The Sedona Conference Journal

Volume 16 2015

Ensuring Long-Term Availability, Usability, and Trustworthiness of Digital Information

Charles M. Dollar & Lori J. Ashley

Recommended Citation:

Charles M. Dollar & Lori J. Ashley, Ensuring Long-Term Availability, Usability, and Trustworthiness of Digital Information, 16 Sedona Conf. J. 175 (2015).

For this and additional publications see: https://thesedonaconference.org/publications

The Sedona Conference Journal® (ISSN 1530-4981) is published on an annual basis, containing selections from the preceding year's conferences and Working Group efforts. The Journal is available on a complementary basis to courthouses and public law libraries and by subscription to others ($95; $45 for conference participants and Working Group members). Send us an email (info@sedonaconference.org) or call (1-602-258-4910) to order or for further information. Check our website for further information about our conferences, Working Groups, and publications: www.thesedonaconference.org.

Comments (strongly encouraged) and requests to reproduce all or portions of this issue should be directed to:
The Sedona Conference at comments@sedonaconference.org or call 1-602-258-4910.

The Sedona Conference Journal® designed by MargoBDesignLLC
See margobdesign.com or mbraman@sedona.net.

Cite items in this volume to "16 Sedona Conf. J. _____ (2015)."

ENSURING LONG-TERM AVAILABILITY, USABILITY, AND TRUSTWORTHINESS OF DIGITAL INFORMATION

*Charles M. Dollar**
Dollar Consulting
Hoschton, GA

*Lori J. Ashley***
Tournesol Consulting
Dousman, WI

*Foreword by Jason R. Baron****
Drinker Biddle & Reath LLP
Washington, D.C.

FOREWORD

The Danish physicist Niels Bohr is purported to have said that "Prediction is very difficult, especially if it's about the

---

* Charles M. Dollar has more than four decades of electronic records management 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 a recipient of the Emmett Leahy Award for Outstanding Contributions to the Records and Information Management Profession. Charles is co-developer with Lori Ashley of the Digital Preservation Capability Maturity Model (DPCMM) and can be reached at thecdollar@att.net.

** Lori J. 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 and talent for developing approaches to jumpstart and sustain cross-functional collaboration among stakeholders who share accountability for effective and efficient life cycle control of valued records and information assets. Lori 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.

*** Jason R. Baron is Of Counsel to the Information Governance and eDiscovery Group at Drinker Biddle & Reath LLP, in Washington, D.C., and

future."[1] There seems little doubt, however, that we face the almost certain prospect of continued exponential growth, at an increasingly accelerated rate, of electronically stored information (ESI) in every form imaginable for as far into the future as we can currently see. At the same time, the torrents of data being churned out on a daily basis may not be accessible to future generations, given the accelerating obsolescence of many varieties of digital media and software.[2]

Unlike straightforward long term maintenance of traditional paper records, records in digital formats pose serious challenges both to public and private sector institutions, given an increasing need for continued preservation in long-term digital formats. Even apart from the special case of the need to maintain public records on a permanent basis (e.g., White House e-mail), a growing number of statutes (such as Sarbanes-Oxley) require the private sector to engage in medium- to long-term preservation of ESI content beyond what may be the expected life of underlying technological platforms. Media and format obsolescence, coupled with insufficient attention to standards based digital preservation systems for protecting long-term digital content, therefore loom large as obstacles to overcome.

---

previously served as Director of Litigation at the National Archives and Records Administration. He is a former Co-chair of the Steering Committee of Working Group 1 on Electronic Document Retention and Production with The Sedona Conference.

1. ARTHUR K. ELLIS, TEACHING AND LEARNING ELEMENTARY SOCIAL STUDIES 431 (1970).

2. Someone who did engage in prediction was Jeff Rothenberg, who made a similar point about media obsolescence in his influential (and controversial) article, *Ensuring the Longevity of Digital Documents*, SCIENTIFIC AMERICAN, vol. 272, no.1, Jan. 1995, at 42-47.

