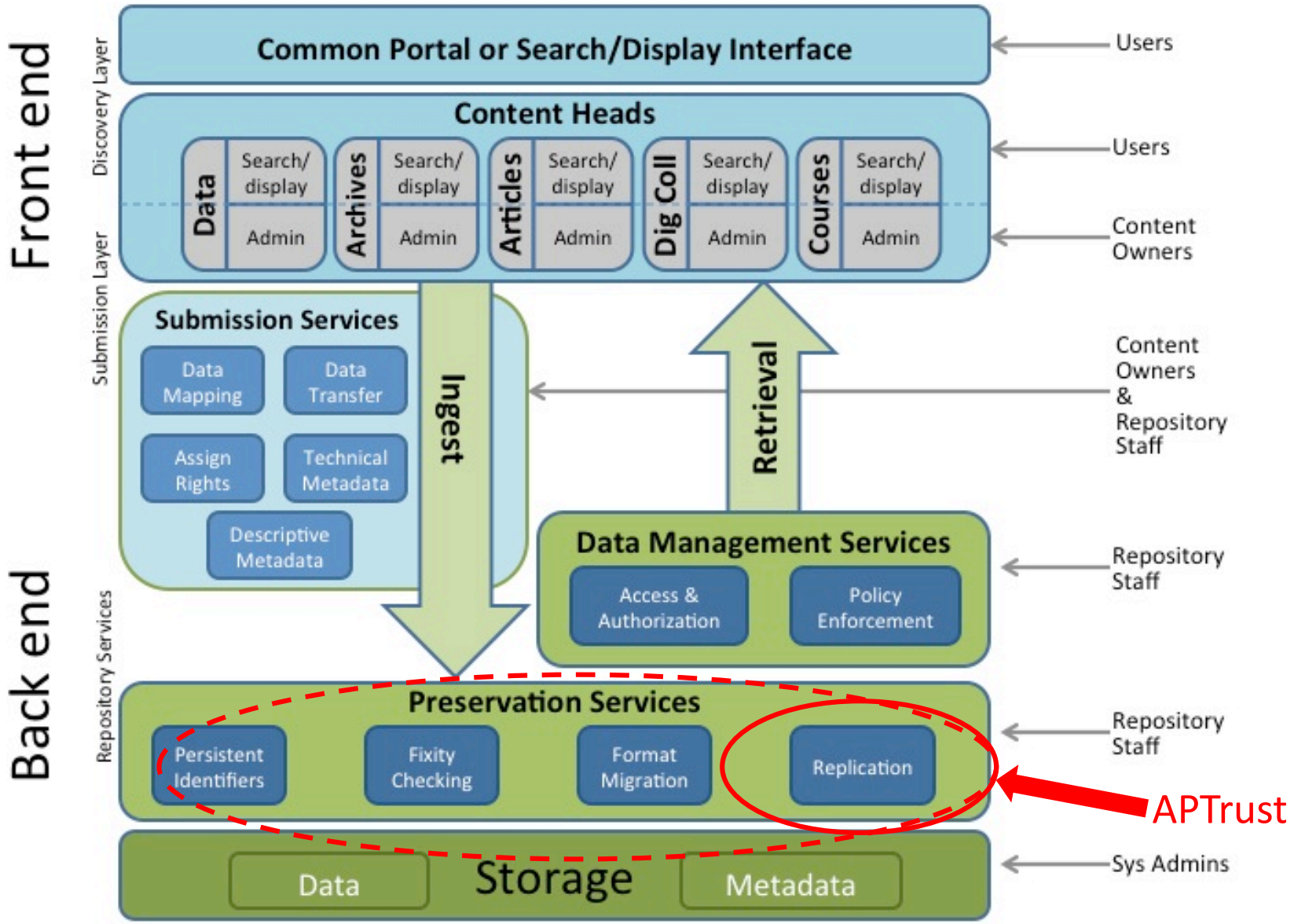


UNIVERSITY
OF MIAMI

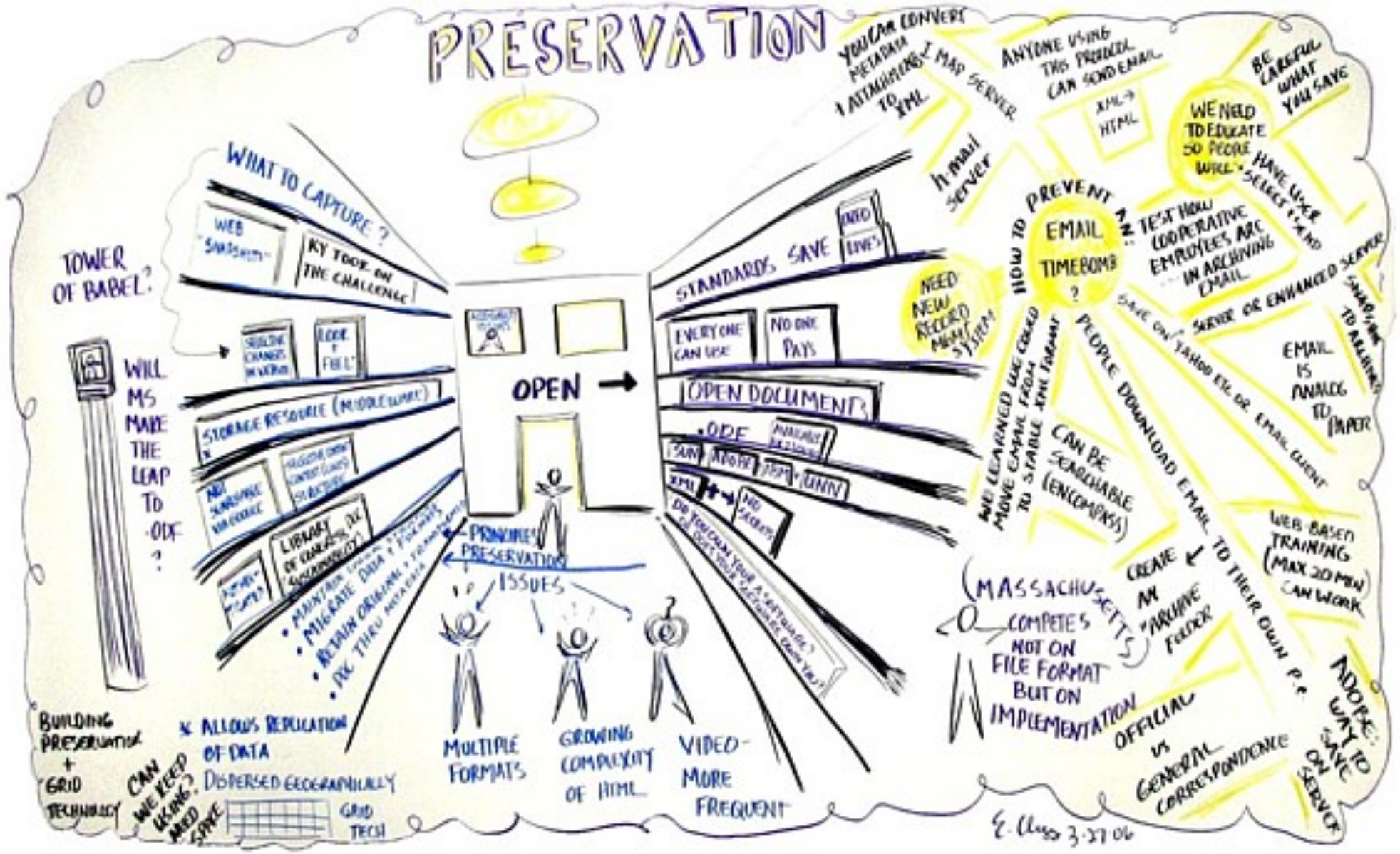
Nathan Tallman – University of Cincinnati

