Digital Preservation Capability Maturity Model© (DPCMM)

BACKGROUND AND PERFORMANCE METRICS

Version 2.7 Released July 6, 2015

This document provides an overview of the Digital Preservation Capability Maturity Model© (DPCMM) including its origins and foundations, performance metrics, and suggested use. The purpose of DPCMM is to provide practitioners with an integrated process model and business case planning tool to aid in benchmarking and improving digital preservation capabilities.

About the DPCMM Developers

Charles Dollar has more than four decades of practical experience and thought leadership as a historian (Oklahoma State University), archivist (National Archives of the United States), archival educator (University of British Columbia), and consultant (Cohasset Consulting, IMERGE Consulting, and Dollar Consulting). He is co-developer with Lori Ashley of the Digital Preservation Capability Maturity Model (DPCMM) and can be reached at thecdollar@att.net.

Lori Ashley is an independent consultant and educator dedicated to advancing records and information management practices and controls. An experienced strategist and organizational development specialist, she has a passion for developing approaches to jumpstart and sustain cross-functional collaboration among stakeholders who share accountability for effective and efficient lifecycle controls for valued records and information assets. She is co-developer with Charles Dollar of the Digital Preservation Capability Maturity Model (DPCMM) and can be reached at loriashley@wi.rr.com and www.securelyrooted.com.

Table of Contents

Document Control

The significant changes made in this version of the Digital Preservation Capability Maturity Model are:

- Added section on Standards-based digital preservation
- Added references to Risk Management and Producer-Archive interface standards
- Deleted section on Thresholds and moved Conformance into the Standards-based Digital Preservation section
- Simplified the DPCMM graphic
- Expanded the planning section to help practitioners make the business case for digital preservation and moved it to the end of the document following the DPCMM performance metrics
- Expanded and re-titled Appendix B, "Recommended Significant Properties of OAIS Information Packages and Associated Actions by Records Producers and Repositories"
- Fine-tuned the Digital Preservation Services performance metrics to align to significant properties

1.0 Introduction and Background

Since the mid-1970s archivists have recognized that the obsolescence of storage devices and media was a major risk to access to electronic records. They also recognized that dependency on computer software to interpret the bits on storage devices/media created an equally compelling risk to access to electronic records of permanent value. Now that most business information is ‘born digital’ virtually no organization remains immune from the need to proactively address the requirements of long-term information assets managed in digitally encoded formats and systems.

A common lament from the archives, library, records management, and business communities is that ensuring access to authentic, usable electronic records that have long-term[1] operational, regulatory, legal, or cultural memory value is so complex, perplexing, and costly it is difficult to know where to begin or how to make a business case for the required investments and resources. This is a message that we understand and appreciate because we have heard it from our clients and from a wide range of information, records and archives management practitioners working in public, private and not-for-profit organizations[2] around the world. Nonetheless, we believe that it is possible to deconstruct aspects of digital preservation to a level that can be readily understood by a range of stakeholders and facilitate planning for a digital continuity[3] program within the available resources of most organizations.

The Digital Preservation Capability Maturity Model© (DPCMM), which this document describes in some detail, draws upon functions and preservation services identified in ISO 14721, the Open archival information systems (“OAIS”) Reference Model, as well as attributes specified in ISO 16363, Audit and certification of trustworthy digital repositories (TDRs). We developed the DPCMM to be used to conduct a gap analysis of current digital preservation capabilities and to help practitioners and organizations delineate a multi-year roadmap of incremental improvements.

It is important to note that the DPCMM is not a "one size fits all" approach and it is not intended to serve as a capability audit tool. Rather, it is a flexible tool that can be adapted to any organization’s specific requirements and resources, and takes into account a range of potential repository models and implementation strategies. The DPCMM identifies core digital preservation requirements which form the basis for debate and dialogue regarding the desired future state of digital preservation capabilities and the level of risk its leadership is willing to take on with regard to protection of and access to its long-term electronic records. In many instances, this is likely to come down to the question of what

[1] Long-term is a period of time long enough for there to be concern about the impacts of changing technologies on digital information systems. This can be as short as five to seven years and extends indefinitely. In this document long-term is assumed to be 10 years or greater (10+ years).

[2] In this document we use the term “organization” broadly to refer to an individual or to any type or size public or private organization that has a duty to create and maintain information and records in the conduct of business activities.

[3] Digital continuity refers to the ability of an organization to ensure digital information is accessible and usable by those who need it for as long as it is needed. Digital preservation is one aspect of digital continuity.

constitutes digital preservation capability that is “good enough” to fulfill the organization’s mission and meet the expectations of its stakeholders.

In August 2014 we released a Digital Preservation Capability self-assessment application that is based on the DPCMM. The tool, which generates a score card and provides the full set of self-assessment statements upon completion of the survey, is free and open to any organization and practitioner. Register at www.DigitalOK.org.

We ask that you begin the self-assessment within 72 hours of registering or your registration will lapse. You can re-register at a more convenient time. It is not necessary to complete the survey in a single session –save it and return to finish it at a later date.

Download your assessment (pdf) to share with digital preservation stakeholders and communities of interest. Use the component descriptions and performance metrics to inform your digital preservation planning and implementation efforts.

Are
Your
Permanent
e-Records
DigitalOK
www.securelyrooted.com/dpcmm

We hope that you find the model and self-assessment useful. We welcome your feedback. Please contact us via email or by visiting www.securelyrooted.com/dpcmm.

Thank you and best wishes.

Charles M. Dollar
thecdollar@att.net

Lori J. Ashley
loriashley@wi.rr.

2.0 Standards-based Digital Preservation

The requirement and duty to preserve electronic records and other digital information assets for the long-term should be driven by an organization’s mission, vision, values and guiding principles. In our experience, every organization – regardless of size or sector – now has permanent and long-term operational records that exist only in digital formats. This situation means that digital preservation needs to move into the mainstream of content, records and information management planning, implementation, and integration.

There are two significant challenges associated with keeping electronic records available, accessible and usable far into the future: 1) the ever changing technology infrastructure upon which electronic information depends, and 2) maintaining adequate information properties about the preserved digital objects to ensure they are understandable and trustworthy when they are needed. This is a formidable challenge today and is likely to worsen over time as the volume of born-digital content grows and the speed of technology change accelerates. Delays in implementing a systematic programmatic effort to address technology obsolescence and the trustworthiness of digital objects means that the risks and requirements will be more difficult and costly to address in the future.

We believe that standards are critical to building capabilities that can meet the challenges over time associated with digital preservation. The primary international standards which feature prominently in the DPCMM and this document are:

- ISO 14721, Space data and information transfer systems - Open archival information systems – Reference model.
- ISO 16363, Space data and information transfer systems - Audit and certification criteria for trustworthy digital repositories.

We also reference several additional standards which we believe will be useful to the reader:

- ISO 20652:2006, Space data and information transfer systems - Producer-archive interface - Methodology abstract standard.
- ISO 3100:2009, Risk Management, Principles and guidelines.
- PREMIS Data Dictionary for Preservation Metadata (Library of Congress).

A corollary to digital preservation is keeping the right information for the right amount of time, whether that means five years or fifty years. It requires planning, resources, commitment and the ability to adapt to ever-changing operational, legal, regulatory, economic, social, and technology environments and requirements.

Vulnerabilities in networked systems and opportunities associated with e-discovery, cloud computing and “big data” that have emerged over the past decade or so are precipitating a transformation in the way that many organizations have begun to view and handle the management of information as an asset. Information Governance (IG)[4] is being advanced[5] as a coordinating decision-making and accountability framework for maximizing the value of information while minimizing its costs and risk. We welcome developments in this area and hope that executive-level interest in IG will help to promote coordinated approaches and technologies that systematically manage the lifecycle of information, including active preservation, defensible disposition and interoperability between records systems and trustworthy digital repositories.

2.1 Conformance Thresholds in the Model

DPCMM is based on OAIS functions (ISO 14721) and trustworthy repository audit criteria (ISO 16363), which when combined with accepted community good practices, set a high threshold for digital preservation capabilites. Preservation strategies include creation of "preservation ready" digital objects at or near the time of capture or receipt wherever practical. Appendix B in this document reviews in some detail the metadata required as evidence of the accuracy, completeness and trustworthiness of Submission Information Packages, Archival Information Packages, and Dissemination Information Packages.

Many organizations with a mandate to preserve and provide access to long-term and permanent electronic records do not yet have the expertise and resources to implement a preservation repository that conforms to the ISO 14721 specifications and best practices. Many have not yet fully adapted their traditional records management and archival practices to address all of the demands of the digital information age and thus have significant gaps between their authority to preserve and disposition electronic records and their capabilities to fulfill these duties. As organizations consider the implementation of trustworthy preservation environments, they would do well to recognize the need for automated workflows and actions to keep up with the scope and scale of expanding volumes of digital content.

DPCMM offers a way for records producers, practitioners, and digital repository operators to explore interdependencies across the chain of custody for valued digital information assets. While we recognize that much work remains to be done to "connect the dots" between content owners/providers (called "Producers" in the OAIS standard) and content custodians/repositories,[6] it is our hope that use of DPCMM will promote collaboration between repositories and their respective communities of interest by providing a common framework within which to chart progress and share solutions.

[4] Gartner's definition: ***Information governance*** is the specification of decision rights and an accountability framework to encourage desirable behavior in the valuation, creation, storage, use, archival and deletion of information. It includes the processes, roles, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals.

[5] www.iginitiative.com

[6] ISO 20652:2006, Producer-archive interface, addresses communication and coordination between records producers and archives from the point of initial contact until objects are received and validated by the archives.

There is a palatable level of interest and investment in digital preservation coming from analysts, legal professionals and technologists. In 2013 The Sedona Conference Commentary on Information Governance identified 11 principles that organizations should take into account when developing and operating an Information Governance program. Principle 9 is especially important because it urges organizations to take reasonable action to ensure on-going integrity and availability of long-term digital assets for their useful life. Within this context, integrity means trustworthiness while "availability" means there are no technology barriers (e.g., obsolescent native proprietary file formats or unreadable storage media) to access. As Information Governance matures we anticipate that digital preservation requirements and actions will increasingly be integrated with content management tools, e-discovery, and legal and regulatory matters.

2.2 Surrogate Digital Preservation Capability and Services

A great deal of work has been done around the world to develop preservation tools, services and repositories. A number of U.S. state archives have built or are testing preservation repositories that are intended to conform with ISO 14721 specifications. Many archives, libraries and cultural memory institutions now routinely accession "born digital" or scanned records through manual or semi-automated workflows while others address digital preservation requirements with a range of tools and services such as Contentdm®, ArchiveIt, BagIt, and LOCKSS, among others. Some institutions have participated in email management and archiving projects, leveraged technical capabilities developed through externally funded projects, or collaborated in grant funded projects. It should be noted that currently no enterprise content management (ECM) system meets the OAIS requirements for a trusted digital repository.

The DPCMM takes into account this spectrum of digital preservation capabilities by distinguishing between ISO 14721 conforming and partially conforming or "surrogate" capabilities and services. In the performance metrics described in Section 3.4 this "threshold" is represented by a blue bar between Intermediate (Level 3) and Nominal (Level 2) capabilities.

Despite not fully conforming with ISO 14721 specifications and the TDR audit and certification criteria, many digital preservation and curation tools and projects are noteworthy and clearly are substantive and represent important emerging capabilities. Examples of surrogate projects, initiatives, tools and services are provided in the table below.

Category of Surrogate Capability	**Examples**[7]
Service Bureau	Web archiving service Archive-It
Curatorial practice-based and middleware assessment consortium	PeDALS (uses LOCKSS)
Best practice for a specific collection	GeoMAPP (for superseded geospatial data sets)
Centralized regional repository	Washington State MSPP
Software or packaging file format to facilitate the transfer of digital content	BagIt
Capture and registration functionality of a DoD 5015.2 certified document and records management application (RMA)	Open source options (Alfresco, Nuxeo) as well as a variety of proprietary solutions by major vendors including EMC, IBM, Hyland, OpenText, Oracle, Vignette and others are available
Digital asset management software and/or hosting solutions that facilitate transfers, indexing, storage, search, and web-based access	Contentdm® and OCLC Hosting Services

Table 1. Examples of Surrogate Digital Preservation Capability

While some surrogate capabilities may be adequate for a period of several years or for a specific collection to meet requirements for long-term preservation and access to electronic records, technology obsolescence will eventually require updates and changes. In addition, some surrogate capabilities are short-term, project-based, and/or severely limited in scope. Successful adoption and integration of "lessons learned" after a project based on surrogate capabilities is difficult and much less certain to deliver sustainable digital preservation capabilities and services.

[7] This table does not presume to provide an inclusive list of available digital preservation capabilities, services or solutions.

3.0 Overview of the Digital Preservation Capability Maturity Model

A capability maturity model (CMM) is a set of structured levels that describe how well the practices, processes and behavior of an organization can reliability and sustainably produce desired outcomes. The CMM identifies a series of associated activities and baseline metrics used to measure performance in a given area. The maturity stages are cumulative: an organization achieving a higher stage of maturity must implement and sustain all of the requirements for that stage in addition to requirements for all of the lower stages.

The goal of the Digital Preservation Capability Maturity Model (DPCMM) presented in this document is to help practitioners and their respective organizations and preservation repositories to:

- identify at a high level where an electronic records management program is in relation to optimal digital preservation capabilities;
- report gaps in capability levels and preservation performance metrics[8] to educate and engage resource allocators and other stakeholders, and
- establish priorities for achieving standards-based capabilities to preserve and ensure access to long-term electronic records.

DPCMM [9] is a five level (or stage) maturity continuum. It is based on the functional specifications of ISO 14721, the auditing criteria of TRAC and ISO 16363, and accepted best practices in operational digital preservation repositories. DPCMM is a systems-based tool for charting an evolutionary path from disorganized and undisciplined management of electronic records, or the lack of a systematic digital continuity approach, into increasingly mature stages of digital preservation capability.