This transformational era of "information inflation," starting with the advent of desktop computing in the 1970s, and taking off especially with the growth of computer networks and the Internet in the 1990s, poses profound issues for the legal profession as well as society as a whole. Both the need and the desire exist to ensure preservation of and access to trustworthy documentation in digital form. This is the case not only just as a matter of ensuring the continued authenticity of increasingly aging but still relevant ESI in lawsuits, but for the greater purposes of the historical record of our era being maintained. Nothing less than our collective cultural memory is at stake.

In light of the above, Charles Dollar and Lori Ashley's article could not be more timely and important. As the authors recognize in citing to Principle 9 of The Sedona Conference's *Commentary on Information Governance*, organizations need to take reasonable steps to ensure the ongoing integrity and availability of long-term digital assets for their useful life. To this end, the authors have made available a Digital Preservation Capability Maturity Model (DPCMM) to assist organizations in conducting gap analyses of their current digital preservation capabilities, in line with prevailing international standards in the space science data and archival communities. They go on to properly urge that active long-term digital preservation strategies be included in the mix, as a necessary component of C-suite conversations involving the legal, regulatory, financial, and operational concerns of a firm or institution. The article constitutes a "call to arms" regarding long-term archival preservation as an important facet of information governance.

I. HISTORICAL PERSPECTIVE ON DIGITAL PRESERVATION ISSUES: RISKS OF TECHNOLOGY OBSOLESCENCE AND TRUSTWORTHY DIGITAL INFORMATION

Organizations are required to keep records and information as long as may be necessary for legal, financial, operational, research, and cultural memory purposes, depending on their mission and objectives. Some of these assets, born and living their entire "lives" in the digital world, must be indefinitely or even permanently retrievable, understandable, and trustworthy.

Risks and serious threats associated with the use of computer technologies have risen significantly for most organizations—public and private—over the past four decades. For organizations that must ensure long-term access to trustworthy business records over successive generations of technologies and custodians, the stakes get even higher. The brief historical perspective that follows sets the stage for consideration of current challenges for ensuring valued digital information assets will be accessible and trustworthy for as long into the future as required.

Storage Device/Media Obsolescence

Since the mid-1970s archivists have recognized that the obsolescence of storage devices and media was a major risk to access to electronic records (called "machine readable records") of permanent value. Magnetic tapes with varying storage densities replaced punch cards. Magnetic hard disks with increasingly higher storage densities accompanied by increasingly smaller form factors such as tape cartridges supplanted open reel magnetic tapes as the primary operational storage devices and media. Optical digital storage media such as CDs, DVDs, and WORM (Write-Once-Read-Many) provided more storage and dissemination options. For the foreseeable

future all digital storage device/media face inevitable technology obsolescence.

File Format Obsolescence

Archivists 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. Many of the most commonly used computer applications rely on proprietary native file formats to create, save, store, manage, and retrieve digital content. Unless the application supports an explicit import/export functionality or the new native format supports backward compatibility, digital content can only be "recognized" and accessed by software used to create and save it. Absent either backward compatibility or an export functionality, proprietary native file formats that vendors no longer support become legacy file formats that cannot be easily rendered into human readable form.[3]

Trustworthiness

In the early years of electronic records management archivists paid little attention to trustworthiness (reliability and integrity) because it was presumed that once the records were

3. One instance of this involves "Computer Enhancements of Autopsy Photographs and X-rays of President John F. Kennedy," which were done by the Aerospace Corporation between 1976 and 1979 as part of the work of the U.S. House of Representatives, Select Committee on Assassinations, using a proprietary image enhancement technology. The original photographs and X-rays along with the enhancements were transferred to the National Archives of the United States in 1979. The National Archives has duly maintained the readability of the bit streams that comprise the enhanced photographs and X-rays for almost four decades, but actual rendering of the enhanced photographs and X-rays requires access to the native proprietary format and the operating system in place at Aerospace Corporation at that time.

in the custody of an archives they would be protected from internal and external corruption. Adherence to strict data processing protocols, it was believed, would mitigate this potential loss of trustworthiness. Of course, this impregnable fortress mentality ignored the potential for computer failures and accidental human actions that could introduce errors in the records or perhaps even delete them. Few people at the time recognized the insidious threat of intentional hacking, data corruption, and theft of records by external parties.