Elisabeth Long – University of Chicago

UChicago Digital Repository Components

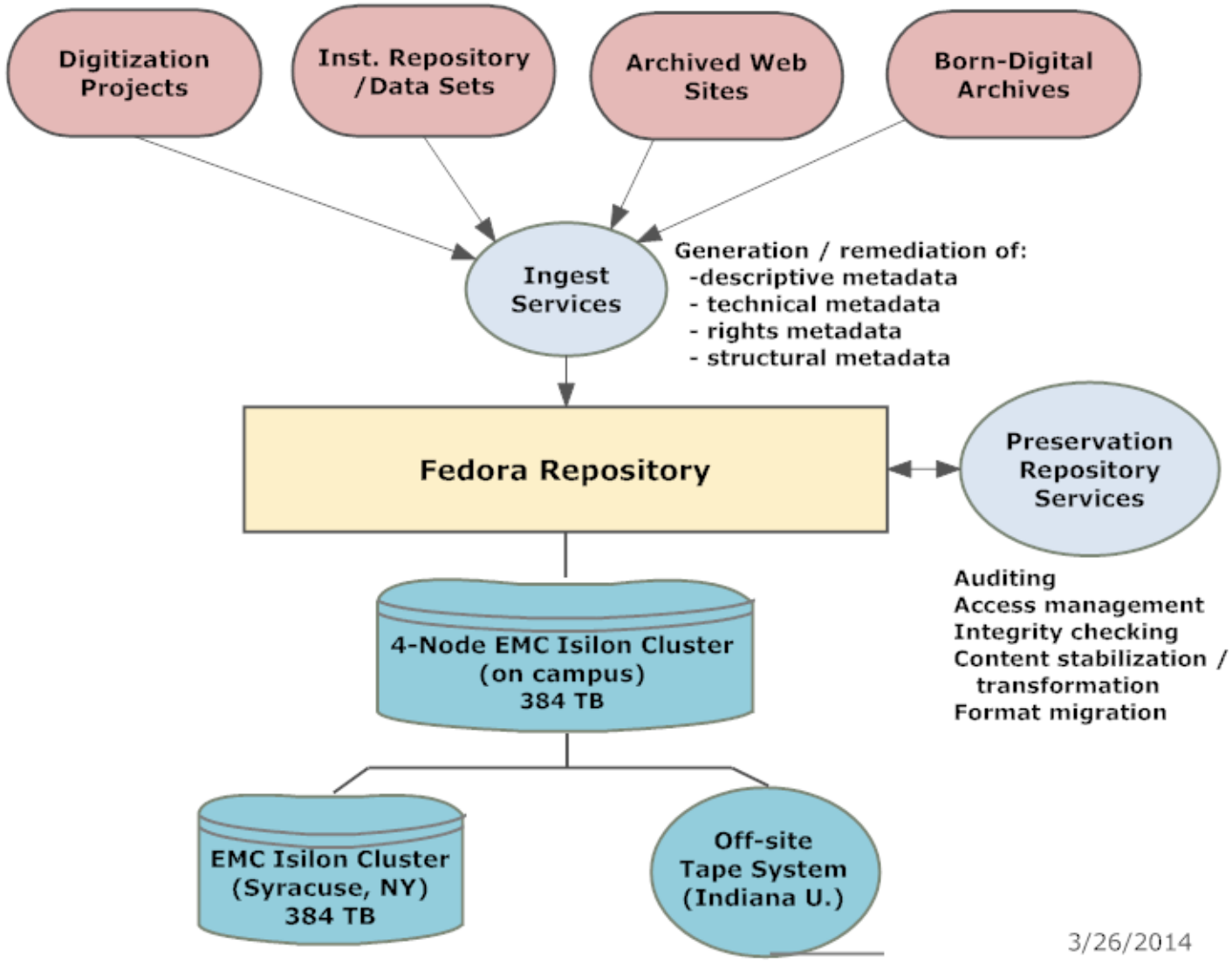


Stephen Davis – Columbia University