Some terms and concepts used in this document may be unfamiliar to some readers. Appendix A: Glossary of Terms provides more than seventy definitions to aid in the use of DPCMM.

[8] The performance metrics were applied while using DPCMM in consulting projects and underwent a significant revision in conjunction with a project sponsored by the Council of State Archivists (CoSA) to adapt the model to a digital preservation capability web survey for fifty-six state and territorial archives. Gary Miller (Wind Lake Solutions), Richard Pearce-Moses (Clayton State University), Milovan Misic (World Intellectual Property Organization) and Ton Bezemer (Anth. P. Bezemer LLM, The Netherlands) provided valuable commentary during development of the CoSA Digital Preservation Capability (DPC) Self-Assessment.

[9] The genesis of this Digital Preservation Capability Maturity Model is rooted in a presentation given to the Arizona Electronic Records Management Task Force in 2002. Introduction to the potential use of an electronic records management capability maturity model by Timothy Sprehe and Charles McClure led to significant enhancements. The Digital Preservation Capability Maturity Model performance metrics were inspired in part by material developed by the International Records Management Trust to support an assessment of an organization's readiness to undertake an electronic records management program. The first use of DPCMM was in a 2007 project at the Delaware Public Archives.

3.1 Five Stages of Digital Preservation Capability

Like other capability maturity models,[10] DPCMM uses a five level or stage approach. Its levels range from Nominal at the lowest end to Optimal at the highest end (Figure 1). In an organization operating at a Digital Preservation Capability Nominal level (Stage 1), a systematic electronic records management and/or digital preservation program has not yet been undertaken or a digital preservation program exists only on paper. In contrast, the highest level (Stage 5 - Optimal) of Digital Preservation Capability represents an organization with sustained, trustworthy capabilities that are systematically managed through process improvement and optimization.

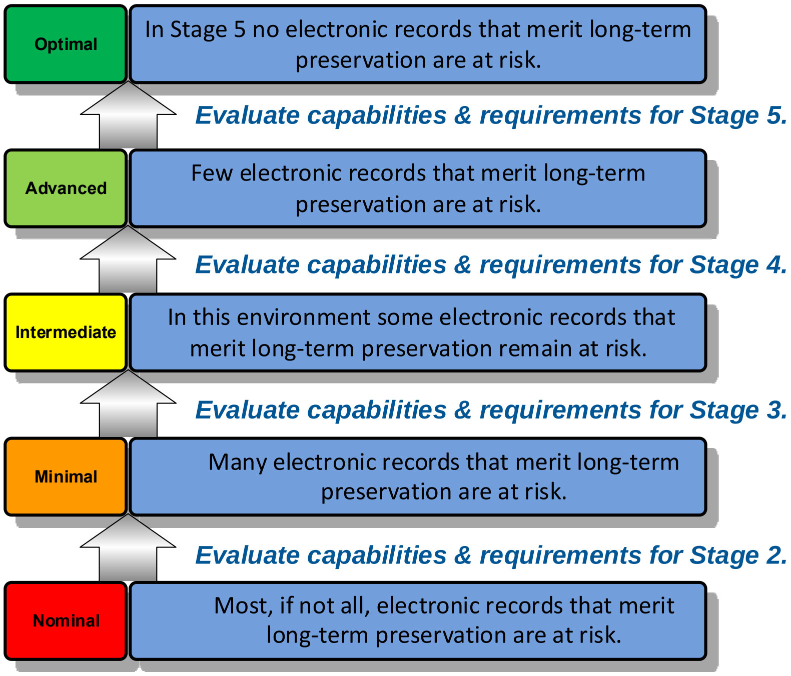

Optimal
In Stage 5 no electronic records that merit long-term preservation are at risk.
Evaluate capabilities & requirements for Stage 5.
Advanced
Few electronic records that merit long-term preservation are at risk.
Evaluate capabilities & requirements for Stage 4.
Intermediate
In this environment some electronic records that merit long-term preservation remain at risk.
Evaluate capabilities & requirements for Stage 3.
Minimal
Many electronic records that merit long-term preservation are at risk.
Evaluate capabilities & requirements for Stage 2.
Nominal
Most, if not all, electronic records that merit long-term preservation are at risk.

Figure 1. Five Stages of Digital Preservation Capability

Conformance to the requirements of ISO 14721 and the audit criteria in ISO 16363 for all 15 DPCMM components is required to achieve Intermediate (Stage 3 capability). A high level description of risk[11] and key characteristics of each stage is provided on the following pages.

[10] "Digital information and records management capability matrix, National Archives of Australia, available at http://www.naa.gov.au/naaresources/documents/capability-matrix.pdf; "Digital Preservation Environment Maturity Matrix," available at http://www.nsla.org.au/publication/digital-preservation-environment-maturity-matrix; ARMA International "Information Governance Maturity Model," available at http://www.arma.org/r2/generally-accepted-br-recordkeeping-principles/metrics; and the Inventory Maturity Model for Information Governance, available at www.rulesmapper.com.

[11] Threats to digital information assets are well known and listed in numerous resources. We recommend that practitioners refer to ISO 31000:2009, Risk management – Principles and guidance, along with related risks management standards to identify and describe for stakeholders the range of potential economic, performance and reputational consequences associated with failure to proactively preserve long-term electronic records.

Stage 5: Optimal Digital Preservation Capability

Stage 5 is the highest level of digital preservation readiness capability that an organization can achieve. It includes a strategic focus on digital preservation outcomes by continuously improving the manner in which electronic records lifecycle management is executed. Stage 5 digital preservation capability also involves benchmarking infrastructure and services relative to other "best in class" digital preservation programs and conducting proactive monitoring for breakthrough technologies that can enable the program to improve its digital preservation performance. **In Stage 5 few if any electronic records that merit long-term preservation are at risk.**

Stage 4: Advanced Digital Preservation Capability

Stage 4 capability is characterized by an organization with a robust infrastructure and digital preservation services that are based on ISO 14721 specifications and TRAC, the Trustworthy Repository Audit and Certification: Criteria and Checklist and/or ISO 16363. At this stage the preservation of electronic records is framed entirely within a collaborative environment in which there are multiple participating stakeholders. Lessons learned from this collaborative framework serve as the basis for adapting and improving capabilities to identify and proactively bring long-term electronic records under lifecycle control and management. **Some electronic records that merit long-term preservation may still be at risk.**

Stage 3: Intermediate Digital Preservation Capability

Stage 3 describes an environment that embraces the ISO 14721 specifications and other best practice standards and schemas and thereby establishes the foundation for sustaining enhanced digital preservation capabilities over time. This foundation includes successfully completing repeatable projects and outcomes that support enterprise digital preservation capabilities and fosters collaboration, including shared resources, between record producing units and entities responsible for managing and maintaining trusted digital repositories. In this environment **many electronic records that merit long-term preservation are likely to remain at risk.**

Stage 2: Minimal Digital Preservation Capability

Stage 2 describes an environment where an ISO 14721-based preservation repository is not yet in place. A surrogate preservation repository[12] for electronic records is available to some records producers that satisfies some but not all of the ISO 14721 specifications. There is some understanding of digital preservation issues and strategies but it is limited to a relatively few individuals. There may be virtually no relationship between the success or failure of one digital preservation initiative and the success or failure of another one. Success is largely the result of

[12] The term 'surrogate' is used in this document for a repository, tool or service used for the preservation of long-term or permanent electronic records that does not fully conform to the specifications in the ISO 14721 reference model.

exceptional (perhaps even heroic) actions of an individual or a project team. Knowledge about such success is not widely shared or institutionalized. **Most electronic records that merit long-term preservation are at risk.**

Stage 1: Nominal Digital Preservation Capability

Stage 1 describes an environment in which the specifications of ISO 14721 and other standards may be known, accepted in principle, or under consideration but have not been formally adopted or implemented by the unit responsible for preservation (i.e., the Archives or Records Management function) or by records producers. Generally, there may be some understanding of digital preservation issues and concerns but this understanding is likely to consist of ad hoc electronic records management practices and digital continuity infrastructure and initiatives. Although there may be some isolated instances of individuals attempting to preserve electronic records on a network or removable storage media (e.g., DVD or hard drive), **practically all electronic records that merit long-term preservation are at risk.**

3.2 Scope of the Digital Preservation Capability Maturity Model

This capability maturity model consists of fifteen (15) components, or key process areas,[13] that are necessary and required for the long-term continuity, access, and preservation of authentic, accessible and reliable electronic records. Each component is described and metrics for each of the five (5) levels of digital preservation capability are identified. **Conformance and sustained performance at any given level is required before the next higher level can be achieved.**

The objective of the model is to provide a process and performance framework (benchmark) against best practice standards and foundational principles of records management, information governance, and archival science. The five levels of capability identified for each of the DPCMM components offer a way for organizations to see what level of sustained effort is required to move to the next higher level.

Note that the model has three separate but interrelated high level features: Digital Preservation Infrastructure, Preservation Repository, and Digital Preservation Services. The following pages include scope notes for the graphic elements in the DPCMM diagram.

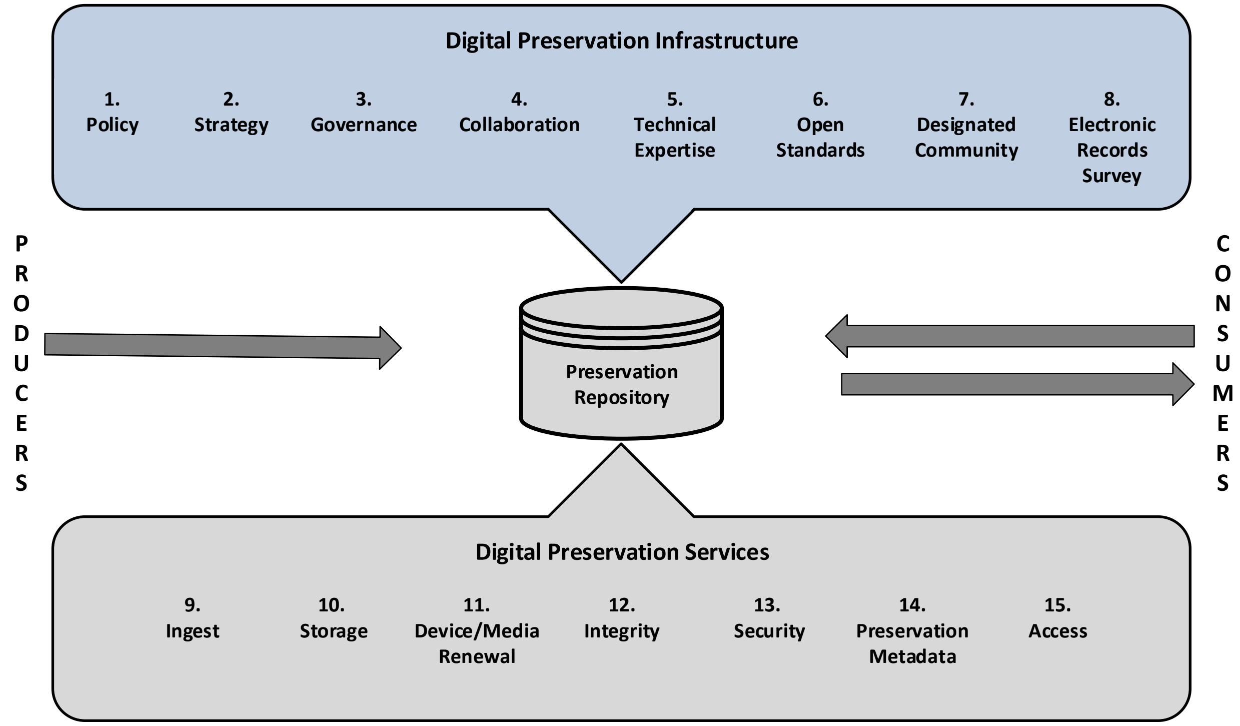


Figure 2. Digital Preservation Capability Maturity Model© (DPCMM)

[13] A Key Process Area (KPA) identifies a set of related activities that when performed together achieve a set of goals considered important.

Producers

Producers is the term used to reference external creators and owners of electronic records who have an obligation to retain long-term (10+ years) and/or permanent records stored in digital format. These stakeholders have a responsibility to provide sufficient information about the origin and use of records to the repository and to engage in active preservation where possible. Producers may have an obligation or the option to transfer permanent and long-term electronic records to one or more specified preservation repositories for safekeeping and access.

Digital Preservation Infrastructure

There are eight (8)) infrastructure components that are essential to ensure a sustained organizational commitment, including adequate and sustained resources, to the long-term preservation of electronic records:

1. Digital Preservation Policy
2. Digital Preservation Strategy
3. Governance
4. Collaboration
5. Technical Expertise
6. Open Standard Technology Neutral ("OS/TN") Formats
7. Designated Community
8. Electronic Records Survey

The eight digital preservation infrastructure components focus on what an organization as a distinct entity does to identify records and collections that require preservation and enable a preservation repository to execute the appropriate digital preservation actions. Or to put it differently, a trusted preservation repository executes services within the constraints of an organization's digital preservation infrastructure.

Preservation Repository

Ensuring the continuity of electronic records and enabling the design, operation, and management of preservation environments requires the integration of people, processes, and technologies. The most complete digital preservation environment is based on models and performance criteria which include ISO 14721, ISO 16363, and generally accepted operational practices. The organization that has custody of the records may manage the repository or may contract with an external third-party. A variety of systems, tools and services may be combined to facilitate end-to-end workflow of records from ingest to access.

A preservation repository may range from a simple system that involves a low-cost file server and software that provides non-integrated preservation services to complex systems comprised of data centers and server farms and interoperable communication networks. It is likely that many organizations initially will rely on "surrogate" digital preservation capabilities and services that approximate but do not offer all of the transfer, data management and access functionality of an ISO 14721 conforming system.

