A Comparison of ARM Literature and Information Protection Standards of Practice

Mel Leverich
Meghan Whyte
Eng Senseveng
&
Fred Cohen

Abstract

Archives and Records Management (ARM) literature surrounding Information Protection (IP) has been developed in relative isolation from the IP field. As a result, it has been unclear until now whether and to what extent ARM literature is consistent with or divergent from the literature of IP. Rather than review all of the literature of both of these fields, the present study undertakes a comparison between an existing IP standard of practice (SoP) and related elements of ARM literature.

This approach takes advantage of a vetted IP tool with a granular approach to topics while adapting specific ARM functions and requirements for control and preservation, such as metadata and transparency. Involvement by the target ARM community will further refine the SoP in terms of developing reasonable and prudent practices.

Background and Introduction

Both the IP field, more commonly spoken of as information security, computer security, cyber-security, and similar terms, and archival theory are ancient disciplines which can be traced back to the beginnings of recorded time when ancient Mesopotamians noted trade and tax information on clay bricks and protected them from alteration by firing the bricks and storing them away from harm.[1] Archival theory concerns the preservation of authentic records while IP was developed to protect information from unauthorized access, manipulation, use, denial of use,[2,3] and a range of objectives like transmission integrity and secrecy, authentication, and so forth. In the mid 20th century, IP was applied to digital technology.[4] Systems developed for military use focused largely on preventing leakage of confidential information by access controls and encryption, both for the digital systems and the physical systems the content was stored in.[5]

1 Amalia E. Gnanadesikan, *The Writing Revolution: Cuneiform to the Internet* (Malden, MA: Wiley-Blackwell, 2009), 14.

2 Jerome H. Salzer, “Basic Principles of Information Protection,” in *The Protection of Information in Computer Systems.* July 14, 2014, http://web.mit.edu/saltzer/www/publications/protection/Basic.html.

3 Margaret van Biene-Hershey, "IT security and IT Auditing Between 1960 and 2000," in *The History of Information Security: a Comprehensive Handbook,* ed. Karl de Leeuw, Maria Michael, and Jan Bergstra (Boston: Elsevier, 2007), 666.

4 Susan W. Brenner, ‘‘History of Computer Crime,’’ in *The History of Information Security: a Comprehensive Handbook,* ed. Karl de Leeuw, Maria Michael, and Jan Bergstra (Boston: Elsevier, 2007), 705–721.

5 Jeffrey R. Yost, “A History of Computer Security Standards,” in *The History of Information Security: a Comprehensive Handbook,* ed. Karl de Leeuw, Maria Michael, and Jan Bergstra (Boston: Elsevier, 2007), 595–621.

Business systems largely adopted the existing technologies for a time, but ultimately determined that their needs differed and balked at using the military technology. As the Internet and networked systems grew into the 1990s, the ease of transfer of data increased the information-related risks in terms of people, records, and systems.[6] Policy and training of workers had to be re-addressed because of the change of work, workers, demographics, and the nature of the use of information and related technologies. Standards for communication systems and coding also changes, requiring new approaches.[7] [8] While IP as a field continued to progress in recent decades,[9] [10] [11] [12] [13] [14] [15] [16] [17] [18] [19] [20] [21] the ARM literature produced an apparently independent set of approaches with respect to digital technology.

---

6 Dragos Ruiu, "Learning from Information Security History," *IEEE Security and Privacy* 4 no. 1 (2006): 77-79.

7 Jeffrey R. Yost, “History of Computer Security,” 595–621.

8 Dieter Gollman, “Security Models,” in *The History of Information Security: a Comprehensive Handbook,* ed. Karl de Leeuw, Maria Michael, and Jan Bergstra (Boston: Elsevier, 2007), 623–635.

9 Department of Defense, *Department of Defense Trusted Computer System Evaluation Criteria* (Washington: Department of Defense, 1986).

10 Commission of the European Communities, *Information Technology Security Evaluation Criteria: Preliminary Harmonised Criteria* (Luxembourg: Office for Official Publications of the European Communities, 1991).

11 Canadian System Security Centre, *Canadian Trusted Computer Product Evaluation Criteria* (Ottawa: Canadian System Security Centre, 1993).

12 International Organization for Standardization, *ISO 17799:2005 Information Technology—Security Techniques—Code of Practice for Information Security Management* (Geneva : International Organization for Standardization, 2005).