One of the earliest efforts to monitor integrity of electronic records was an initiative of the Machine Readable Archives Division of the U.S. National Archives and Records Service[4] (NARS) in the late 1970s to generate a bit/byte count before and after replicating electronic records. This was a primitive initiative because bit/byte counts are aggregate measurements for a large volume of bit/bytes that can contain undetected errors. Within a decade the newly named National Archives and Records Administration was evaluating the use of cryptographic hash digests to support validation of the integrity of electronic records.

II. EVOLVING DIGITAL PRESERVATION ECOSYSTEMS

So what has changed over the last two to three decades? There are at least four noteworthy changes in business and computing environments that impact how active digital preservation can be accomplished:

- The emergence of technology neutral open standard formats that mitigate file format

4. In 1984, Congress changed the name of the U.S. National Archives and Records Service to the U.S. National Archives and Records Administration as part of the legislation that made it an Independent Federal Agency.

obsolescence for structured and unstructured content while still in the custody of records owners/producers
- International standards for trustworthy digital repositories
- Cryptographic hash digests that validate the integrity of digital content
- The emergence of Information Governance as a coordinating accountability framework for enterprise-wide information life cycle management, including defensible disposition

Technology Neutral Open Standard Formats

Technology neutral open standard formats greatly mitigate file format obsolescence because they are platform agnostic: they are interoperable on any system that implements the specifications. Commonly used technology neutral open standard file formats[5] include:

- XML, Extensible Markup Language. W3C Internet Engineering Task Force.
- PDF/A, Portable Document Format/Archive. ISO 19005-2:2011.
- HTML, Hyper Text Markup Language. ISO 15445:2000.
- PNG, Portable Network Graphics. ISO 15948:2003.

5. Tagged Interchange File Format (TIFF) is not included, because it is not an approved open standard raster image format; although, based upon usage it is a de facto standard. In addition, a set of geographic/geometric standards for information concerning objects or phenomena that are directly or indirectly associated with a location relative to the Earth is under development by IS0 TC 211.

- SVG, Scalable Vector Graphics. W3C Internet Engineering Task Force: 2001.
- JPEG, Joint Photographic Engineering Group 2000. ISO 15444-1:2004.
- Moving JPEG 2000, Joint Photographic Experts Group 2000. ISO 15444-3:2007.
- MPEG-3, Moving Image Experts Group. ISO 11172:1999.
- Web ARChive (WARC). ISO 28500:2009, Information and documentation—WARC file format.

Open standard technology neutral file formats are not a one-time solution, nor are they viable if inconsistently used.[6] Over time, formats that take advantage of new technologies will supplant existing ones. These new open standard technology neutral formats will support backward compatibility so that transformation of digital objects will be relatively straightforward.

Trustworthy Repository Standard

A major breakthrough occurred in 2003 when the International Organization for Standardization issued ISO 14721 Space data and information transfer systems—Open archival information system—Reference model.[7] Popularly

6. PREFORMA, PREservation FORMATs for culture information/e-archives, is a procurement project co-sponsored by the European Commission, with a stated goal to assist cultural memory institutions ingest digital content through file format standardization and conformance tools. *See generally* PREFORMA, http://www.preforma-project.eu/project.html.

7. ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies who prepare international standards through the work of technical committees. Copies of international standards may be obtained for a fee at www.iso.org.

known as "OAIS," it identifies a high level framework for functions and actions an Archive[8] must undertake to preserve permanent, or manage indefinite long-term retention of, digital information.

In 2005, the Research Library Group and the National Archives and Records Administration (RLG-NARA) issued "Trustworthy Repositories Audit and Certification: Criteria and Checklist" (TRAC) to support certification of a range of repositories and archives. TRAC became the basis for ISO 16363:2012, Space data and information transfer systems—Audit and certification of trustworthy digital repositories, a recommended practice for assessing the trustworthiness of ISO 14721 conforming repositories.

A small number of repositories have successfully been certified to TRAC. A series of test audits using the ISO 16363 standard in Europe and the United States were undertaken in 2011. The establishment of certifying and accrediting institutions to support ISO 16363 is underway in earnest,[9] and a number of world class institutions (U.S. Government Publishing Office and Library and Archives Canada) have stated their intention to seek ISO 16363 certification.[10] At least one Italian

8. The standard defines OAIS as an Archive which may be part of a larger 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 described in ISO 14721 that distinguishes it from other uses of the term 'archive.' Available free from http://public.ccsds.org/publications/archive/650x0m2.pdf.