Digital Preservation Services

There are seven (7) key business process areas required for continuous monitoring of external and internal environments in order to plan and take preservation actions that sustain the integrity, security, usability and accessibility of electronic information and records stored in preservation repositories:

9. Ingest
10. Archival Storage
11. Media/Device Renewal
12. Integrity
13. Security
14. Preservation Metadata
15. Access

The seven digital preservation services focus on a range of actions required to ingest and sustain long-term and permanent electronic records and continuously monitor the technical environment upon which they depend. The ability to efficiently plan and execute preservation actions to sustain the integrity, security, usability and accessibility of records stored in the repository relies on the record producing organization to systematically identify and transfer electronic records of long-term value as well as provide sufficient strategic direction and resources.

Consumers

Consumers or users or electronic records comprise a Designated Community consisting of external individuals or groups with an interest in and/or right to access records in the preservation repository. These stakeholders are likely to represent a variety of interests and their access requirements are likely to change over time.

3.3 Digital Preservation Capability Index Score

Each of the 15 DPCMM components has five capability performance metrics associated with it. Each digital preservation capability metric has a value between 0 and 4. If a self-assessment exercise determines that a performance score of 3 for a specific component is appropriate, for Digital Preservation Policy, for example, it becomes the **index value** for the organization’s Digital Preservation Policy capability. This procedure is repeated for the remaining fourteen components of the DPCMM which results in an aggregated digital preservation capability score.

The range of composite index scores[14] organized by each of the five levels is:

	Capability Levels	Composite Index Score
🟥	Nominal Digital Preservation Capability	0
🟧	Minimal Digital Preservation Capability	1 - 15
🟨	Intermediate Digital Preservation Capability	16 - 30
🟩	Advanced Digital Preservation Capability	31 - 45
🟩	Optimum Digital Preservation Capability	46 – 60

Figure 3. Range of Digital Preservation Capability Index Score

3.4 Digital Preservation Capability Components and Metrics

The DPCMM consists of 15 components. This section describes each component and the associated set of five digital preservation capability metrics. Definitions can be found in the Glossary of Terms (Appendix A). Throughout the metrics section we use the terms "organization" and "records producer" to denote the legal entity (company, institution, association, agency, individual, etc.) that is charged with or has taken on the task of enabling the continuity and preservation of long-term and/or permanent records.

The term "preservation repository" is used to denote the integrated people, processes and technologies charged with ingesting, storing, protecting, managing and providing access to the electronic records. This function may be provided by an internal business or technology unit, operated as one or more standalone repositories under the control of an Archives or Records Management unit, include participation in a federated or regional repository system, and/or include the use of digital preservation services provided by one or more third parties. Individuals or groups who seek access to the electronic records in the preservation repository are referred to as "users." We recognize and acknowledge that different organizational or functional units and/or stakeholders may have these responsibilities. We encourage the use of alternative terms for these conventions where this is desirable.

Conformance to ISO 14721 requires sustained capabilities at lower levels as depicted by the use of a blue bar (see below) in the metrics tables.

Level	Digital Preservation Capability Metrics
0	
1	
2	
🟦	ISO 14721 Conformance
3	
4	

Figure 4. Conformance Threshold

[14] Specific communities of interest may choose to develop a modified range of composite index scores.

Digital Preservation Infrastructure: Components 1 – 8

1. Digital Preservation Policy

Preservation of accessible, authentic, and usable electronic records for as far into the future as necessary relies on digital information technologies but is equally dependent upon organizational commitment and practices. The organization charged with ensuring preservation and access to long-term and permanent legal, fiscal, and/or historical records should state its policy in writing, communicate the policy to all stakeholders, and periodically audit the policy for compliance.

A written digital preservation policy includes the purpose, scope, accountability, and approach to the transfer of records and the operational management and sustainability of trustworthy preservation repositories.

Level	Digital Preservation Policy Capability Metrics
0	The organization does not have a written digital preservation policy.
1	The organization has a digital preservation policy in development but it has not yet been approved or issued.
2	The organization has issued a digital preservation policy and it is widely disseminated to stakeholders.
	ISO 14721 Conformance
3	The organization annually conducts a self-assessment and reports adherence to the digital preservation policy to its governing body.
4	The organization arranges for a periodic peer review or external audit of the digital preservation policy and revises the policy as appropriate.

2. Digital Preservation Strategy

The organization charged with the preservation of long-term and permanent electronic records must proactively address risks associated with technology obsolescence. While no single strategy is appropriate for all organizations, information types and resources, there must be plans to periodically upgrade storage devices, storage media, and file formats.

Left unchecked , the obsolescence of storage devices and media eventually will render the bit streams of electronic records unreadable. The inevitable obsolescence of file formats, especially native, proprietary ones, means that over time software applications will not be able to render bit streams into understandable and usable electronic records.

The generally accepted strategy is to mitigate the obsolescence of storage devices/media through planned, periodic renewal, which over time ensures that "bit streams" can be read by current technologies (*see Component 11*). The generally accepted strategy for mitigation of file format obsolescence is reliance on interoperable, open standard technology neutral formats, which are otherwise considered “preferred preservation formats” (*see Component 5*).

Level	Digital Preservation Strategy Capability Metrics
0	The organization does not have a formal strategy to address technology obsolescence.
1	The strategy calls for accepting electronic records in native formats on an ad hoc basis and keeping the bit streams alive until software and other resources are available to transform the records into open standard technology neutral file formats.
2	The strategy calls for encouraging records producers to convert electronic records of long-term and permanent value in their custody to “preservation ready” formats at or near the time of receipt and creation. The strategy includes ad hoc monitoring of changes in technologies that may impact digital records collections in the custody of records producers and preservation repositories.
	ISO 14721 Conformance
3	In addition to promotion of “preservation ready” records, the strategy calls for transformation of electronic records in five (5) selected native file formats to preferred preservation formats at ingest and proactive monitoring of changes in technologies that affect the preservation of electronic records.
4	The strategy calls for the transformation of electronic records in native file formats to ten (10) or more preferred preservation formats at ingest. Electronic records in archival storage are automatically transformed to newer interoperable forms as they displace current ones. Proactive monitoring of changes in technologies that affect the preservation of electronic records is on-going.

3. Governance

An organization with a digital preservation mandate should have a formal decision-making process aligned to its enterprise information governance framework that assigns accountability and authority for the preservation of electronic records with permanent value, and articulates approaches and practices for preservation repositories sufficient to meet stakeholder needs. This capability ideally leverages existing organizational rules, practices and protocols as well as engages cross-functional stakeholders.

Long-term preservation, however, may require the creation of new authorities to address the threats of technology obsolescence. A preservation repository may be run by a business or technology unit, operated as one or more standalone repositories under the control of a Records Management unit or Archives, include participation in a federated or regional repository system, and/or use digital preservation services provided by one or more third parties.

The organization exercises digital preservation governance in conjunction with archives, information management/technology functions, and with other custodians and digital preservation stakeholders such as records producers and users. The governance framework enables compliance of the preservation repository with applicable laws, regulations, record retention schedules, disposition authorities, and standards. Plans and decisions resulting from governance activities, including repository operational statistics, are shared with internal stakeholders and third-party operators.

Level	Governance Capability Metrics
0	The organization's current information governance activities do not specifically address digital preservation requirements.
1	The organization has a limited, project-based digital preservation governance framework that is operational or has been successfully completed.
2	The organization is developing an enterprise governance framework that identifies roles and responsibilities for electronic records lifecycle management and digital preservation.
	ISO 14721 Conformance
3	The organization has adopted an enterprise digital preservation governance framework that includes comprehensive policies and procedures and specifies an on-going commitment to the sustainability of one or more preservation repositories.
4	The enterprise digital preservation governance framework supports one or more preservation repositories and is reviewed and updated at least every two years to take into account changing technologies and organizational requirements.

4. Collaboration

Digital preservation is a multi-faceted discipline that takes into account the organization's information architecture and technology environment as well as accepted standards and best practices. An organization with a mandate to preserve electronic records is well served by maintaining and promoting collaboration among its many stakeholders.

Plans for different types of records, models for preservation approaches and criteria, and a framework of repository components and services require tighter cooperation and engagement between long-standing partners such as IT, peer organizations, software and service providers, and other support functions. Collaboration should acknowledge the interdependencies between and among the operations of records producers, legal and statutory requirements, information technology policies and governance, and historical accountability.

Active engagement in addressing the challenges of long-term digital preservation makes the best use of resources and lessons learned. The collaborative framework evolves in response to changes in information technologies and the business operations of Record Producers. This collaborative framework seeks to leverage financial, human, and technical resources, promote stewardship, and exchange knowledge about the current and future state of digital initiatives. This collaborative framework may extend beyond the organization to include other repositories, federal or other public sector agencies, as well as consortia of other organizations with a similar or shared mission.

Level	Collaboration Capability Metrics
0	No collaborative digital preservation environment exists within or across the organization.
1	The organization is currently working to establish a framework for collaborative engagement on electronic records management and digital preservation issues.
2	Under its collaborative digital preservation framework the organization has successfully engaged or is currently engaged with selected stakeholder entities to proactively address digital preservation requirements. These engagements may include externally funded collaborative digital preservation initiatives.
	ISO 14721 Conformance
3	Under its collaborative digital preservation framework the organization has successfully engaged or is currently engaged with most stakeholders to proactively identify and meet their digital preservation requirements.
4	The organization continuously monitors and updates its digital preservation collaboration framework to support proactive outreach to all stakeholders to identify and meet their digital preservation requirements.

5. Technical Expertise

A viable digital preservation capability requires organizations to have sufficient expertise in electronic records management and digital preservation to support all of the infrastructure and requisite key processes, including on-going professional development for personnel and certification of the repository. Technical expertise may exist within internal or contracted staff, may be provided by a centralized service bureau, or by external service providers.

NOTE: It is likely that many organizations will initiate a long-term digital preservation program with one or more electronic records management applications (RMA) that conform with country or regional-level standards, such as Department of Defense (DoD) Directive 5015.2-STD, Model Requirements for the Management of Electronic Records (MoReq2010), and Victorian Electronic Records Strategy version 2 (VERS2). These systems may support some but not all ISO 14721 functions.

Level	Technical Expertise Capability Metrics
0	The organization has little or no operational access to specialized professional technical expertise in digital preservation or electronic records management.
1	The organization has access to internal or external professional technical expertise that supports only narrowly defined project-based digital preservation initiatives. This may also include technical expertise in deploying electronic records management applications (RMA) certified to one or more standards.
2	The organization has access to internal or external professional technical expertise who assist records producers in the creation of preservation ready records and/or support surrogate ingest and archival storage services.
	ISO 14721 Conformance
3	The organization has access to internal or external professional technical expertise that supports all functions of an ISO 14721 preservation repository.
4	The organization has access to internal or external professional technical expertise that supports all functions of an ISO 14721 preservation repository, along with the capability to assess the impact of emerging technologies that should be taken into account in long-term digital preservation planning activities.

6. Open Standard Technology Neutral Formats

A requisite for a sustainable digital preservation program that ensures long-term access to usable and understandable electronic records is mitigation of file format obsolescence. Current best practice for mitigation of file format obsolescence involves three separate but related actions.

> The first action is to support a **Technology Watch Program** on the sustainability of file formats. This can be achieved through an external service like the U.S. Library of Congress[15] or PRONOM[16], the technical registry of the National Archives of the United Kingdom.
>
> The second action involves the commitment of the preservation repository to **adopt open standard technology neutral ("OS/TN") file formats to use as preservation formats.**
>
> The third action pertains to **proactive engagement and collaborative working relationships with Records producers** to advise them on the use of preservation ready file formats when they create and maintain electronic records of long-term and permanent historical, legal, or financial value that will be transferred to the custody of a preservation repository.

Open standard platform-neutral file are developed in an open, public setting, are issued by a certified standards organization, and have few or no technology dependencies. Current preferred OS/TN file formats include:

CSV for spreadsheets
HTML, Plain Text, XML, ODF, and PDF/A for text
JPGE 2000 for photographs
PDF/A, PNG, and TIFF for scanned images
SVG for graphics
MPEG-4 and Motion JPEG2000 for video
WAVE_BWF LPCM for audio
WARC for web pages

Over time digital preservation tools and solutions will emerge that require new open standard technology neutral standard file formats. Open standard technology neutral formats are backwardly compatible so they can support interoperability across technology platforms over an extended period of time and space.

Capability metrics for Open Standard Technology Neutral Formats are provided on the next page.

[15] Visit the Library of Congress Digital Formats Web Site at www.digital preservation.gov/formats/index.shtml
[16] Visit http://www.nationalarchives.gov.uk/PRONOM/Default.aspx

Level	Open Standard Technology Neutral Formats Capability Metrics
0	The organization has not yet adopted any open standard technology (OS/TN) file format as a preferred preservation format.
1	The organization has adopted at least one OS/TN file format as a preferred preservation format.
2	The organization has adopted **no more than three** OS/TN formats as preferred preservation formats.
	ISO 14721 Conformance
3	The organization has adopted **no more than five** open standard technology neutral formats as preferred digital preservation formats (text, spreadsheets, scanned images, vector graphics, digital photos, audio, video, and web pages). A Technology Watch Program is used to monitor the sustainability of these OS/TN file formats.
4	The organization has adopted **ten or more** OS/TN neutral formats as preferred digital preservation formats and continuously monitors the emergence of new OS/TN file formats and adopts them as appropriate for use as preferred digital preservation formats.

7. Designated Community

The organization that has responsibility for preservation and access to permanent electronic records is well served through proactive outreach and engagement with its Designated Community of Records producers and users. While this activity has traditionally taken place with representatives of the records producers in the form of records appraisal and retention schedule review and disposition authorization, the challenges of digital preservation demand that records management practitioners engage in additional "upstream" actions in the lifecycle management of long-term and permanent electronic records. Submission agreements[17] and transfer protocols should be standardized and service level agreements defined for repository operations. Formal agreements and procedures with records producers document the content, rights, and conditions under which the preservation repository will ingest, preserve, and provide access to electronic records. Specific assurances are given to ensure privacy and protection of intellectual property as appropriate.