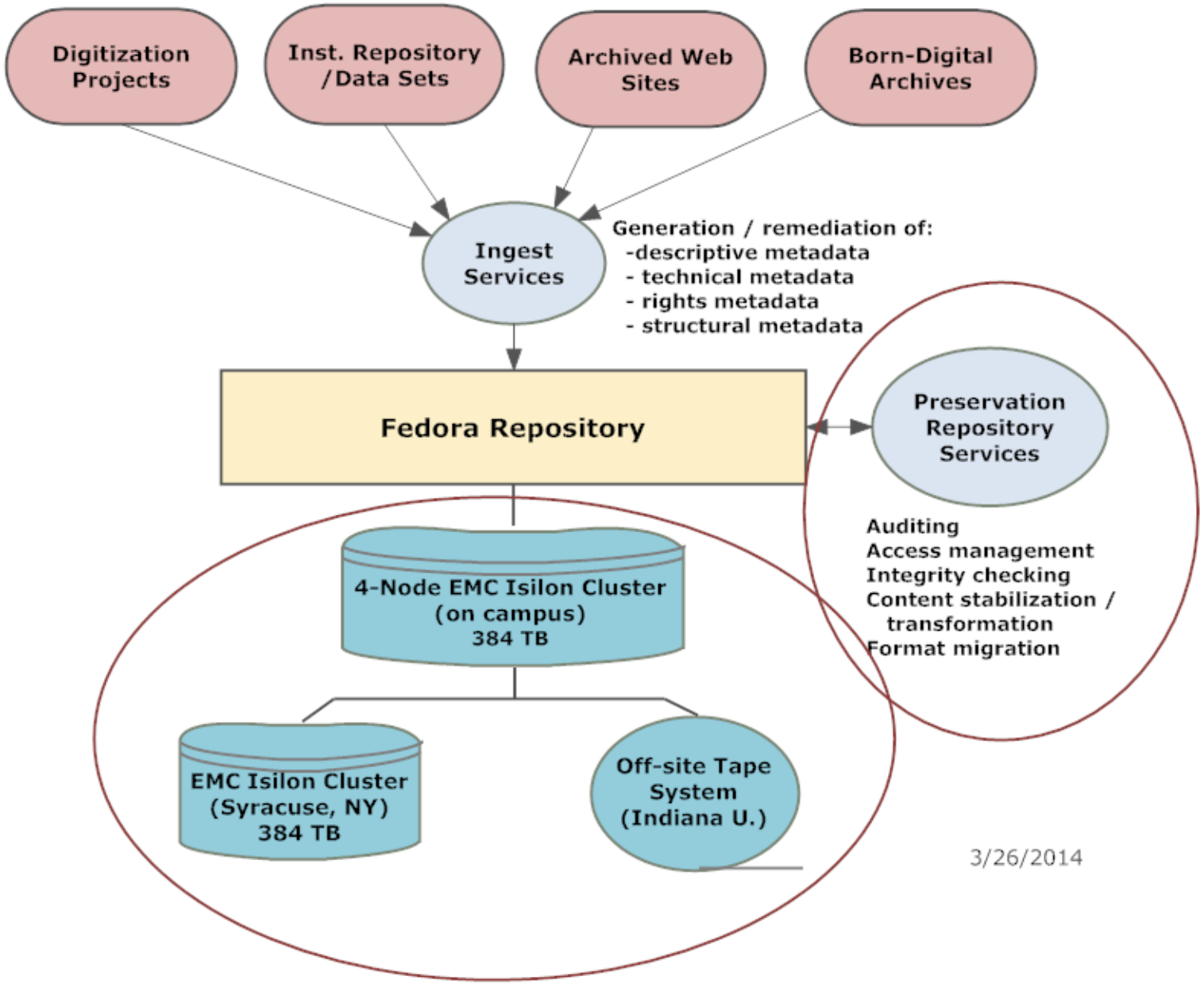
By **Eileen Clegg**

Columbia University Libraries / Information Systems
Digital Asset / Preservation Architecture