13 International Organization for Standardization, *ISO 15408-1:2009 Information Technology—Security Techniques—Evaluation Criteria for IT Security* (Geneva : International Organization for Standardization, 2009).

14 International Organization for Standardization, *ISO 9798-1:2010 Information Technology—Security Techniques—Entity Authentication*, (Geneva : International Organisation for Standardization, 2010).

15 Information Systems Security Association, *Generally Accepted Information Security Principles* v. 3.0 (ISSA, 2005).

16 National Institute of Standards and Technology, *Advanced Encryption Standard FPS 197-12* (Gaithersburg, MD : Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 2001).

17 National Institute of Standards and Technology, *Digital Signature Standard (DSS) 186-2* (Gaithersburg, MD : Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 2000).

18 National Institute of Standards and Technology, *Personal Identity Verification (PIV) of Federal Employees and Contractors 201-1* (Gaithersburg, MD : Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 2006).

19 National Institute of Standards and Technology, M*inimum Security Requirements for Federal Information and Information Systems 200* (Gaithersburg, MD : Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 2006).

20 National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organization Special Publication (SP) 800-53 Revision 4*, (Gaithersburg, MD : Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 2013).

21 ISACA, *COBIT 4.1: Framework for IT Governance and Control* (2007). July 14, 2014, http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx.

In the ARM field, “Early attention to the difficulties in preserving digital information focused on the longevity of the physical media on which the information is stored,” as opposed to digital records themselves.[22] The first generation of digital information was typically administrative, statistical, or survey data of short-term value.[23] Digital files were “largely viewed as 'data,'” with informational value, “not 'records',” with evidential value, and therefore not perceived as the responsibility of records managers and archivists.[24] The 1980's saw increasing attention to digital media and archival management, but not until the 1990's did the preservation of digital records through technological change become a topic of speciality in the ARM field.[25] [26] [27] [28] [29] In the 2000's, the ARM field developed numerous models, standards, guidelines, and tools with respect to long-term digital preservation.[30] [31] [32] [33] [34]

Having developed along parallel tracks, ARM and IP diverged. While IP's purpose is keeping people from harm associated with symbolic representations in the general sense[35], the ARM field's concern has been the archival creation, management, and preservation of digital records. In the ARM field, IP is typically conceived of as either a necessary antecedent, supplement or

---

22 Donald Waters and John Garrett, *Preserving Digital Information: Report of the Task Force on Archiving of Digital Information*, (Washington: The Commission on Preservation and Access, Research Libraries Group,1996), 5. http://www.clir.org/pubs/reports/pub63.

23 Terry Cook, "Easy to Byte, Harder to Chew: The Second Generation of Electronic Records Archives," *Archivaria* 33, no. 1 (1991), 203. http://journals.sfu.ca/archivar/index.php/archivaria/article/view/11812/12763.

24 Ibid., 204.

25 Ibid.

26 Luciana Duranti, “The Long-Term Preservation of Authentic Electronic Records,” in P*roceedings of the 27th VLDB Conference, Roma, Italy*, ed. P.M.G. Aspers et al. (Orlando, FL: Morgan Kaufmann, 2001). http://www.vldb.org/conf/2001/P625.pdf.

27 Luciana Duranti and Heather MacNeil, “The Protection of the Integrity of Electronic Records: An Overview of the UBC-MAS Research Project,” *Archivaria* 42 no 1. (1996): 46-67.

28 Waters and Garrett, “Preserving Digital Information.”

29 Wendy Duff, “Ensuring the Preservation of Reliable Evidence: A Research Project Funded by the NHPRC,” *Archivaria* 42, no. 1 (1996): 28-45.

30 Consultative Committee for Space Data Systems, *Reference Model for an Open Archival Information System*, (Washington: CCSDS Secretariat, 2002). July 12, 2014, www.ccsds.org/publications/archive/650x0b1.pdf.

31 Consultative Committee for Space Data Systems, *Producer-Archive Interface Methodology Abstract Standard* (Washington: CCSDS Secretariat, 2002). July 12, 2014. www.ccsds.org/publications/archive//651x0b1.pdf.

32 National Library of Australia, *Guidelines For The Preservation Of Digital Heritage* (Information Society Division United Nations Educational, Scientific and Cultural Organization, 2003). July 12, 2014, http://unesdoc.unesco.org/images/0013/001300/130071e.pdf.