The organization maintains written procedures regarding access to its electronic collections. Dissemination Information Packages (DIPs) are developed and updated in conjunction with its user communities (e.g., scholars, genealogists, the public, etc.). Procedures are regularly reviewed and updated to take into account changing business practices of Records producers as well as the research interests and access capabilities of users.

Level	Designated Community Capability Metrics
0	The organization has no formal documentation that defines the rights, obligations, and responsibilities of the Designated Community for electronic records to be transferred to or held by a preservation repository.
1	The organization has ad hoc agreements with selected records producers that support the transfer of electronic records to a preservation repository.
2	The organization has formal, written agreements with a few records producers that support the transfer of surrogate SIPs and proactively reaches out to select users to identify their specific needs and requirements for access to electronic records in its custody.
	ISO 14721 Conformance
3	The organization engages with most records producers in its mandated domain to establish written agreements about their rights, obligations, and responsibilities for transferring Submission Information Packages (SIPs) to the preservation repository. The organization works closely with most users to establish DIP profiles that meet their needs and requirements.
4	The organization actively engages all records producers in its mandated domain to establish written agreements about their rights, obligations and responsibilities for transferring SIPs. Profiles of conforming SIPS are regularly reviewed and updated to take into account changing business practices of Records producers. The organization works closely with all users to establish DIP profiles that meet their evolving needs and requirements.

[17] Submission agreements specify the data model and the logical constructs used by the records producer and how they are represented on each media delivery to the repository.

8. Electronic Records Survey

All public and private organizations are responsible for records created, received or acquired that are evidence of its business activities, regardless of the format or media used. They have an obligation to ensure the authenticity, integrity, usability and reliability of the records for as long as they are required.

Records with long-term retention requirements or permanent value were traditionally transferred from an operations area or unit to the custody of a centralized Records Management and/or Archives function for preservation. Due to the fragility of electronic records, organizations are advised to proactively address digital preservation **as close to the time of electronic records creation or capture as practicable**. This is especially important for long-term operational records, that is, records that will remain in the custody of the operations unit and are considered “active” records.

One effective way to accomplish proactive preservation is to maintain a comprehensive inventory of electronic records and systems as well as collaborative working relationships between stakeholders that include records producers, Legal/Compliance, Archives, Records Management, Information Services/Technology and third-party application, solution and service providers.

A key feature of conforming ISO 14721 digital repositories is reliance on open standard technology neutral formats. During the ingest process electronic records in proprietary formats are transformed into preferred preservation formats that the organization and/or repository has adopted. Over time and with increasing volumes of electronic records, format transformation during the ingest process may become burdensome. This obligation can be mitigated in part if "preservation ready" records, that is, records that are in open standard interoperable technology neutral formats, are made at or near the time records producers create or capture the records.

The objective of an Electronic Records Survey is to identify three broad categories of electronic records with retention requirements of ten (10) years or more in order to support planning and preservation activities:

- "Preservation Ready" electronic records.
- "Near-Preservation Ready" records, that is electronic records in formats for which tools are available that can export native format documents to open standard interoperable technology neutral formats. An example is Microsoft Word 2007 that contains a tool to transform Word documents into PDF/A format.
- “Legacy” records, that is, electronic records in a proprietary native format for which no export tools exist. Transformation of proprietary native formats into open standard, interoperable, and technology neutral formats is likely to require writing code to support this transformation, which in turn can be costly.

The collection and analysis of data for an Electronic Records Survey can be accomplished by a variety of means including web-enabled surveys of records producers, interviews with selected business units or third parties that routinely create, receive or acquire electronic records, review of records retention and disposition schedules, analysis of the organization’s information technology portfolio, as well as the use of search engines and algorithms to identify specific file formats currently used in the capture and storage of electronic records on network drives.

Capability descriptions for Electronic Records Survey are provided below.

Level	Electronic Records Survey Capability Metrics
0	The organization has little or no capability or resources to collect and analyze information about the volume, location, media, format types, and lifecycle management requirements for electronic records.
1	The organization uses existing retention schedules to identify electronic records of permanent historical, fiscal, and legal value in the custody of records producers. It may also conduct ad hoc, one-time interviews and surveys to identify other electronic records of permanent historical, fiscal, and legal value.
2	The organization uses systematic interviews, surveys, and retrospective analysis of existing retention schedules to identify electronic records of permanent historical, fiscal, and legal value in the custody of select records producers. This effort may be enhanced by focusing on identified "at risk" electronic records.
	ISO 14721 Conformance
3	The organization supplements analysis of "at risk" electronic records through collection of information about the volume and location, media and format types (preservation ready and near-preservation ready) of permanent electronic records in the custody of records producers.
4	The organization has identified and categorized all preservation ready, near-preservation ready, and legacy permanent electronic records in the custody of all records producers.

Digital Preservation Services: Components 9- 15

The DPCMM was designed for organizations and repositories charged with the preservation of long-term and permanent electronic records to benchmark their capabilities against the specifications of ISO 14721, ISO 16363, and digital preservation community accepted practices based upon mapping these capabilities to DPCMM performance metrics. DPCMM uses performance metrics to distinguish between capabilities that rise to the level of OAIS (ISO 14721) conformance and digital preservation infrastructure and services that do not fully conform.

A corollary to the differentiation between surrogate and fully conforming performance metrics is the concept of "significant properties and actions" associated with OAIS information packages (Submission Information Packages -DIPs, Archival Information Packages – AIPs, and Dissemination Information Packages – DIPs that are critical to the preservation of accessible, usable, understandable, and trustworthy long-term and permanent electronic records. "Significant properties" are preservation metadata while actions are digital preservation tasks that must be executed.

The properties are organized into categories:

- Administration (ADM)
- Technical (TEC)
- Provenance (PRO)
- Preservation Description (PRE)
- Content Description (CON)
- Packaging Information (PAC)
- Access (ACC)

Appendix B presents forty-seven significant properties that support the intellectual and technical survival of digital objects along with the associated actions and responsibilities of Records Producers and Respositories. Please refer to this Appendix for additional information.

9. Ingest

A preservation repository that conforms to ISO 14721 functional specifications and associated best practices has the capability to systematically ingest (receive and accept) electronic records from records producers in the form of Submission Information Packages (SIPs).

The preservation repository accepts SIPs from records producers, validates the agreements and integrity of the digital content, moves the SIPs to a staging area where virus checks and content and format validations are performed, transforms electronic records into designated preservation formats as appropriate, extracts metadata from SIPs and writes it to Preservation Description Information (PDI), creates Archival Information Packages (AIPs), and transfers the AIPs to the repository's storage function.

Level	Ingest Capability Metrics
0	The organization does not have a digital preservation repository capable of receiving or ingesting long-term and permanent electronic records.
1	The preservation repository receives electronic records from records producers based on ad hoc agreements without regard to format, integrity, virus checks, and metadata quality. None of this rises to the level of an ISO 14721 conforming SIP.
2	The repository receives surrogate SIPs that are held in a staging area while virus checks and format validations are manually executed. Surrogate AIPs are manually created and transferred to archival storage.
	ISO 14721 Conformance
3	The preservation repository ingests SIPs through **semi-automated means** that validate the completeness of Administration, Technical, Provenance, Content Description, and Preservation Description significant properties. The significant properties are extracted from SIPs and written to Preservation Description Information (PDI). Archival Information Packages (AIPs) are created and transferred to the repository's storage function.
4	The preservation repository ingests SIPs through **automated means** that validate the completeness of Administration, Technical, Provenance, Content Description, and Preservation Description significant properties. The significant properties are extracted from SIPs and written to Preservation Description Information (PDI). Archival Information Packages (AIPs) are created and transferred to the repository's storage function.

10. Archival Storage

The ISO 14721 open archival information system reference model delineates a number of systematic automated storage services that support receipt and validation of successful transfer of AIPs from ingest, creation of Preservation Description Information (PDI) for each AIP that confirms its fixity (i.e., no corruption has occurred) during any preservation actions through the capture and maintenance of error logs, updates to PDI, including transformation (i.e., migration) of electronic records to new formats, multiple instances of geographically separated repositories, production of Dissemination Information Packages (DIPs) for access, and collection of operational statistics.

Archival storage is dependent on other preservation services depicted in the capability maturity model including Device/Media Renewal, Integrity and Security protections, and on the availability and enforcement of Preservation Metadata standards.

Level	Archival Storage Capability Metrics
0	The preservation repository either does not accession electronic records or its holdings consist of primitive archival storage (e.g., a shared drive or CDs/DVDs) where it is available.
1	A single instance of a preservation repository supports the storage of surrogate AIPs with limited metadata that can be mapped to Preservation Description Information (PDI).
2	A single instance of a surrogate preservation repository supports the storage of surrogate AIPs that include manual capture of some significant properties of Administration, Technical, Provenance, and Content Information, and repeatable preservation actions.
	ISO 14721 Conformance
3	A single instance of a preservation repository supports the storage of AIPs. **Semi-automated tools** confirm the completeness of significant properties and capture all properties of repeatable preservation actions. Results are transferred to Preservation Description Information, which constitutes an auditible chain of electronic custody.
4	Two or more geographically-separated instances of a preservation repository support the storage of AIPs. **Automated tools** confirm the completeness of significant properties and capture of all properties of repeatable preservation actions. Results are transferred to Preservation Description Information, which constitutes an auditible chain of electronic custody. Capture of preservation repository storage and operational statistics supports on-going comprehensive digital preservation planning.

11. Media/Device Renewal

There is no known digital device or storage medium that is invulnerable to decay and obsolescence. A foundational digital preservation capability for an organization that has the responsibility to preserve electronic records of long-term and permanent value is ensuring the readability of the bit streams underlying the electronic records. ISO 14721 specifies that a trustworthy digital repository's storage devices and storage media should be monitored and renewed ("replicate"/"repackage") periodically to ensure that the bit streams remain readable over time.

Decay of magnetic and optical storage media is inevitable. Accelerated aging tests predict that most magnetic and optical storage media have a life expectancy of 100 years or more if stored in a controlled environment. However, predicted media life expectancies of hundreds or even thousands of years is of little practical benefit because the fundament issue in device and storage media for a preservation repository is technology obsolescence. This is likely to occur when:

- There is a change in the physical form factor (e.g., from 10.5 inch reels of magnetic tape to tape cartridges)
- There is a change in the method of physically encoding information on the recording surface that makes it impossible to transfer electronic content from an obsolescent tape or disk drive to a contemporary one.
- A vendor decides to discontinue a product
- A legacy system or application is decommissioned without exporting electronic records to the new computing environment.

A preservation repository should support a robust device/storage media renewal program. Depending upon available resources, this renewal program can range from non-network storage devices/storage media, to local network based storage devices/storage media, to external third parties that provide storage services that include device/storage media renewal.

Regardless of how and when device/storage media renewal occurs, a critical requirement is that a protocol is in place that mandates the capture and preservation of the results of periodic validation of the integrity of electronic records before and after completion of device/digital storage renewal.

Capability descriptions for Media/Device Renewal are provided on the next page.

Level	Media/Device Renewal Capability Metrics
0	The preservation repository has no formal device and media renewal protocol in force.
1	The preservation repository mandates device/media renewal when they are on the verge of becoming obsolescent.
2	The preservation repository mandates device/media renewal on a regularly scheduled basis (e.g., every ten years).
	ISO 14721 Conformance
3	The current device and media renewal program supports an annual media inspection program that identifies preservation repository storage media facing imminent catastrophic data loss and executes device/media renewal as appropriate.
4	The current device and media renewal program continuously monitors the potential loss of the readability of electronic records and automatically replaces devices/storage media and writes the records to new storage media as appropriate.

12. Integrity

A key capability in conforming ISO 14721 preservation repositories is ensuring the integrity ("fixity") of records in its custody. Accidental or intentional alterations can occur during device/media renewal, internal data transfers, and other preservation actions. One way to establish integrity is through the use of cryptographic hash digests that are digital fingerprints of electronic records in a SIP, an AIP or some aggregation of them.

A cryptographic hash digest computed before a digital preservation operation and after its completion will detect any changes, even down to a single bit. Hash digests are stored in Preservation Description Information (PDI) where they can be reviewed to confirm that no changes occurred during device/medial renewal, internal data transfers, and other preservation actions, thereby supporting an unbroken chain of electronic custody. The strength of hash digests varies, the lowest being MD5 and the highest is SHA-3.[18]

Hash digests do not support the chain of electronic custody when the preservation action involves format transformation because the underlying bit streams of transformed digital records will not match the bit streams before they were transformed. However, this can be compensated for with the collection of information about all of the preservation actions undertaken with regard to AIPs and storing this information in AIP Preservation Description Information. Affixing a digital signature to AIPs encapsulated in XML after each preservation action also provides a strong electronic chain of custody.

Level	Integrity Capability Metrics
0	The preservation repository has no documented procedure for integrity protection of electronic records in its custody.
1	The preservation repository generates and preserves MD-5 hash digests of electronic records before and after device/media renewal and other archival storage preservation actions.
2	The preservation repository generates and preserves SHA-1 hash digests before and after device/media renewal and other internal preservation actions.
	ISO 14721 Conformance
3	The preservation repository generates and validates **SHA-2 hash digests** before and after all significant properties of repeatable preservation actions for AIPs through **semi-automated means** and stores them in Preservation Description Information (PDI).
4	The preservation repository generates and validates **SHA-2 hash digests** before and after all significant properties of repeatable preservation actions for AIPs through **automated means,** encapsulates them in XML, and signs them with a digital signature. Integrity protection procedures are continuously evaluated and updated as new tools and approaches become available.

[18] In October 2012 the National Institute of Standards and Technology (NIST) selected the algorithm to be used in SHA-3. NIST released the draft specification in April 2014: http://csrc.nist.gov/publications/drafts/fips-202/fips_202_draft.pdf

13. Security

Digital preservation requires processes that restrict access to the physical repository where digital content is stored, ensure the security of electronic records through techniques that block unauthorized access, protect the confidentiality and privacy of records and intellectual property rights, support periodic backup of electronic records that are stored at offsite storage repositories, and support disaster recovery and business continuity.