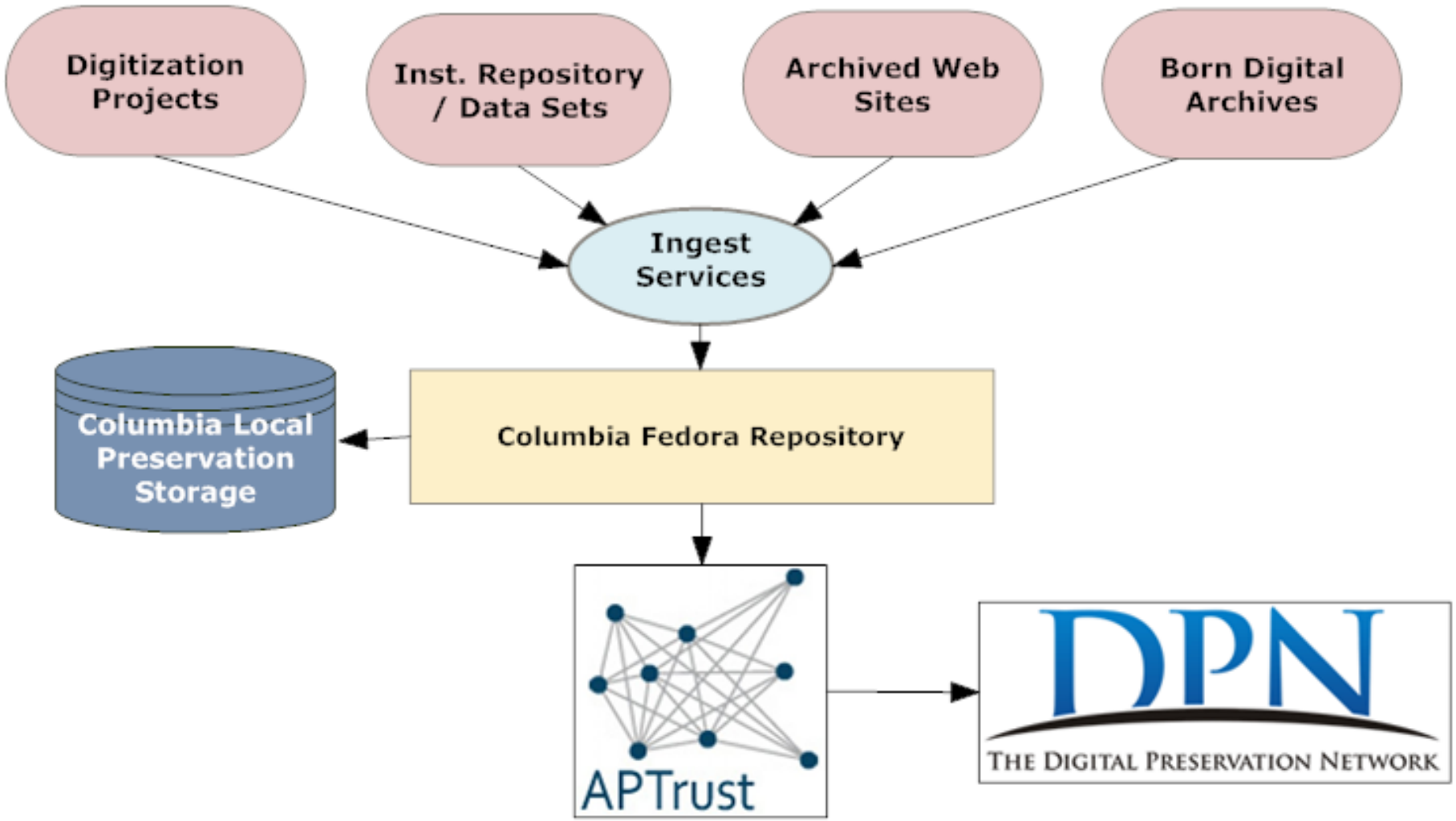
3/26/2014

Columbia University Libraries / Information Systems
Digital Asset / Preservation Architecture



3/26/2014

Columbia University Libraries / Information Systems
Future Digital Asset / Preservation Architecture



“Trusted Digital Repositories”

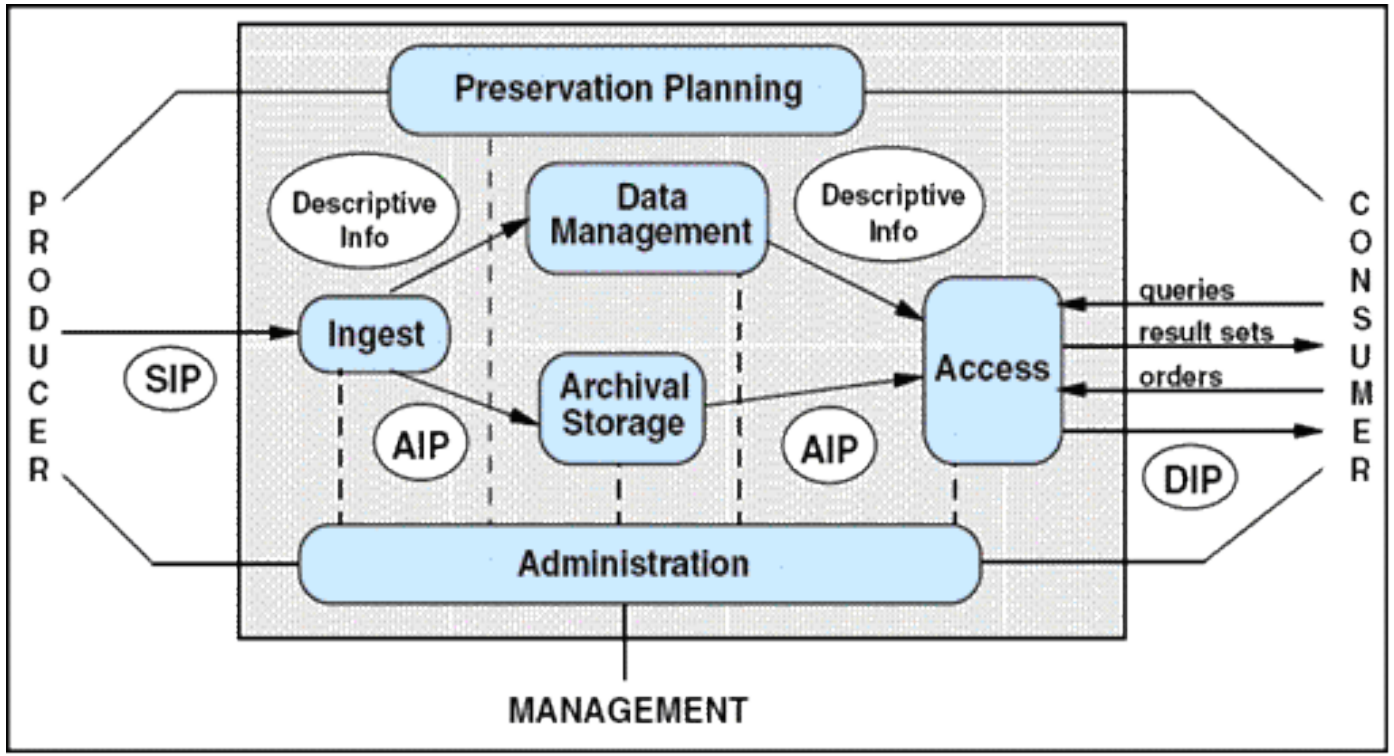
- *Open Archival Information System (OAIS) Reference Model*: CCSDS (2002) “Blue Book”
- *Trustworthy Repositories Audit & Certification: Criteria and Checklist* “Version 1.0” (2007)
- *Audit and Certification of Trustworth Digital Repositories*: CCSDS 652.0-M-1 (2011) “Magenta”
- ISO/DIS 16363:2012 *Space data and information transfer systems -- Audit and certification of trustworthy digital repositories* (2012)