33 PREMIS Working Group, *Data Dictionary for Preservation Metadata: Final Report of the PREMIS Working Group* (Dublin, OH : OCLC and RLG, 2005). July 12, 2014, www.oclc.org/research/projects/pmwg/premis-final.pdf.

34 Nestor Working Group on Trusted Repositories Certification, *Catalogue of Criteria for Trusted Digital Repositories,* Version 1 (Frankfurt am Main: nestor c/o Deutsche Nationalbibliothek 2006). July 12, 2014, http://edoc.hu-berlin.de/series/nestor-materialien/8en/PDF/8en.pdf.

35 F. Cohen, “Introductory Information Protection”, 1987-9, http://all.net/edu/curr/ip/index.html

service to archival management, rather than an integral part of the archival management and preservation process. The theoretical domains and responsibilities of IP and ARM overlap considerably in theory: both are concerned with ensuring the persistence of content with certain qualities. For IP those qualities typically include confidentiality, integrity, and availability among others.[36] Digital Preservation authors offer varying sets of principles based in archival theory. Based on an analysis of digital preservation literature, the SPOT model lists the following principles: availability, identity, persistence, renderability, understandability, and authenticity.[37] In the OAIS Reference Model, the de facto model for digital repositories, the mandatory criteria are "fixity, reference, provenance, context, understandability and availability of content" over time.[38] The InterPARES Project, on the other hand, takes diplomatics as a framework; InterPARES research is concerned with the traditional archival value of authenticity, defined as "The trustworthiness of a record as a record; i.e., the quality of a record that is what it purports to be and that is free from tampering or corruption," and related values of reliability and integrity.[39]

Becker et al. describe Digital Preservation as "information management with a long-term mission" compared to the "medium-term vision" of Information Governance and the IP fields. Digital Preservation is absent of formal, qualitative frameworks and guidance on "effective and efficient processes," which IP offers, while IP often suffers from a lack of long-term planning.[40] IP frameworks such as CoBit "are concerned with continuity and change, but do not integrate long-term effects into their processes. Specifically, they do not consider the implications of technology change and misalignment of access technologies on the authenticity and understandability of digital materials."[41] Becker et al. write that the potential to integrate digital preservation concerns into the disciplines of information systems and technology is "still unclear."[42]

The ARM IP fields should more fully integrate in order to progress in their shared responsibilities regarding the protection and preservation of records and information. This involves translating values, adapting concepts, and resolving differing understandings of shared terminology in order to communicate effectively. To this end an Archives and Records Management Information Protection Standards of Practice (ARM-SoP) for archives is being developed with InterPARES Trust. IP knowledge will be compounded with the knowledge and requirements of the ARM disciplines. The ARM-SoP will be specific to the proteciton aspects, priorities, and contexts of ARM systems.

---

36 Chad Perrin, *The CIA Triad*, (2008). July 14, 2014, http://www.techrepublic.com/blog/it-security/the-cia-triad/.

37 Ibid.

38 Sally Vermaaten, Brian Lavoie, and Priscilla Caplan, "Identifying Threats to Successful Digital Preservation: the SPOT Model for Risk Assessment," *D-Lib Magazine*, 18.9-10 (2012), n.pag. July 14, 2014, http://www.dlib.org/dlib/september12/vermaaten/09vermaaten.html.

39 InterPARES, "Authenticity," *The InterPARES 2 Project Dictiona*ry. July 12, 2014, http://www.interpares.org/ip2/display_file.cfmdoc=ip2_dictionary.pdf&CFID=4164403&CFTOKEN=69638790.

40 Christoph Becker, Gonçalo Antunes, José Barateiro, Ricardo Vieira, and José Borbinha, "Control objectives for dp: Digital preservation as an integrated part of it governance," *Proceedings of the American Society for Information Science and Technology* 48, no. 1 (2011): 1-10.