Level	Security Capability Metrics
0	The preservation repository does not have formal disaster recovery, backups, or firewall procedures in place to protect the security of electronic records.
1	The preservation repository supports the security of electronic records in its custody through disaster recovery procedures.
2	The preservation repository supports the security of electronic records in its custody through a comprehensive firewall protection.
	ISO 14721 Conformance
3	The preservation repository supports the security of electronic records in its custody through comprehensive role-based access rights management.
4	The preservation repository support the security of electronic records in its custody by continuously monitoring security protection processes and revising them in response to evolving technology capabilities and changing business requirements.

14. Preservation Metadata

A preservation repository collects and maintains metadata that describes preservation actions associated with custody of permanent electronic records. Preservation metadata includes an audit trail that documents preservation actions carried out, why and when they were performed, how they were carried out and with what results.

A current best practice is the use of a PREMIS-based preservation metadata schema for all permanent electronic records to support an electronic chain of custody that documents authenticity over time as preservation actions are executed. Capture of all related metadata, transfer of the metadata to any new formats/systems, and secure storage of metadata is critical. All of this associated metadata is stored in the Preservation Description Information (PDI) and logically mapped to AIPs.

Level	Preservation Metadata Capability Metrics
0	A primitive preservation repository has little or no preservation metadata for electronic records in its custody.
1	The preservation repository supports an ad hoc preservation metadata schema and establishes a minimal chain of custody for electronic records in its custody.
2	The preservation repository supports a surrogate PREMIS schema for electronic records in its custody that supports a limited chain of custody.
	ISO 14721 Conformance
3	The preservation repository supports a **semi-automated PREMIS-based schema** for most electronic records in its custody that supports a systematic auditable chain of custody.
4	The preservation repository supports an **automated PREMIS schema** for all electronic records in its custody that supports a systematic auditable chain of custody.

15. Access

The purpose of digital preservation is to ensure that usable, understandable, and trustworthy electronic records are accessible as far into the future as may be necessary, subject to any restrictions imposed by the records producers. Consequently, communities of users should have access to Dissemination Information Packages (DIPs) derived from Archival Information Packages (AIPs) that a trustworthy digital repository properly preserves. In some instances the repository may post unrestricted DIPs on its website. Based upon user expectations and interests, the repository may choose to limit the “significant properties and associated actions” included in DIPs with the understanding that they will be made available if requested.

This access capability may include the creation and maintenance of user searchable retrieval metadata that can be queried to identify information of interest and disclosure free (redacted to protect privacy, confidentiality, and other rights where appropriate). In no instance will users have direct access to Archival Information Packages (AIPs) or Preservation Description Information.

Level	Access Capability Metrics
0	The preservation repository either has no electronic records in its custody or has no capability to support access to electronic records in its custody.
1	The preservation repository supports access to electronic records in a single format (e.g., JPEG or PDF) while enforcing all access restrictions.
2	The preservation repository supports access to electronic records in at least three open standard technology neutral formats (e.g., PDF/A, JPEG, and TIFF formats) while enforcing all access restrictions.
	ISO 14721 Conformance
3	The preservation repository has a robust integrated search functionality that **supports semi-automated production of DIPs** along with their associated significant properties. Auditable documentation for the production of DIPs is captured and user query trends are used to identify the need for updated accessibility tools.
4	The preservation repository has a robust integrated search functionality that supports **automated production of DIPs** and their associated significant properties. User query trends are used to identify the need for updated accessibility tools and audit DIP production results.

4.0 Building a Business Case for Digital Preservation

Increasingly many public and private organizations recognize that systematic management of the lifecycle of their digital assets requires implementation of a program that can assure access to authentic records of long-term value. But competing for the attention of senior management and for the financial and technical resources that will be needed to ensure digital continuity of electronic records is a significant challenge.

We recommend that practitioners leverage standard business planning tools and methods to raise the profile of digital preservation requirements and make the business case for resources and support. These methods are likely to include strategic planning, risk analysis and management, enterprise architecture, technology portfolio management, performance management, benchmarking and funding.

A digital preservation planning framework should identify metrics and incremental capability improvement priorities over a specified period of time. The level of improvement is likely to be shaped by an assessment of "at risk" digital collections and systems as well as available financial, technology and skilled human resources.

The goal of digital preservation planning is to establish and sustain sufficient preservation repositories that conform to the specifications of ISO 14721, the de facto standard, to preserve the organization's long-term records. In most instances, however, it is unlikely that 100 percent conformance with all of the specifications will ever be achieved. Nonetheless, prioritizing digital assets, repositories and transfer needs will help to rationalize investment decisions and engage stakeholders.

4.1 Mission, Vision, Values and Guiding Principles

An organization's mission, vision, values and guiding principles should drive the requirements and duty to preserve electronic records and other digital information assets. The opening sections of a digital preservation business case should focus on issues and risks that are compelling to the audience. Key business drivers (compliance, risk mitigation, cost reduction, institutional memory, etc.) associated with lifecycle management of digital information and assets should be identified early in the document and leveraged throughout the business case to justify a multi-year action plan.

4.2 Regulatory, Legal, Operational and Cultural Memory Environments

An "informed" scan of the regulatory, legal, operational, and cultural memory environment that identifies laws and regulations, standards, best practices, and benchmarks that bear upon long-term access to and protection of electronic records is an essential component. Requirements for this domain are available on various public sector and industry association websites. Many resources in the form of national and international standards, specifications, protocols, and tools also have emerged and can be factored into digital continuity planning exercises and repository service level agreements.

4.3 Information Technology Systems, Platforms and File Formats

A business case for digital preservation requires a working knowledge of the current and planned information technology systems and platforms as well as the file formats used to create and store electronic records (e.g., Electronic Records Survey). This includes an understanding of the functionality of core business applications and document and content management systems that may be required to transfer digital content from an operational environment to a trustworthy digital preservation repository. Decision makers will need to understand which systems and types of records are most likely to be impacted by technology obsolescence to help them focus attention on “at risk” information assets and move forward with the implementation of mitigation strategies and initiatives.

4.4 Strategy and Tactics

Based on each organization’s specific goals and objectives, a strategy to achieve the desired future state of digital preservation capabilities and lifecycle control of its information assets can be developed that take into account both the external and internal requirements and operating environments. This is likely to require dialogue among stakeholders about what constitutes digital preservation that is “good enough” to fulfill the organization’s mission and meet the expectations of its stakeholders within its constrained resources.

4.5 Governance and Accountability

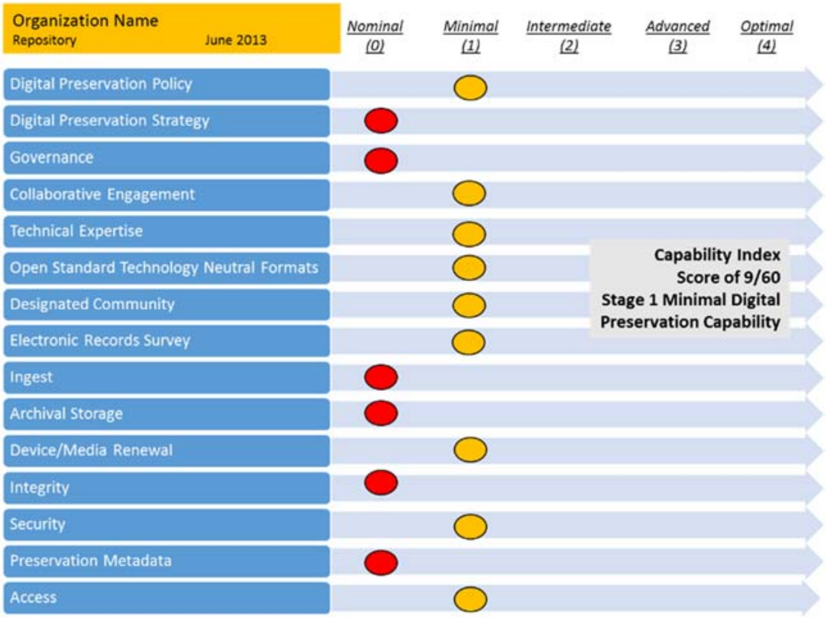
A clear delineation of the roles and responsibilities across the chain of electronic records management for record producers, system administrators, and repository custodians is a fundamental component of sustainable organization-wide information governance. Identification of the roles and responsibilities of current and future internal and external stakeholders is an essential part of a business case for digital preservation.

4.6 Return on Investment

A digital preservation business case should identify a Return on Investment (ROI) in the preservation of information assets over an extended period of time. Typically, this can be defined as Cost Avoidance in mitigating future technology obsolescence, which is the major impediment to access to electronic records as far into the future as required. In this context it is likely that few preservation repositories will ever fully conform to the specifications of ISO 14721. Nonetheless, the planning and justification for the financial and technical resources required for preserving and enabling future access to electronic records over time and technology platforms will provide resource allocators with a stronger sense of the digital preservation value proposition.

4.7 Incremental Digital Preservation Capability Improvement Road Map

Organizations can use the results of a Digital Preservation Capability self-assessment (see Figure 5 below) to develop a roadmap for incremental capability improvement as well as measure their status against peer organizations. The improvement roadmap should take into account both available resources and on-going strategic and tactical business initiatives.



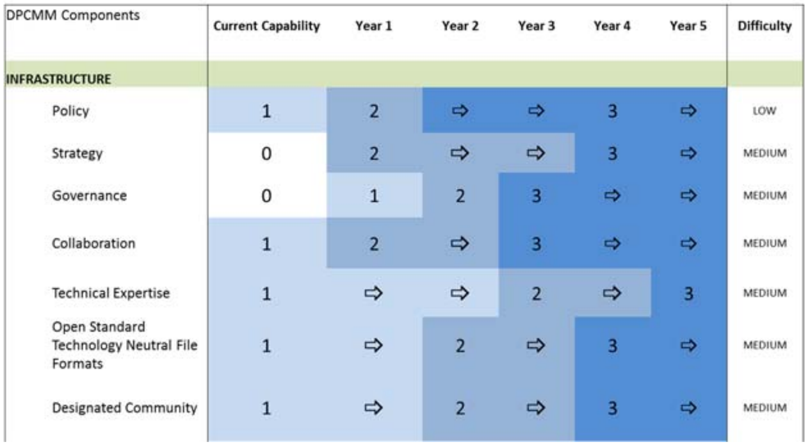
Organization Name Repository June 2013	Nominal (0)	Minimal (1)	Intermediate (2)	Advanced (3)	Optimal (4)
Digital Preservation Policy		●			
Digital Preservation Strategy	●				
Governance	●				
Collaborative Engagement		●			
Technical Expertise		●			
Open Standard Technology Neutral Formats		●			
Designated Community		●			
Electronic Records Survey		●			
Ingest	●				
Archival Storage	●				
Device/Media Renewal		●			
Integrity	●				
Security		●			
Preservation Metadata	●				
Access		●			

Capability Index
Score of 9/60
Stage 1 Minimal Digital
Preservation Capability

Figure 5. Digital Preservation Capability Self-Assessment Scorecard

An important consideration in designing an incremental digital preservation plan that is suited to the organization's mission and designated communities of stakeholders is to mitigate near-term risk exposure for as many of the components as is feasible. It is likely that constrained resources will require the prioritization of some components where significant improvement may be achieved while other components by default may undergo little improvement for the foreseeable future.

Figure 6 on the next page displays a "real world" digital preservation infrastructure improvement plan that maps to the capability results shown in Figure 5. There are two (2) aspects of this improvement plan that should be highlighted. First, at the end of four (4) years each infrastructure capability score has increased to 3, which represents Advanced digital preservation capability. Second, at the time this plan was developed the organization's resources doid not support moving beyond this level.



DPCMM Components	Current Capability	Year 1	Year 2	Year 3	Year 4	Year 5	Difficulty
INFRASTRUCTURE							
Policy	1	2	⇨	⇨	3	⇨	LOW
Strategy	0	2	⇨	⇨	3	⇨	MEDIUM
Governance	0	1	2	3	⇨	⇨	MEDIUM
Collaboration	1	2	⇨	3	⇨	⇨	MEDIUM
Technical Expertise	1	⇨	⇨	2	⇨	3	MEDIUM
Open Standard Technology Neutral File Formats	1	⇨	2	⇨	3	⇨	MEDIUM
Designated Community	1	⇨	2	⇨	3	⇨	MEDIUM

Figure 6. Digital Preservation Infrastructure Improvement Plan

The organization established priorities on when to begin and to implement each infrastructure component. For example, Governance begins with a 0 score and by the end of year 3 it will achieve a Level 3 capability score. In contrast, Technical Expertise begins at Level 1 and will achieve Level 2 by the end of year 3 and Level 3 by the end of year 5. The “Difficulty” column indicates an assessment of the level of effort that may be required to reach level 3 capability.

5.0 Summary

Modern society's reliance on computer networks and born-digital information demands a significant improvement in digital preservation capabilities by nearly all public and private organizations. No longer the exclusive domain of scientists, archivists, and librarians, we believe that standards-based digital preservation requirements and practices should take their rightful place within each organization's information governance framework, records lifecycle management practices, and technology infrastructure.

These capabilities are essential to support the availability, usability, and trustworthiness of electronic records for future and current users in ever changing technology environments. Mitigation of technology obsolescence, of course, is the underlying challenge that robust and sustainable digital preservation capabilities, infrastructure, and services must address.

One of the key benefits of using DPCMM is its ability to assess an organization's current digital preservation capabilities vis-à-vis desired future digital preservation capabilities. Once this assessment is done, organizations can use DPCMM to benchmark against peers and strategically identify incremental improvements in digital preservation capabilities required to fulfill its mission and mandate. Linking investments and improvements in digital preservation capability to risk mitigation and other organizational priorities will help to make a strong business case for incremental improvements.