9. ISO 16919:2014, *Requirements for Bodies Providing Audit and Certification of Candidate Trustworthy Digital Repositories* supplements ISO 16363 by specifying the competencies that auditors must have, and the way an audit must be performed, in line with the ISO international process.

10. Audit and Certification of Trustworthy Digital Repositories, ISO, http://www.iso16363.org/.

jurisdiction has passed into law[11] a requirement for government digital repositories to become certified. It seems reasonable to expect that additional sectors and industries will follow suit within the next few years.

Cryptographic Hash Digests

Ensuring the integrity of digital content in the age of cyberattacks is proving to be quite challenging and costly for public and private sector organizations alike. Cryptographic hash digests, however, are powerful validators of the integrity of digital content over time. Essentially, they are algorithms that compress digital objects without regard to the number of bytes they contain to hash digests of fixed-length bit streams ranging from 128 bits (MD5) to 512 bits (Secure Hash Algorithm-512). Currently, it is considered computationally infeasible to reproduce the original bits of a document or other digital content from a Secure Hash Algorithm digest of 160 or greater bits.

Cryptographic hash digests can be generated before and after a preservation action such as replication of digital content and the two hash digests will be identical. If there has been a change of only 1 bit, the second hash digest value will be different. Management of pre- and post- hash digests in documentation of preservation actions helps establish a chain of electronic custody that constitutes the "circumstances of preservation" over time.

11. *Accreditamento e conservatori*, AGENZIA PER L'ITALIA DIGITALE (July 2, 2015), http://www.agid.gov.it/agenda-digitale/pubblica-amministrazione/conservazione/accreditamento-conservatori.

Emergence of Information Governance

Vulnerabilities and opportunities associated with e-discovery, cloud computing, and "big data" that have emerged over the past decade or so are helping to precipitate a transformation in the way that many organizations view and handle the management of information as an asset. Information Governance (IG) is being advanced[12] as a coordinating decision-making and accountability framework for maximizing the value of information while minimizing its costs and risk. This type of transformation requires a top-down organization-wide commitment as well as coordinated approaches and technologies to systematically manage the life cycle of information, including defensible disposition. Enterprise legal, financial, regulatory, operational use, privacy/security, records management, compliance/risk management, and IT requirements and practices are ideally addressed in a cross-disciplinary and programmatic manner.

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.[13] 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.[14] Within this context, integrity means trustworthiness while "availability" means there are no technology barriers (e.g., obsolescent native

12. *See generally*, INFORMATION GOVERNANCE INITIATIVE, www.iginitiative.com.

13. The Sedona Conference, *Commentary on Information Governance*, 15 SEDONA CONF. J. 125 (2014).

14. *Id.* at 150-51.

proprietary file formats or unreadable storage media) to access.[15]

The Commentary does not use digital preservation or technology obsolescence in its discussion of Principle 9, but it is clear that "ensuring the on-going integrity and availability of long-term digital assets" is preservation by another name. There are two important implications of this, the first of which is that ensuring the integrity and availability of long-term and permanent assets is no longer the exclusive domain of archivists and librarians; it is an enterprise domain with many stakeholders and responsible parties.

The second implication is that resolution of technology obsolescence and integrity of long-term digital content must begin proactively in the operational environment. Essentially, this means that content creators and business process owners working in tandem with a broad spectrum of technologists must mitigate the many risks associated with integrity and preservation of long-term digital information while the assets are managed within production environments.

The Digital Preservation Capability Maturity Model (DPCMM), which is discussed below, provides practitioners and digital preservation system operators with a structured framework to explore "processes and operations involved in ensuring the technical and intellectual survival of authentic records through time."[16] Strategies include creation of "preservation-ready" digital objects at or near the time of capture or receipt wherever practical and providing sufficient metadata as evidence of trustworthiness at the point of transfer to the archival repository. DPCMM is also meant to support

15. *See id.*

16. ISO 15489-1:2001, 3.14 preservation.

planning and coordination between content owners/providers ("Producers" in the OAIS standard) and repositories. Finally, DPCMM provides a way for executive leadership and resource allocators to assess risk and measure the impact of investments in digital preservation capability improvements.