41 Ibid., 1.

42 Ibid.

Archives Information Protection Standard of Practice

The purpose of the "InterPARES Trust, Archives Information Protection Standard of Practice (SoP) project" is to develop a standard of practice for archival repositories in Information Protection based on the Enterprise Information Protection Standard of Practice.[43] A standard of practice is a decision-making methodology used to help professionals determine reasonable and prudent courses of action for a given institutional circumstance. The concept of a "reasonable and prudent" action originates in English tort law with the "reasonable man."[44] An action is reasonable and prudent if it is what a prudent person with reasonable amount of expertise or knowledge might have done given the same circumstances. ARM institutions will be able to use the SoP, developed from an existing SoP for IP, an ARM literature review, and a community consensus-seeking process, to evaluate their own practices against those of the ARM community. As a methodology, the SoP provides reasonable and prudent approaches to common IP issues, and facilitates the identification of current and reasonable and prudent future states of institutions' overall IP. However, the current and anticipated SoPs do not uniquely identify reasonable and prudent practices. That is, if an SoP identifies something as reasonable and prudent in a situation, that does not mean that another approach is not reasonable and prudent. Without the ARM focused SoP, IP actions are likely to be dependent on the knowledge of individuals directly involved in the institutional IP effort, rather than a more broadly studied analysis based on community consensus regarding what is reasonable and prudent and the relevant IP and ARM literature.

The ARM-SoP currently contains 111 elements. Each element collects factual information about the institution or concerns a particular decision nexus, and is organized in four parts. The title is phrased in the form of a question (e.g., "How are real-time interdependency risks managed?"). The Option section of each element contains a non-exhaustive set of alternatives by which the titular question may be answered. The Decision section contains a decision-making process and the methodology to determine which Option(s) is(are) most likely to be reasonable and prudent for a given situation. The Basis section is used to provide underlying definitions and rationale for the decision. In the application of the ARM-SoP, the original (as-is) situation is collected and codified, and a reasonable and prudent future state is developed based on applying the decision criteria in context. The basis for decisions is included as well so that the reasoning behind the decisions is documented. The Decision methodology can be applied by rote, however it is meant to be supported and invoked by an expert analyst with knowledge of the subject's particular circumstances and in a group process involving parties with relevant knowledge of specifics.[45]

Beginning in October 2013, the SoP research team reviewed standards and literature from the ARM domains containing recommendations about information security. The team compared the reviewed literature against the pre-existing Enterprise Information Protection SoP for incongruities and gaps. This Standard of Practice was adapted to take into consideration ARM

[43] Fred Cohen, "Enterprise Information Protection Standard of Practice," All.net, accessed July 7 2014, available at http://all.net/SoP/SecDec/index.html.

[44] Vaughan v Menlove, (1837) 3 Bing. N.C. 467, 132 E.R. 490 (C.P.).

[45] See Fred Cohen's Fearless Security webinar series, available at http://courses.all.net/index.html.

literature regarding information security, producing the first draft of the ARM SoP (hereafter SoP) in early 2014. In February 2014, the draft SoP was used to develop a proof of concept system specification for a low risk and low consequence archives in order to demonstrate one of the many possible applications of the SoP.

In 2014-2015, the draft SoP has and will continue to be applied to ARM institution volunteers. The study seeks to solicit up to twenty-five subject institutions in ARM in order to represent the diversity of the profession. One or more individuals knowledgeable of the subject institutions' IP practices is required to complete the interview in one working day. The information gathered is used to develop the institution's "As-Is" Information Protection practices for each element of the SoP. After the interview, subjects are given a copy of the as-is report and are asked to fill out a survey identifying anything they found divergent or missing from their experience. A "rote" analysis is then performed using the decision-making methodology of the SoP to identify recommended Future States for the institution. A rote analysis applies the Decision methodology in the SoP without the expert mediation of the analyst.

Directly after the conclusion of the interview, fill out a questionnaire on the interview process. Ten days later, the rote analysis is completed and provided to the subject along with a second questionnaire asking subjects to comment on the results of the rote application of the SoP to their institution, in particular to evaluate whether and to what extent they find the results reasonable and prudent. Roughly four months after the conclusion of the interviews, a third questionnaire asks subjects and InterPARES Trust members to comment on the application of the SoP to pseudonymized results of other institutions. The third questionnaire again asks the respondents to comment on whether the SoP's rote recommendations are reasonable and prudent for the institution's circumstances, and why. As practicing professionals, these individuals are presumed to have sufficient expertise and knowledge in order to comment on what IP actions they believe to be reasonable and prudent for ARM institutions. Following the data gathering portion of this study, the questionnaire results will be analyzed for community consensus on reasonable and prudent actions. Where consensus is found, it will be identified in the methodology of the SoP, and where it is not present, the issue will be identified as a result of the effort.