There is no better time than right now to adopt the prevailing standards and engage with stakeholders to lay the groundwork for long-term digital preservation capabilities. Delays will only make it more difficult and costly in the future to bring lifecycle control over valued information assets and records. We believe that incremental improvement can be achieved with an initially modest outlay of resources. Over time enhanced and sustained capabilities will be required to keep pace with the growing complexity and volume of digital content to be preserved.

Appendix A: Glossary of Terms

Access. The OAIS entity that contains the services and functions which make the archival information holdings and related services visible to Consumers.

Access Rights Information: The information that identifies the access restrictions pertaining to the Content Information, including the legal framework, licensing terms, and access control. It contains the access and distribution conditions stated within the Submission Agreement, related to both preservation (by the OAIS) and final usage (by the Consumer). It also includes the specifications for the application of rights enforcement measures.

Archival Information Package (AIP). An Information Package, consisting of the Content Information and the associated Preservation Description Information (PDI), which is preserved within an ISO 14721 (OAIS) based digital repository.

Authenticity. The degree to which a person, object, activity, or event is what it purports to be. An authentic record is one that can be demonstrated by evidence to be what it purports to be.

Born Digital. Refers to materials that originate in digital form.

Chain of Custody. A formal procedure that documents an information object (e.g., a record) as always being in the custody of an entity (person, system, organization and the like) legally responsible for maintaining the integrity of the object.

Collection. In contrast with archival material, a collection of digital material may share a common purpose but it is brought together from one or more sources without regard for original provenance. A collection can be functionally equivalent to a Record Group in that both represent the highest level of categorization of digital content.

Comma-Separate Values (CSV). A de facto standard for importing and exporting tabular data from spreadsheets and databases. The tabular data consists of rows of plain text (e.g., ASCII) in organized fields (columns) that are delimited by separate by comas, semicolons, or spaces. Rows are considered as data records, each of which has the same sequence of fields.

Compression. A technique to reduce the volume of bits of digital objects being transferred or stored that can be reconstructed at the time of rendering. Typically, compression is associated with digital images and audio and video digital content. There are two forms of compression, lossy and lossless. Lossy references a compression technique that permanently removes some bits that cannot be restored during decompression. Lossless denotes a compression technique that enables restoration of all of the bits during decompression.

Conforming AIPs. See *Appendix B, Recommended Significant Properties of OAIS Information Packages and Associated Actions by Records Producers and Repositories*

Conforming DIPs. See *Appendix B, Recommended Significant Properties of OAIS Information Packages and Associated Actions by Records Producers and Repositories*

Conforming SIPs. See *Appendix B, Recommended Significant Properties of OAIS Information Packages and Associated Actions by Records Producers and Repositories*

Consumer. An OAIS term that is functionally equivalent to user and describes those persons or client sytems who are interested in the holdings of the repository and interact with OAIS services to find preserved information of interest and to access that information in detail. It can include other OAISs as well as internal OAIS persons or systems.

Content Information. The set of information that is the original target of preservation. It is an Information Object comprised of its Content Data Object and its Representation Information. An example of Content Information could be a single table of numbers representing, and understandable as, temperatures, but excluding the documentation that would explain its history and origin, how it relates to other observations, etc.

Cryptograph Hash Algorithm. A mathematical transformation of digital content without regard to its size that reduces it to a fix-length string (e.g., 160 bits) which is called a hash value (sometimes called a message digest, a digital fingerprint, a digest, or a checksum). A cryptographic hash algorithm is relatively easy to reproduce from the original data but it is computationally infeasible to reproduce the original string of data from a hash digest. It is also computationally infeasible that two slightly different strings of data will have the same hash digest. In digital preservation cryptographic hash algorithms play an important role in validating the integrity of digital records by demonstrating that no changes have occurred over time.

Designated Community. An identified group of potential consumers who should be able to understand a particular set of information. The Designated Community may be composed of multiple user communities.

Digital Signature. A cryptographic technique for creating a bit stream that can be affixed to a document (or any other digital object) and thereby attest to its authenticity. A digital signature includes a private key that is known only to its owner and a reciprocal public key that can be made available to anyone. A digital object signed with a private key can only be validated by its reciprocal public key. It is computationally infeasible for anyone to generate a valid digital signature that does not possess the private key. It is computationally infeasible to create a private key from a public key.

Disclosure-free. Associated with a copy of a record that contains no personally identifiable information (e.g., a Social Security Number) or otherwise restricted access information. *See Redacted.*

Dissemination Information Package (DIP). The Information Package, derived from one or more AIPs, received by the Consumer in response to a request to the ISO 14721 (OAIS) based digital repository.

DoD 5015.2 Criteria for Electronic Records Management Software Applications. A standard that specifies mandatory and optional baseline functional requirements for records management application software employed in the Department of Defense. DoD 5015.2 certification means that a records management software application has passed received formal certification that it conforms to these specifications. Since its introduction, DoD 5015.2 has become a de facto standard for electronic records management applications.

Dublin Core. An international standard (ISO 15836), Dublin Core defines metadata elements that describe and support on-line access to material. It consists of 15 elements: title, creator, subject, description, publisher, contributor, date, type, format, identifier, source, language, relation, coverage, and rights.

Electronic Record. Any combination of text, graphics, data, audio, pictorial or other information representation in digital form set aside for future reference that is created, used, modified, stored, and retrieved by a computer application/system.

Encapsulation. A technique for placing digital records and associated metadata in a container or wrapper that can be manipulated or transmitted without regard to what the wrapper contains. XML supports the use of Document Type Definitions in wrappers that separate logical structures (i.e. content structure) from their rendered physical representations.

Extensible Markup Language (XML). XML is a World Wide Web Consortium (W3C) standard for marking up text based documents that are interoperable. Interoperability is achieved through the assignment of tags (Document Type Definition) to the logical structure of text based digital content and the use of a Style Sheet for rendering the content into human readable form. A Document Type Definition assigns tags that define the logical and semantic structure of text based documents. In the context of DPCMM XML can be considered a "preferred preservation format."

Fixity of Information. The information which documents the authentication mechanisms and provides authentication keys to ensure that the Content Information object has not been altered in an undocumented manner.

Form of Material. Form of material is not equivalent to format but rather it conveys the type of content in a digital record. Current forms of digital material include but are not limited to books, reports, letters, memos, correspondence, photographs, email, maps, spreadsheets, graphics, database, audio, moving images, web pages, and social media.

Format. A wrapper for the 1s and 0s of bit streams that underlie electronic records. It specifies how the 1s and 0s are encoded and how they are to be interpreted. Typically, the extension to electronic content denotes the format used (e.g., TXT for ASCII Text, PDF for Portable File Format).

Format Validation. The process that identifies the format of electronic records and confirms that the format used conforms to its formal published specifications.

Hyper Text Markup Language (HTML). HTML is a mark-up (i.e., tags) language initially designed (1990) for creating interoperable text, image, and audio digital context for web browsers. In 2000 it became an international standard: ISO 15445:2000.

Information Package. The Content Information and associated Preservation Description Information which is needed to aid in the preservation of the Content Information. The Information Package has associated Packaging Information used to delimit and identify the Content Information and Preservation Description Information.

Information Governance. Decision rights and an accountability framework to encourage desirable behavior in the valuation, creation, storage, use, archival and deletion of information. Information governance includes processes, roles, standards and metrics that ensure effective and efficient use of information in enabling an organization to achieve its goals.

Ingest. The OAIS entity that contains the services and functions that accept Submission Information Packages from Producers, prepares Archival Information Packages for storage, and ensures that Archival Information Packages and their supporting Descriptive Information become established within to the ISO 14721 (OAIS) based digital repository.

Internal and External Stakeholders. A digital preservation stakeholder is any organization or individual who can affect or is affected by digital preservation policy, strategy, initiatives, or projects. Broadly speaking, internal references individuals/organizations inside an organization while external references individuals/ organizations outside the organization. ISO 14721 references internal and external stakeholders under the rubric “Defined Community.”

Interoperable File Format. *See Open Standard Technology Neutral Format*.

Joint Photographic Experts Group 2000 (JPEG 2000). JPEG 2000 is an international standard (ISO 15444-1) that supports both lossy and lossless compression of digital photographic images. In the context of the Digital Preservation Capability Model it can be a “preferred preservation format.”

Legacy Electronic Records. Legacy electronic records are embedded in obsolete software or formats with no backward compatibility or export function to newer software and formats. Legacy records can only be retrieved and rendered by the software application and/or format in which they are embedded or by a viewer. Typically, computer code must be written to transform legacy records into newer, technology neutral open file formats.

Long-Term. A period of time long enough for there to be concern about the impacts of changing technologies, including support for new media and data formats, and of a changing user community, on the information being held in a repository. This period extends into the indefinite future.

Long-Term Preservation. The combined actions of a preservation repository to ensure that electronic records are accessible, usable, understandable, and trustworthy over technology generations for as long as may be required.

Moving Pictures Expert Group-4 (MPEG-4). MPEG-4 is an International Standard (ISO 14496) for the compression of digital audio content. In the context of the DPCMM it can be considered a “preferred preservation format.”

Metadata. Metadata is data (information) about data (information), which is technically correct but simplistic because metadata may serve several purposes in information systems. Descriptive metadata facilitates the search and retrieval of information objects. Administrative metadata supports the management and tracking of information objects. Structural metadata denotes how complex information objects can be reassembled for rendering. Preservation metadata supports activities that ensure the accessibility, usability, understandability, and authenticity of information objects.

Migration. In ISO 14721 migration references actions associated with the transfer of digital content within an ISO 14721 conforming preservation repository. In this context, there are four different actions that may be undertaken. *See Refreshment, Replication, Repackage, and Transformation.*

Motion Joint Photographs Engineering Group (Moving JPEG 2000). Motion JPEG 2000 (MJPEG 2000) is an International Standard (ISO 15444-3) for lossless compression of each video frame in a digital video sequence separately as a JPEG image.

Native File Formats. Native file formats are proprietary formats specific to a software application used to create, store, save, and retrieve electronic records. They are not interoperable in the sense that digital objects embedded in proprietary native file formats can only be "recognized" and opened by the software application used to create and save them unless the software supports an explicit import/export functionality.

Near-Preservation Ready Information. Near preservation ready digital information is encoded in a native, proprietary format but tools exist that can transform it into a technology neutral open standard format. An example is the transformation of Word documents to PDF/A. Some additional processing may be required to assemble the appropriate metadata.

Open Archival Information System (OAIS). An archive, consisting of an organization of people and systems that has accepted the responsibility to preserve information and make it available for a Designated Community. It meets a set of responsibilities, as defined in 3.1 of the ISO 14721:2003 standard that allows an OAIS archive to be distinguished from other uses of the term 'archive'. The term 'Open' in OAIS is used to imply that this Recommendation and future related Recommendations and standards are developed in open forums, and it does not imply that access to the archive is unrestricted.

Open Document Format (ODF). ODF is an International Standards Organization standard, ISO 26300:2000. It is an XML (markup language) standard for creating interoperable office documents, including text, spreadsheets, presentations, and charts.

Open Standard Technology Neutral Format. A technology neutral file format is one that is designed to run on multiple platforms in a variety of software applications. It is an open file format in that the design of the specification involves collaboration in an open, public environment. Open standard technology neutral open file formats can evolve as technology changes and thereby provide a backward compatibility to older versions. Examples of open standards technology neutral file formats are XML and PDF/A.

Persistent Identifier. A unique identification code (numeric and/or character string) that is intended to enable a permanent, unambiguous link to individual digital objects. Once a persistent identifier is assigned to a digital object, it is forever linked to the object. Interoperability of Persistent Identifier (PI) systems is an on-going issue in digital preservation.

Plain Text. Plain text is textual material encoded in American Standard Character Interchange (ASCI) without regard for its appearance when rendered. Essentially, plain text is a string of alphanumeric characters with minimal formatting – for example, upper case, lower case, space, spacing, carriage return, $, and * along with alphabetic characters and numbers 0 – 9 among others. Each character is assigned a specific decimal value (A = 65) and a binary value (01000000). Because Plain Text has no formatting functionality like word processing applications, it is interoperable on virtually any technology platform and can be rendered by any text editor.

Portable Network Graphic (PNG). PNG (ISO 15948) is an interoperable international standard lossless compression algorithm for raster images. Among other things, it supports 48 bits of true color and 16 bits per pixel for grayscale raster images.

Preservation Description Information (PDI). A component of Archival Storage in an ISO 14721 conforming repository, PDI contains metadata that is necessary for adequate preservation of the Content Information and which can be categorized as Provenance, Reference, Fixity, and Context information.

Preservation Metadata Implementation Strategy (PREMIS). PREMIS is a standard developed by the Library of Congress that enables designers, managers, and practitioners of digital repositories to have a clear understanding of what a digital preservation system needs in order to execute digital preservation functions. One way this is accomplished is through a Data Dictionary that defines uniform attributes that support an electronic chain of custody that documents the integrity over time as preservation actions are executed.

Preservation Ready Information. Preservation ready information is encoded in a technology neutral open standard format and all necessary metadata has been assembled so that it can be moved (i.e., ingest) into a digital preservation repository with little or no additional processing.

Producer. An OAIS term that describes external individuals, groups, and client systems which create and use electronic information that must be preserved. Producers can include other OAISs or internal OAIS persons or systems.

Redaction. Historically, redaction describes the process of altering multiple documents slightly and combining them into a single document. Its contemporary meaning refers to concealing content from unauthorized review by obscuring or otherwise deleting specific information that is protected by privacy, proprietary, or national security considerations. Redacted documents are also known as "Disclosure Free."

Refreshment. Refreshment is an ISO 14721 migration activity that references a media instance holding one or more AIPs that is replaced by a media instance of the same type by copying the bits underlying the AIPs. There is no change in Packaging Content, Content Information, Preservation Description Information, and the Archival Storage mapping information or the underlying bit stream of the AIPs information objects

Repackage. Repackage is an ISO 14721 migration activity in an instance in which the replacement of current storage media with different storage media causes in the Content Information and Preservation Description Information. However, there is a change in the bit stream underlying Packaging Information.