III. DIGITAL PRESERVATION CAPABILITY MATURITY MODEL (DPCMM)

The Open Archival Information System standard (OAIS, ISO 14721:2012) describes preservation functions and associated actions at a very high level as a reference model, not as an implementation model. Accordingly, these functions and associated actions must be deconstructed into terms that are readily understood and can be applied in a variety of operational environments.

For many institutions (e.g., state archives and cultural memory institutions), this understanding will have a significant bearing on their ability to secure sufficient financial and technical resources to establish digital preservation systems and prepare for the deluge of born-digital content which they are increasingly expected to accession, store, and make available to users upon demand. For all organizations, a clear delineation of the roles and responsibilities across the chain of electronic records management for record producers, owners, and custodians has become a critical component of supporting enterprise information governance.

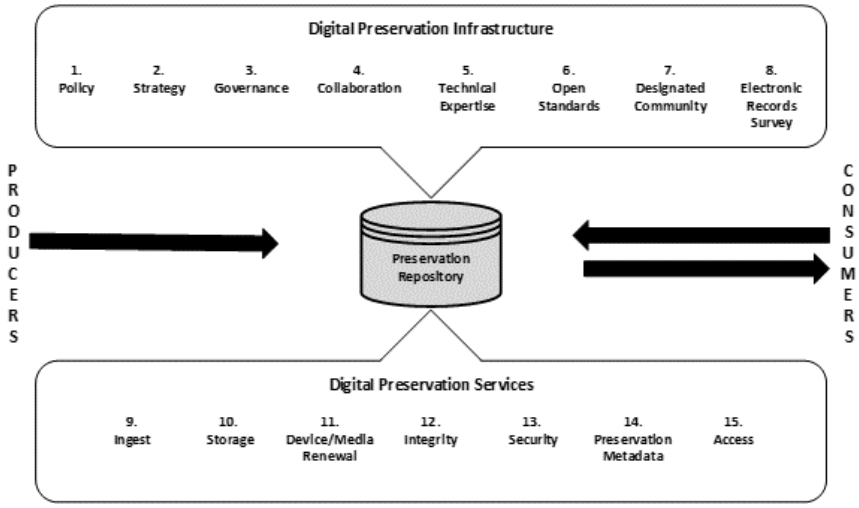

Figure 1. Digital Preservation Capability Maturity Model (DPCMM)

In 2007, the authors developed a Digital Preservation Capability Maturity Model (DPCMM) for use in a project for the Delaware Public Archives. A maturity model is a set of structured levels that describe how well the practices, processes, and behavior of an organization can reliably and sustainably produce desired outcomes. The components of DPCMM (Figure 1), which cover a range of governance, operational, and data management functions, are organized into three domains: Infrastructure, Repository, and Services.

Digital Preservation Infrastructure features eight (8) components which define the mandate, means, and methods used to ensure the long-term preservation of digital information assets:

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

Digital Preservation Services include seven (7) components that are required for planning, continuous monitoring of external and internal environments, and necessary preservation actions that sustain the integrity, security, usability and accessibility of digital information assets stored in repositories:

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

The third component in DPCMM is an ISO 14721 conforming digital repository that embraces the audit and certification criteria of TRAC and ISO 16363. The organization that has responsibility for preserving the records may operate the repository, or an external third party may provide digital preservation system infrastructure and services.

Five Levels of Digital Preservation Capability

The DPCMM identifies five levels of incremental digital preservation capability (*Figure 2*). In addition to providing a useful framework for analysis and planning among archivists and records managers, using a capability maturity model (CMM) to convey the requirements provides a familiar construct for information technology (IT) architects and system administrators.

Each of the 15 DPCMM components has five incremental stages of capability called digital preservation performance metrics. The performance metrics of each component correlate to the five stages of maturity capability shown below.