[CCSDS => Consultative Committee for Space Data Systems]

TRAC Compliance #1

OAIS compliance

Conformity with the OAIS Standard



TRAC Compliance #2

Administrative responsibility

A commitment to track and comply with current and emerging standards embraced by the preservation community.

TRAC Compliance #3

Organizational viability

Capacity to receive, store, preserve, and provide access to digital materials under its care, encompassing legal, fiscal, and ethical considerations and requirements.

TRAC Compliance #4

Financial Sustainability

Accounting and budget policies and procedures that are part of a business plan to define and protect requisite resources for the digital preservation program.

TRAC Compliance #5

Technological Suitability

Capacity to develop and maintain requisite hardware, software, expertise, and techniques to support and enable the digital preservation program, including adherence to relevant standards and industry best practice.

TRAC Compliance #6

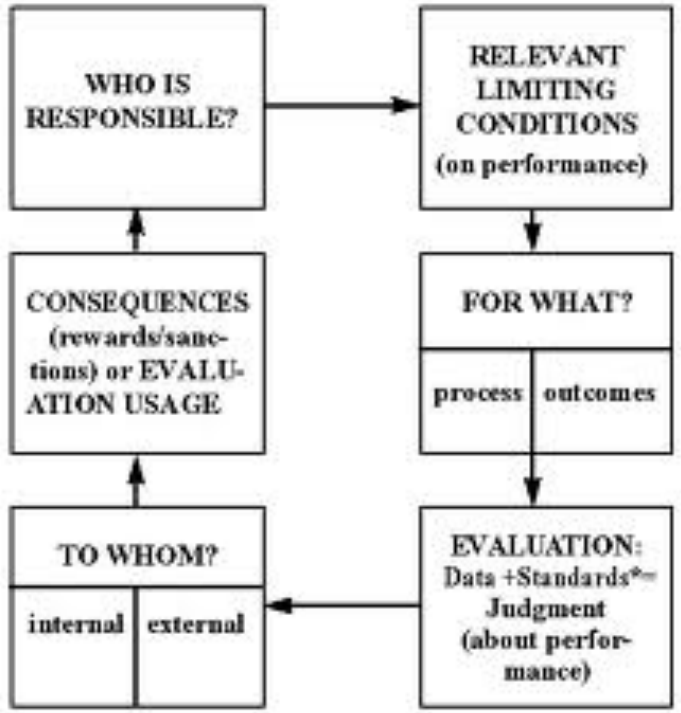
System Security

A commitment to maintaining a constant and appropriate level of environmental and online protection; surveillance; and risk detection, response, and mitigation to safeguard the integrity of digital assets.

TRAC Compliance #7

Procedural Accountability

A means for documenting, sharing, and applying the set of policy statements and associated procedures and prevailing practice.



TRAC Compliance #8

Succession Plan / Exit Strategy

An appropriate, formal 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.


TRUST