Replication. Replication is an ISO 14721 migration activity in which the replacement of storage media of the same type or a new type causes no change in the Content Information and Preservation Description Information. However, there could be a change in the Packaging Content bit streams.

Significant Properties (SIP, AIP, and DIP). Attributes of conforming ISO 14721 Information Packages and digital preservation community best practices. *For more information see Appendix B.*

Storage Tier Level. Storage tier levels reference the assignment of different categories of data to different types of storage media in order to reduce total storage cost. Categories may be based on levels of protection needed, performance requirements, frequency of use, and other considerations. Storage tier level considerations will play an increasingly important role when a digital repository has a large volume of digital content (e.g., Terabytes), some of which is accessed frequently and some which is infrequently or not accessed at all.

Submission Agreement: The agreement reached between an OAIS and the Producer that specifies a data model for the Data Submission Session. This data model identifies format/contents and the logical constructs used by the Producer and how they are represented on each media delivery or in a telecommunication session.

Submission Information Package (SIP): An Information Package that is delivered by the records producer to the OAIS for use in the construction of one or more AIPs.

Scalable Vector Graphics (SVG). SVG is a World Wide Consortium (W3C) XMD-based markup that supports interoperable two-dimensional vector graphic images. In the context of DPCMM it can be considered a "preferred preservation format."

Surrogate. Surrogate is used in DPCMM discussion materials to denote a repository, tool or service used for the preservation of long-term or permanent electronic records that does not fully conform to the specifications in the ISO 14721 reference model.

Technology Watch Program. Programs such as the United Kingdom National Archives PRONOM program and the Library of Congress Sustainability of Digital Formats Web Site that encompass a variety of tools, and services to support digital preservation functions such as preservation risk assessment, file format sustainability, migration planning, and metadata extraction, among others.

Tagged Image File Format (TIFF). TIFF is an interoperable de facto standard widely used in the capture and storage of digital images. In the context of DPCMM it can be considered a "preferred preservation format."

Type of Transmission. Identification of the means of transfer from a records producer to a preservation repository.

Transformation. Transformation is an ISO 14721 migration activity associated with replacing current interoperable formats with new interoperable formats to mitigate format obsolescence. There will be changes in the underlying bit streams of Packaging, Information Content, and Preservation Description Information. The resulting AIP is intended to replace the existing AIP.

Trustworthy Digital Repository. In ISO 14721 a trusted digital repository is committed to provide long-term access to managed digital resources; accepts responsibility for the long-term maintenance of digital resources on behalf of its depositors and for the benefit of current and future users; designs its system(s) in accordance with commonly accepted conventions and standards to ensure the ongoing management, access, and security of materials deposited within it; establishes methodologies for system evaluation that meet community expectations of trustworthiness; can be depended upon to carry out its long-term responsibilities to depositors and users openly and explicitly; and whose policies, practices, and performance can be audited and measured.

Trustworthy Records. Trustworthy electronic records are reliable and authentic records whose integrity has been preserved over time. Reliability references that records can be trusted as an accurate representation of the activities and facts associated with a transaction(s) because they were captured at or near the time of the transaction. Authenticity means that electronic records are what they purport to be.

Web ARChive (WARC). WARC is an interoperable international standard (ISO 28500) for harvesting, accessing, and exchanging digital content over the Web. In the context of DPCMM it can be considered a “preferred preservation format.”

Appendix B: Recommended Significant Properties of OAIS Information Packages and Associated Actions by Records Producers and Repositories

Background

The Open Archival Information System (OAIS) Reference Model uses the concept of information packages as logical containers for electronic information (content information and associated metadata) that a repository preserves. The concepts of Submission Information Packages (SIPs), Archival Information Packages (AIPs), and Dissemination Information Packages (DIPs) are used to distinguish between digital objects that a trusted repository receives from a records producer and the actual digital objects that it preserves and subsequently makes available to its Designated Community of users.

Digital assets appraised[19] to have long-term value come into an ISO 14721 conforming preservation repository through Submission Information Packages that include the digital content (i.e., the electronic records) and specified metadata values, especially technical packaging information. After processing that validates and characterizes the digital content and captures additional metadata, the repository accepts the SIPs and transforms them into Archival Information Packages (AIPs).[20] Initially, AIPs contain all of the SIP content plus any other metadata captured as part of the transfer to Archival Storage but over time other metadata is added that documents any action taken that affects the content of the AIP. These actions include but are not limited to device-media renewal and format transformation as new, interoperable, open–standard, technology-neutral formats displace existing ones. DIPs, which can be produced on-demand or published to a website for 24/7 access, contain information in selected AIPs plus information that documents how users can identify and access digital resources of interest to them.

ISO 14721 and ISO 16363 specify that SIPs, AIPs, and DIPs should meet minimum requirements for completeness but only do this for a handful of metadata properties, such as evidence of authenticity, accepted naming conventions, access restrictions and enforcement requirements, and persistent unique identifiers. Presumably, the digital preservation community must draw upon its expertise and experience to flesh out these complete properties.

[19] Preparation of appraisal reports that assign long-term value to digital assets are outside the scope of these significant properties.

[20] It is likely that there will be instances when the SIP to AIP relationship is not 1 to 1, especially when multiple SIPs may be integrated into a single AIP.

Our Perspective

The recommendations in this Appendix represent our contribution to this evolving discussion and are intended to serve two purposes: 1) advance an understanding of what SIP, AIP, and DIP metadata properties are significant[21] for trusted repositories that conform to the OAIS requirements, and 2) identify these properties in such a way that they can be incorporated into DPCMM performance metrics in the next major update (2016).

These recommended properties are drawn from a variety of sources including InterPARES Project 3, General Study 15 – Application Profile for Authenticity Metadata,[22] Dublin Core elements, Archivematica digital preservation metadata called significant characteristics,[23] Preservica[24] digital preservation significant properties, the Tufts University SIPs prototype project,[25] and accepted digital preservation community good practices, such as those described in "Preservation Metadata (2nd edition),"[26] and the "Planets Report on policy and strategy models for libraries, archives, and data centres."[27] A peer review panel offered their perspectives on the recommended significant properties.[28]

Key Terms

On the following pages, a description of requirements and a table of forty-seven significant properties and actions are provided for OAIS Information Packages (SIP, AIP and DIP). This material employs several key terms that require some discussion.

Accuracy

The accuracy[29] of the content of digital objects in SIPs is presumed when agents of records producers created, used, and filed official working papers or records in the ordinary course of business in accordance with office protocols (e.g., review and or concurrence by an authoritative

[21] In 2008 Andrew Wilson of the National Archives of Australia identified digital preservation metadata that he called "significant properties." He defined "significant properties" of records as digital preservation metadata "that must be preserved over time in order to ensure the continued accessibility, usability, and meaning of the objects, and their capacity to be accepted as evidence of what they purport to record." See "Significant Properties of Digital Objects," JTSC Significant Properties Workshop, April 7, 2008, available under Previous Events at http://www.dpconline.org/events/previous-events?start=75.
[22] Available at www.ip3_metadata_application_profile_final_report.pdf.
[23] Archivematica is a free open source digital preservation system (www.archivematic.org).
[24] Preservica is a commercial digital preservation system (www.preservica.com).
[25] Available at http://dca.tufts.edu/features/nhprc/reports/ingest/index.html.
[26] Brian Lavoie and Richard Gartner, a *DPC Technology Watch Report 13-03 May 2013.* Available at http://dx.doi.org/10.7207/twr13-03.
[27] Available at www.ip3_metadata_application_profile_final_report.pdf.
[28] We acknowledge and appreciate valuable feedback received from a panel of peers that included: Carol Brock, Jelain Chubb, Kevin DeVorcey, Ric Ferrante, Karen Horsfall, Carol Kussmann, Veronica Martzahl, Glenn McAnich, Julia McLeod, Mark Myers, Richard Pearce-Moses, Corrine Rogers, Pauline Sinclair, and Caryn Wojcik. Their participation in the panel review should not be construed as endorsing the content of Appendix B. The authors are solely responsible for any factual errors, incorrect interpretations, and conclusions in Appendix B.
[29] The InterPARES Glossary defines accuracy as "The degree to which data, information, documents or records are precise, correct, truthful, and free of error or distortions." The glossary is available at www.interpares.org/

third-party or acceptance by the recipient of the working papers or records). The accuracy of significant properties means that they have been validated against a reliable source. Such sources can include an official list of the names of records producers, a convention for specifying dates, technical registries (e.g., PRONOM), to name only a few.

AIPs inherit (*see Inheritance discussion below*) all of the SIP significant properties that the trusted repository has confirmed and accepted. Those significant properties that are unique to AIPs (e.g., preservation activities like device/medial renewal, file format transformation, and the like) require the trusted repository to document their accuracy.

DIPs may inherit all of the significant AIP properties plus the significant properties unique to access. In fact, some users may choose to receive DIPs that contain only a limited set of significant AIP properties while others may choose a larger set.

Completeness

Like accuracy, the completeness[30] of digital objects in SIPs is presumed when agents of records producers created, used, and filed official working papers or records in the ordinary course of business in accordance with office protocols (e.g., review and or concurrence by an authoritative third-party or acceptance by the recipient of the working papers or records). Completeness of significant properties means that all of the characteristics specified in adopted metadata schemas are present.

Inheritance

There are two aspects of inheritance, explicit and implicit. The latter occurs when one or more properties are "nested" under a higher level property as in the instance of hierarchical relationships such as parent, children, siblings, and the like. For example, a file folder can inherit all of the attributes of a record series. Explicit inheritance occurs when non-relational significant properties of SIPs that the trusted repository has confirmed and accepted are transferred to AIPs and DIPs (as appropriate). In this instance the function of inheritance is to ensure that significant properties accompany the respective digital objects from Ingest to Archival Storage to Access.

Repeatability

Repeatability conveys the notion that preservation activities in Archival Storage employing the same methods may recur as many times as may be required. Two instances readily come to mind that involve repeatable actions over time: the renewal of digital storage devices and media and transformation of older file formats to newer ones. Associated with some preservation actions is the execution of hash algorithms before and after each preservation action to validate

[30] The InterPARES Glossary defines completeness as "The characteristic of a record that refers to the presence within it of all the elements required by the creator and the juridical system for it to be capable of generating consequences."

the integrity of SIPs, AIPs, and DIPs. Other preservation actions may include adding new content description information or changes to registries of unique persistent identifiers.

The forty-seven significant properties for SIPs, AIPs, and DIPs listed in the tables that follow provide a high level logical preservation metadata framework that must be implemented with schemas, naming conventions, rules, and workflows, among other considerations in a trusted repository environment, that are outside the scope of this white paper. Wherever possible the schemas, naming conventions, rules, and workflows should conform to the specifications of PREMIS and ISO 28301-2: 2009 Information and Documentation - records management processes – Metadata for records – Part 1: Conceptual and implementation. Schemas, naming conventions, rules and workflows can be adapted to the specific requirements of each trusted repository.

Submission Information Packages (SIPs)

A trusted repository that conforms to ISO 14721 functional specifications and ISO 16363 audit criteria and associated good practices must have the capability to systematically ingest (receive and process) digital content from records producers in the form of Submission Information Packages (SIPs). SIPs should have "complete" information properties and associated actions for five components: Administration (ADM), Technical (TEC), Provenance (PRO), Preservation Description (PRE), Content Description (CON), and Packaging Information (PAC).[31]

The following table lists thirty-four recommended significant properties for SIPs that are organized by responsibility and component (e.g., ADM, TEC, etc.) Four of the significant properties and actions are mapped to two components: PRO-2/ADM-2, PRO-3/ADM-3, CON-1/TEC-7, and CON-3/ADM-3. These are logical linkages and therefore used more than one time. Note that the properties identify whether the record producer or the repository has the responsibility for creating or validating the information content of these properties.[32]

Records producers are responsible for creating and capturing all but ten of these properties while the Repository is responsible for creating and capturing metadata for these ten properties and confirming the accuracy and completeness of the remaining significant SIP properties. In the short run records producers may be unable or unwilling to consistently provide this level of detail about SIPs. Packaging information is a case in point. Therefore, the repository will have to take on this task.

The volume and complexity of digital records that repositories are likely to receive in the future is such that fully automated ingest tools must be adopted that require little if no human intervention. Of course some repositories may decide that a subset of the SIP significant properties is "good enough" or that only certain records are of sufficient value and/or interest to merit capture of all of the significant SIP properties.

[31] These five categories are derived in part from based on principles of ISO 14721 and ISO 16363 and the Lavoie and Gartner, *DPC Technology Watch Report*. A sixth component, Access, is included in the DIPs preservation metadata and actions.

[32] The primary responsibilities for Records Producers represent an ideal environment that may not exist in every instance of receiving and processing SIPs. In such instances preservation repositories will have to determine which, if any, missing SIP significant properties they will provide.