Assignment of a numeric value (0-4) to each of the performance metrics enables computation of an overall digital preservation index score. Ranges of potential digital preservation index scores are:

Capability Level	Index Score Range
Nominal Digital Preservation Capability	0
Minimal Digital Preservation Capability	1 - 15
Intermediate Digital Preservation Capability	16 - 30
Advanced Digital Preservation Capability	31 - 45
Optimal Digital Preservation Capability	46 - 60

Figure 2. Five Stages (Levels) of Digital Preservation Capability

Self-Assessment Scorecard

A Digital Preservation Capability assessment can be produced that provides an aggregate score as well as a numeric score for each of the fifteen components. The individual component scores can be used to develop a prioritized incremental improvement plan that is tailored to the resources available as well as establish what level of digital preservation capability is "good enough" for any given organization or repository.

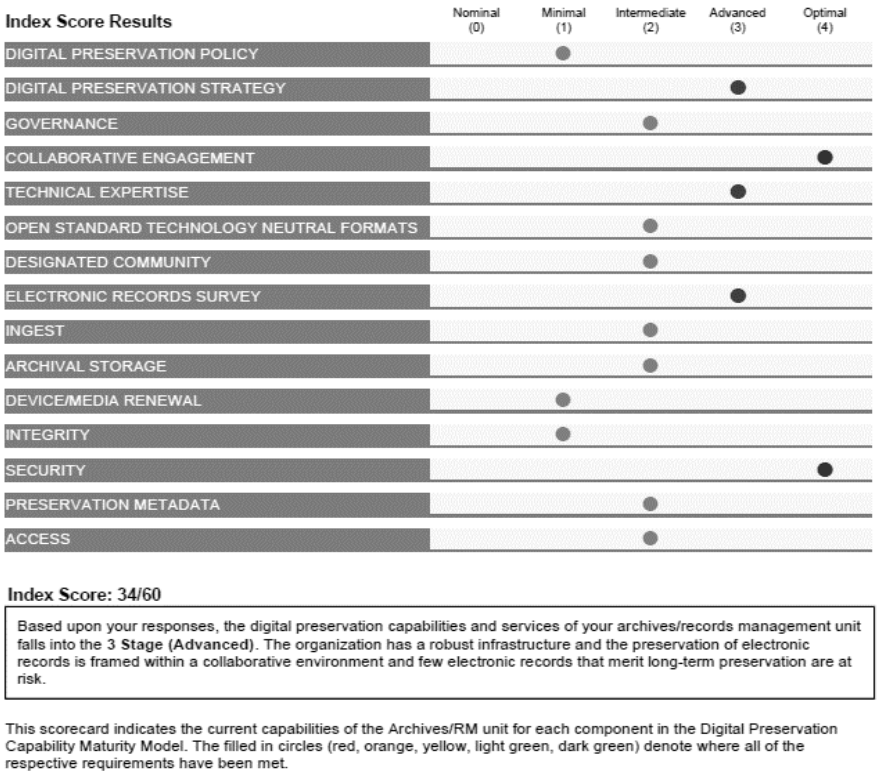

Figure 3. Sample Digital Preservation Capability Self-Assessment Scorecard. Image captured from full-color web-based application.

IV. DPCMM CASE STUDIES

The DPCMM has now been in active use for eight years. Within the past four years, a digital preservation capability self-assessment survey tool based on DPCMM has been successfully applied by two groups, the Council of State Archivists (CoSA) and the Section of International Organisations (SIO) of the International Council on Archives (ICA). Case studies of their experience with the digital preservation capability self-assessment tool are described in this section.

In 2012, archivists of the fifty-six states, territories, and District of Columbia administered the self-assessment. A description of the trajectory of CoSA's use of DPCMM is provided below. The second round of self-assessments by CoSA members closed at the end of May 2015. Longitudinal results from the largest community thus far to use DPCMM are expected to become available in Fall 2015.

A third iteration of the digital preservation self-assessment survey was developed in 2013 to support a mobile application Proof of Concept (POC) for the International Council on Archives (ICA). Details are offered in the second case study in this section.

Members of these groups are practitioners, primarily from archives in the early stages of establishing digital preservation capabilities. Many of the practitioners also have records management duties. Commonalities among practitioners in the two communities include the following:

- Need to raise awareness and educate a broad spectrum of stakeholders on digital system requirements
- Need to attract sufficient expertise in archives and digital preservation systems to address growing digital collections

- Improved governance over transfer and ingest functions, including agreements with donors and owners that meet minimum standards for submissions to the archives/digital preservation system
- Strategies to mitigate risk of technology obsolescence over the lifetime of valued digital information assets

With the endorsement of CoSA's State Electronic Records Initiative (SERI) Steering Committee and permission from the National Historical Publications & Records Commission (NHPRC), the authors of this paper developed a public version of the Digital Preservation Capability self-assessment tool[17] and formally introduced it during the 2014 Society of American Archivists (SAA) conference in Washington, D.C. The objective of this release was to enable a broad range of organizations to use the tool and advance dialogue about digital preservation.

DCPMM Case Study: Council of State Archivists

In July 2011, the Council of State Archivists (CoSA) launched a nationwide initiative focused on improving efforts to manage, preserve, and provide access to U.S. state government electronic records. The goal of SERI Phase 1 of the State Electronic Records Initiative was to create a profile of electronic records programs in order to develop an action plan to address the needs of state archives and records management programs and identify next steps.

CoSA compiled information on electronic records management and digital preservation programs as part of the SERI Phase 1 initiative. Responses to questions and transcripts

17. www.DigitalOK.org is free and open for use to any practitioner interested in assessing digital preservation capabilities and repositories.

from phone interviews with the directors and electronic records staff were collected from 55 state and territorial archives. CoSA invited Dollar and Ashley to analyze the survey results and map the findings to the fifteen (15) components of the model.[18] In addition to providing a composite "score" on the readiness of each state and territory archives to preserve long-term and permanent electronic records, the analysis highlighted current good practices as well as enormous gaps. The consultant report stated that "[a]lmost one-half (21) of the responding states/territories (48) registered an absolute Nominal digital preservation capability index score on each of the fifteen key process areas."

In November 2011, CoSA President Julia Marks Young included excerpts from this analysis at a meeting of the National Historical Publications and Records Commission. She urged immediate action and declared state archives ready to tackle the challenge of digital records.

Subsequently, in 2012, the Institute of Museums and Library Services (IMLS) awarded CoSA a three-year $500,000 grant (*Laura Bush 21st Century Librarian Program*) to identify training needs and priorities for state archives, to organize and conduct training programs, and to benchmark the effectiveness of the program. The program called for each state archives to take a self-assessment survey and establish a base-line digital

18. CoSA SERI Phase 1, *Mapping of Survey Results to the Digital Preservation Capability Maturity Model, Findings and Recommendations*, Charles M. Dollar & Lori J. Ashley, September 2011, page 4. Highlights of the Dollar and Ashley deliverable are incorporated into the *Report from the Council of State Archivists' State Electronic Records Initiative (SERI) Committee, available at* http://www.statearchivists.org/seri/SERI%20Phase%20One%20Report%20-%20final%20review%20draft%20-%202012-06.pdf.

preservation capability score. At the end of the grant program each state archives will take the self-assessment survey again.

The Council of State Archivists (CoSA) engaged the authors of this paper to develop a self-assessment tool based on their Digital Preservation Capability Maturity Model. Development of the web-based survey tool was funded through an NHPRC grant and used between May and June 2012 by all 56 state and territorial archives to establish a baseline[19] for their digital preservation infrastructure and services capabilities. By August 2013, at *ARCHIVES New Orleans / 2013, the Joint Annual Meeting of CoSA and SAA*, representatives from the Mississippi, Wyoming, and Alabama State Archives were ready to share the stage[20] to discuss the self-assessment tool, their respective capability scorecards, and describe on-going improvement plans.

Development of a resource portal (PERTTS) also began in 2013. The portal provides useful materials addressing electronic records management and preservation. A series of webinars have also been delivered and are available in a variety of interactive and self-directed modules. The portal and training initiatives both leverage a State Electronic Records Program (SERP) Framework which was adapted from DPCMM. In addition to a breakdown of the components and metrics, the framework links users to resources and case studies.

---

19. The SERI Steering Committee assigned its members into quartiles on the basis of an adjusted Digital Preservation Capability self-assessment score. Training scholarships and three week-long institutes were offered in 2013-14.

20. Charles M. Dollar & Lori J. Ashley, *Digital Preservation in State and Territorial Archives: Current State and Prospects for Improvement*, Society of American Archivists: 2013 Joint Annual Meeting Call for Proposals (Aug. 2013) (on file with author).