Submission Information Packages from Records Producers to an ISO 14721 Preservation Repository

SIP Categories of Significant Properties and Actions	Records Producer Responsibilities for Metadata Properties and Associated Actions	Trusted Repository Responsibilities for Metadata Properties and Associated Actions
Administration (ADM)	ADM-1 Submission Information Agreement including terms binding on both parties	ADM-1 Confirmation of completeness and accuracy of Submission Information Agreement terms
	ADM-2 Name of Record Producer that created and used the Records	ADM-2 Confirmation of completeness and accuracy of Name of Record Producer that created and used the Records
	ADM-3 Name of the Business Unit, Function, or other Entity that had custody of the Records at transfer	ADM-3 Confirmation of the Name of Business Unit, Function, or other Entity that had custody of the Records at transfer
	NA	ADM-4 Accession Number and Date of Transfer
	ADM-5 Evidence of Transfer of legal custody to the archives, including date and authority	ADM-5 Confirmation and acceptance of the completeness and accuracy of the Evidence of of Tansfer of Legal Transfer
	ADM-6 Rights, Privacy, Restrictions	ADM-6 Confirmation of completeness and accuracy of Rights, Privacy, Restrictions
Technical (TEC)	TEC-1 Type of Transmission	TEC-1 Confirmation of completeness and accuracy of Type of Transmission
	NA	TEC-2 Declaration of Virus and Malware Free
	TEC-3 Number of bytes (MB/GB/TB)	TEC-3 Confirmation of Number of bytes (MB/GB/TB)
	TEC-4 Number of files	TEC-4 Confirmation of completeness and accuracy of Number of files
	TEC-5 Format type(s)	TEC-5 Confirmation of accuracy of Format type(s)
	TEC-6 Hash digest of transferred digital objects	TEC-6 Confirmation and acceptance of Hash digest of transferred digital objects
	NA	TEC-7 Assign unique Persistent Identifier (PI)
	TEC-8 Name of software and operating system used to create, use, and store the digital records	TEC-8 Confirmation and acceptance of the Name of software and operating system used to create, use, and store the digital records
	TEC-9 Form of material	TEC-9 Confirmation of Form of material

SIP Categories of Significant Properties and Actions	Records Producer Responsibilities for Metadata Properties and Associated Actions	Trusted Repository Responsibilities for Metadata Properties and Associated Actions
Provenance (PRO)	PRO-1/ADM-2 Name of Records Producer that created and used the Records	PRO-1/ADM-2 Confirmation and acceptance of the completeness and accuracy of the Name of the Record Producer that created and used the Records
	PRO-2 Capture of Archival Bond (e.g, record classification code, record retention schedule item, or Donor name)	PRO-2 Confirmation and acceptance of Archival Bond (e.g., record classification code, record retention schedule it, or Donor name)
	PRO-3/ADM-3 Name of Business Unit, Function, or other Entity that had custody of the records at transfer	PRO-3/ADM-3 Confirmation and acceptance of Name of Business Unit, Function, or other Entity that had custody of the records at transfer
	PRO-4A Hierarchical Relation – Level 1 Name and description of Business Function/ Organization/ Collection	PRO-4A Confirmation and acceptance of Hierarchical Relation Name and description of Business Function/ Organization/ Collection
	PRO-4B Hierarchial Relation – Level 2 Name and description of Series Content *(Appropriate)*	PRO-4B Confirmation and acceptance of Hierarchial Relation – Level 2 Name and description of Series Content *(As Appropriate)*
	PRO-4C Hierarchial Relation – Level 3 Name and description of Folder Content *(As Appropriate)*	PRO-4C Confirmation and acceptance of Hierarchical Relation – Level 3 Name and description of Folder Content *(As Appropriate)*
	PRO-4D Hierarchial Relation Level 4 Name and description of items *(As Appropriate)*	PRO-4D Confirmation and acceptance of Hierarchial Relation Level 4 Name and description of items *(As Appropriate)*
Preservation Description (PRE)	NA	PRE-1 Preservation action (e.g., storage device/media renewal, format transformation, creation of AIPs, transfer to Archival Storage, among others)
	NA	PRE-2 Name of agent/entity responsible for the preservation action
	NA	PRE-3 Date of preservation action
	NA	PRE-4 Declaration of successful completion of preservation action
	NA	PRE-5 Integrity validation (hash digest) before and after preservation action

SIP Categories of Significant Properties and Actions	**Records Producer Responsibilities for Metadata Properties and Associated Actions**	**Trusted Repository Responsibilities for Metadata Properties and Associated Actions**
Content Description (CON)	NA	CON-1/TEC-7 Capture of Persistent Identifier in the data object and system file registry
	CON-2 Time Coverage of Records	CON-2 Confirmation and acceptance of Time Coverage of Records
	CON-3/ADM-2 Name of Record Producer that created and used the Records	CON-3/ADM-2 Confirmation of Name of Record Producer that created and used the Records
	CON-4 Name of Contributor and/or Creator (Author)	CON-4 Confirmation and acceptance of name of Contributor and/or Creator (Author)
	CON-5 Brief description of digital content along with subjects, topics, and other relevant information	CON-5 Brief description of digital content along with subjects, topics, and other relevant information
Packaging Information (PAC)	PAC-1 Identification of all files and their structure/relationships in the SIP	PAC-1 Capture or confirmation of completeness of identification of all files and structure/relationships in the SIP
	PAC-2 Create pointers to other relevant physical or virtual Administration, Technical, Provoance, Preservation Description, and Content Description metadata	PAC-2 Capture or confirmation of completeness of pointers to other relevant physical or virtual Administration, Technical, Provenance, Preservation Description, and Content Description metadata

Archival Information Packages (AIPs)

When SIPs are converted to Archival Information Packages they inherit all of the preservation metadata identified in the previous table (Administration, Technical Information, Provenance, Preservation Description, Content Description, and Packaging Information). Additional metadata (e.g., transformation of the formats of digital objects in SIPs to an acceptable open standard technology neutral format) will be captured as part of the transfer to Archival Storage.

Over time additional metadata is added to AIPs that document any action taken that affects the significant properties. These actions include but are not limited to device/media renewal and format transformation as new open standard technology neutral formats displace existing ones. Note that all but six of the thirty-five AIPs significant metadata properties and actions are inherited from SIP metadata attributes and require no additional input from the Repository.

The AIP significant properties that the Repository is responsible for encompass all of the internal digital preservation actions associated with a trusted repository, including but not limited to repackaging and renewing digital/device storage, transforming accepted preservation file formats to newer ones as they are displaced, and computing hash digests before and after any digital preservation activity is undertaken. All of these significant properties of digital preservation actions constitute an “electronic chain of custody,” which is a reliable tool for ensuring the authenticity of digital records over time and technological change. In addition, AIPs are considered “dark AIPs” in that they will never be accessible to the Designated Community of users. Only copies of unrestricted AIPs or DIP extracts from the AIPs will be accessible.

Archival Information Packages Created and Maintained by an ISO 14721 Preservation Repository

AIP Categories of Significant Properties and Actions	Records Producer Responsibilities for Metadata Properties and Associated Actions	Trusted Repository Responsibilities for Metadata Properties and Associated Actions
Administration (ADM)	NA	ADM-1 Inherited confirmation of completeness and accuracy of Submission Information Agreement terms
	NA	ADM-2 Inherited confirmation of completeness and accuracy of Name of Record Producer that created and used the Records
	NA	ADM-3 Inherited confirmation of Name or Business Unit, Function, or other Entity that had custody at transfer
	NA	ADM-4 Inherited confirmation of Accession Number and Date of Transfer
	NA	ADM-5 Inherited confirmation of Evidence of Completeness of Legal Transfer
	NA	ADM-6 Inherited confirmation of Completeness of Rights, Privacy, Restrictions
Technical (TEC)	NA	TEC-1 Inherited confirmation of Completeness of Type(s) of Transmission
	NA	TEC-2 Inherited confirmation of Virus Malware Free
	NA	TEC-3 Inherited confirmation of Number of bytes (MB/GB/TB)
	NA	TEC-4 Inherited confirmation of Number of files
	NA	TEC-5 Inherited confirmation of Format Type(s)
	NA	TEC-6 Inherited confirmation of Integrity Validation (hash digest)
		TEC-7 Inherited confirmation of Persistent Identifier
	NA	TEC-8 Inherited confirmation of Name of software and operating system used to create, use, and store records
	NA	TEC-9 Inherited confirmation of Form of material
Provenance (PRO)	NA	PRO-1/ADM-2 Inherited confirmation of Name of the Record Producer
	NA	PRO-2 Inherited confirmation of Archival Bond
	NA	PRO-3/ADM-3 Inherited confirmation of name of Business Unit, Function , or other Entity that had custody of the records at transfer

AIP Categories of Significant Properties and Actions	Records Producer Responsibilities for Metadata Properties and Associated Actions	Trusted Repository Responsibilities for Metadata Properties and Associated Actions
	NA	PRO-4A Inherited confirmation of Hierarchicial Relation Level 1 Name and description of Business Function/ Organization/ Collection
	NA	PRO-4B Inherited confirmation of Hierarchial Relation Level 2 Name and description of Series Content (*As Appropriate*)
	NA	PRO-4C Inherited confirmation of Hierarchial Relation Level 3 Name and description of Folder Content (*As Appropriate*)
	NA	PRO-4D Inherited confirmation of Hierarchial Relation Level 4 Name and description of Item *(As Appropriate)*
Preservation Description (PRE)	NA	PRE-1 Cumulative transaction history of preservation action (e.g., storage device/media renewal, format transformation, creation of AIPs, transfer to Archival Storage, among others) - Repeatable
	NA	PRE-2 Cumulative transaction history of the agent/entity responsible for the preservation actions – Repeatable
	NA	PRE-3 Cumulative transaction history of date of preservation actions - Repeatable
	NA	PRE-4 Cumulative transaction history of successful completion of preservation actions - Repeatable
	NA	PRE-5 Cumulatve transaction history of Integrity Validations (hash digest) before and after preservation actions- Repeatable
	NA	PRE-6 Cumulative transaction history of periodic random samples of of integrity validations (hash digest) of AIPs - Repeatable
Content Description (CON)	NA	CON-1/TEC-7 Inherited Persistent Identifier
	NA	CON-2 Inherited confirmation of Time Coverage of Records
	NA	CON-3/TADM-2 Inherited confirmation of Name of Record Producer that created and used the Records
	NA	CON-4 Inherited confirmation of name of Contributor and/or Creator (Author)
	NA	CON-5 Brief description of digital content along with subjects, topics, and other relevant information

AIP Categories of Significant Properties and Actions	Records Producer Responsibilities for Metadata Properties and Associated Actions	Trusted Repository Responsibilities for Metadata Properties and Associated Actions
Packaging Information (PAC)	NA	PAC-1 Inherited confirmation of completeness of pointers to other physical or virtual Administration, Technical, Provenance, Preservation Description, and Content Description metadata
	NA	PAC -2 Inherited confirmation of completeness of pointers to other relevant physical or virtual Administration, Technical, Provenance, Preservation Description, and Content Description metadata

Dissemination Information Packages (DIPs)

The mission of a digital preservation repository is to ensure future access to trustworthy, understandable and usable information contained in AIPs in its custody. This access functionality includes presenting to users the Provenance and Preservation Description metadata inherited from Archival Information Packages. In addition, there are twelve specific access significant properties and actions that support a robust access program for a Designated Community of users along with the capture of information about requested DIPs that support repository statistical reporting and digital preservation planning.

The delivery of DIPs presumes that a robust search engine is in place that supports browsing and retrieval of both metadata properties and full text of digital objects, and can filter for narrower and broader searches. Many users are unlikely to have an interest in Administration, Technical, and Packaging Information so they can be routinely hidden from view for search and retrieval. The information in these three categories should be available to any user who requests it.

Dissemination Information Packages Produced by an ISO 14721 Preservation Repository

DIP Categories of Significant Properties and Actions	Records Producer Responsibilities for Metadata Properties and Associated Actions	Trusted Repository Responsibilities for Metadata Properties and Associated Actions
Administration (ADM)	NA	NA
Technical (TEC)	NA	NA
Provenance (PRO)	NA	PRO-1/ADM-2 Inherited confirmation of Name of Record Producer
	NA	PRO-2 Inherited confirmation of Archival Bond
	NA	PRO-3/AMD-3 Inherited confirmation name of of Business Unit, Function, or other Entity that had custody of records at transfer
	NA	PRO4-A Inherited confirmation of Hierarchical Relation – Level 1 Name and description of Business Function/Organization/Collection *(As Appropriate)*
	NA	PRO-4B Inherited confirmation of Hierarchial Relation Level 2 Name and description of Series Content *(As Appropriate)*
	NA	PRO-4C Inherited confirmation of Hierarchial Relation Level 3 Name and description of Folder Content *(As Appropriate)*
	NA	PRO-4D Inherited confirmation of Hiearchial Relation Level 4 Name and description of Items *(As Appropriate)*
Preservation Description (PRE)	NA	PRE-1 Inherited cumulative transaction history of preservation action (e.g., storage device/media renewal, format transformation, creation of AIPs, transfer to Archival Storage, among others)
	NA	PRE-2 Inherited cumulative transaction history of the agent/entity responsible for the preservation activity- Repeatable
	NA	PRE-3 Inherited cumulative transaction history of date of preservation actions
	NA	PRE-4 Inherited cumulative transaction history of successful completion of preservation action
	NA	PRE-5 Inherited cumulative transaction history of Integrity Validation (hash digest)
	NA	PRE-6 Inherited cumulative transaction history of periodic random samples of Integrity Validations (hash digest) of AIPs

DIP Categories of Significant Properties and Actions	Records Producer Responsibilities for Metadata Properties and Associated Actions	Trusted Repository Responsibilities for Metadata Properties and Associated Actions
Content Description (CON)	NA	CON-1/TEC-7 Inherited Persistent Identifier in a system file registry
	NA	CON-2 Inherited confirmation of Time Coverage of Records
	NA	CON-3/TEC-2 Inherited confirmation of Name of Record Producer
	NA	CON-4 Inherited confirmation of name of Contributor and/or Creator
	NA	CON-5 Brief description of digital content along with subjects, topics, and other relevant information
Access (ACC)	NA	ACC-1 Posting of Content Information of all non-restricted DIPs to website
	NA	ACC-2 Standalone search engine or search capabilities integrated into digital preservation system
	NA	ACC-3 Routing of search engine query findings to Access/DIPs production function
	NA	ACC-4 Confirmation of User Request for one or more DIPs by Agent name
	NA	ACC-5 Confirmation by Entity/Agent that no Restrictions limit access to requested AIPs
	NA	ACC-6 Confirmation that redaction if required was correctly executed by Agent Name
	NA	ACC-7 Confirmation of the format(s) of DIPs requested
	NA	ACC-8 Production of requested DIPs including date
	NA	ACC-9 Attach one or more hash digests that validate the integrity of DIPs
	NA	ACC-10 Attach electronic customer service survey form
	NA	ACC-11 Confirmation of delivery of date and time of DIPs
	NA	ACC-12 Capture relevant details of requested AIPs and delivery of DIPs for statistical reports and preservation planning
Packaging Information (PAC)	NA	NA