CoSA's SERI initiative is noteworthy because it is an acknowledgement that the digital capability of state archives as a custodian of permanent public records of the executive branch is critical to government accountability and transparency. Ensuring the availability, usability, and trustworthiness of permanent digital records, however, transcends the traditional boundaries between the executive, the legislative, and judicial branches of state governments. Dialogue and collaboration between and among state archives, state legislatures, and state courts about their mutual interest in this domain should be a high priority for all parties.

DPCMM Case Study: International Council on Archives Mobile Archives Standardization Tool (MAST)

In 2012, the newly elected President of the International Council on Archives (ICA) Section of International Organizations (SIO or "Section") initiated development of a multi-year work plan to advance records and archives management among the section members. The aim of the Section is to "promote the management and use of records and archives of international organisations and their preservation through the sharing of experiences, knowledge, research and best practices on professional archival and records management matters."[21]

The Section had an on-going interest in digital preservation issues so the president invited the authors of this paper to organize a workshop on the Digital Preservation Capability Maturity Model and its potential use at the 39th Annual Meeting of the SIO held in Brussels, Belgium, in June

21. International Council of Archives: Section of International Organisations—ICA/SIO, UNESCO, http://www.unesco.org/webworld/ica_sio/statutes.shtml (last visited June 14, 2015).

2013. In attendance was the Chief Inspector of the Joint Inspection Unit (JUI) who was in the final stages of completing his review and analysis of records and archives management in the United Nations. His report[22] identified the growing worldwide concern regarding the continuity of digital information and expressed appreciation for the technical considerations, especially those associated with DPCMM, shared during the workshop. The fourth of the six recommendations contained in the report references the importance of capturing, creating, and managing e-records in ways that meet international standards for recordkeeping and the preservation of digital records and archives.

The SIO work plan included a proposal for the development of mobile technology that could promote and make accessible international standards and training materials to ICA members. In 2013, ICA leadership agreed to fund a proof of concept (POC) for a mobile application tool designed to support practitioners in the lifecycle management of records and archives.

The Mobile Archives Standardization Tool (MAST©) was conceived as a practical tool for records management and archives practitioners who are working in low resource environments, such as Africa, the Caribbean, and South America. Low resource means low availability of electrical service, low connectivity, and limited professional records and archives management expertise. Use of mobile technology, combined with additional functionalities, is intended to directly support implementation of e-government administrative

22. *See* United Nations, *Records and Archives Management in the United Nations* (JU/REP/2013/2), *available at* https://www.unjiu.org/en/reports-notes/JIU%20Products/JIU_REP_2013_2_English.pdf.

reforms, access to information, and adequate management and preservation of digital records.

The POC MAST version included a high level self-assessment survey based on DPCMM, links to international standards, and sample training curriculum. The first release of the curriculum included two ICA modules on Digital Preservation and Managing Metadata. MAST is currently available on Android and Apple platforms, making it suitable for most commonly used mobile devices. MAST is being considered for use in a training program for a consortium of United Nations agencies in Africa with the potential to expand its use in other regions.

Providing a digital preservation self-assessment component via a mobile application was intended to help practitioners to baseline their programs and consolidate their improvement efforts. MAST modules and links to ICA and other resources can directly support capacity building for records and archive management programs and move them towards full compliance with internationally recognized standards.

V. SUMMARY

This paper makes the case that 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. For the public sector, the capability to protect and preserve long-term records is essential for governmental accountability. Private sector organizations that submit electronic records to regulatory agencies and the courts bear the burden of demonstrating that the "circumstances of creation and preservation" of long-term records support their authenticity.

Standards-based tools and approaches such as the Digital Preservation Capability Maturity Model (DPCMM) enable public and private organizations to conduct a gap analysis of their current capabilities based on international standards. This benchmark can be used to develop an incremental improvement road map that takes into account priorities based on a risk assessment analysis.

Organizations embracing Information Governance (IG) should incorporate digital preservation requirements, standards, and good practices into their program development and operation. Organizations without an explicit commitment to IG can benefit from incorporating digital preservation concerns into their existing risk management, strategic planning, and/or enterprise information architecture models to begin addressing how to ensure accessible, usable, and trustworthy digital information for as far into the future as may be required by their organizational mission, mandates, and needs.