Development

Thus far, the draft SoP has been adapted from the pre-existing standards of practice based on research into digital preservation and archival standards and literature. The following additions were made to the previous IP-only versions:

- A new element with the ARMA International Maturity Model for Information Governance, "Overarching: ARMA maturity model: What GARPM maturity levels do different aspects of the archive have?" The SoP research team is considering removing the ARMA maturity model from the SoP due to its internal inconsistency and definitions of terms which differ from those in the SoP and other ARM and protection literature.
- A new element on metadata with the Application Profile for Authenticity Metadata, General Study 15 of InterPARES 3, "Technical Security Architecture: Metadata: What

Metadata should be ingested, created, retained, and presented?"[46] The Application Profile is based on the Chain of Preservation model and related standards.

- For the ARM-SoP, Custody and Transparency were added to the protection model in the element "Overarching: Protection model: What model is used to understand Information Protection issues?" and these concepts were fused throughout the remainder of the SoP. This was carried back into the other SoP protection models because these concepts were so clearly relevant across the entire spectrum even though they were largely ignored in the protection field prior to this effort.
- A simplified Open Archival Information System (OAIS) model was added to the Options of "Business modelling: Is an explicit business model used to support Information Protection decision-making?"[47]
- Ingest, Preserve and Access were added to the simplified business model.
- Chain of Custody mechanisms are now recommended for Low risk institutions in "Content control: What mechanisms keep control over content with business utility?"

The following changes were made to both the Enterprise SoP and the Archives SoP. This list excludes minor changes that were unrelated to research conducted during the InterPARES study:

- A new element on identity based on *Identity Proofing and Verification of an Individual,* "Control Architecture: Identity proofing: How are asserted identities proofed after originally identified?"[48]
- A new element on intellectual property management, "Content control: How is intellectual property protected?" was added covering elements including ARM literature as well as other literature from other field. This previously existed as embedded in various other components of the SoP and was consolidated because of its prominence in ARM literature.
- New example content types were added to "Overarching: Content: What content does the enterprise have and what are the consequences of protection failures?"[49] This

---

[46] The InterPARES 3 Project. "General Study 15 – Application Profile for Authenticity Metadata." InterPARES. February 1, 2012. Accessed July 7, 2014. http://www.interpares.org/ip3/display_file.cfm?doc=ip3_metadata_application_profiles_final_report.pdf.

[47] International Organization for Standardization, *ISO/IEC 14721:2012 Space data and information transfer systems -- Open archival information system (OAIS) – Reference model*, (Geneva : International Organisation for Standardization, 2012)

[48] The National Technical Authority for Information Assurance & Cabinet Office, "Good Practice Guide No. 45 Identity Proofing and Verification of an Individual," 2.2, (2013), accessed July 14, 2014. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/271266/GPG_45_Identity_proofing_and_verification_of_an_individual_-_issue_2.2_December_2013.pdf.

[49] "Legal documents presumed trustworthy; Historical documents presumed trustworthy; Metadata associated with stored content; Mechanisms used to link content to metadata; Operational information used to support business functions; Provenance information associated with content; Information used to assert integrity of other content; Information used to determine proper accessibility; Archived data in authoritative repositories; Planning information; Mechanisms supporting use of obsolete content forms; Chain of preservation or custody data; Information provided for transparency." Fred Cohen, *Archive Information Protection Standard of Practice*, All.net, accessed August 15 2014 http://all.net/SoP/Archives/index.html.

included specific elements of ARM metadata (as opposed to the less well defined and poorly thought out metadata of the Information Protection field).
- New consequences of protection failures were added to the examples for consideration in "Overarching: Content: What content does the enterprise have and what are the consequences of protection failures?"[50]
- "Legal hold" was given a new emphasis in the Content lifecycle.
- "Migration" was explicitly identified and called out as part of data retention and disposition to bring greater clarity to ARM-related needs.
- All of these changes also included updates to the Basis aspects of these SoP elements so that the written basis for understanding decisions was augmented to reflect added understanding form the ARM literature.

Comparative Analysis

In the following sections, we compare the purpose and scope of the ARM standards and other documents which were compared against the Enterprise Information Protection SoP for the purposes of developing the Archives Information Protection SoP.

InterPARES 2: Benchmark Requirements Supporting the Presumption of Authenticity and Baseline Requirements Supporting the Production of Authentic Copies of Electronic Records[51]

The InterPARES 2 Benchmark and Baseline Requirements were developed to be the most basic conditions in which records and their reproductions can be presumed to be authentic. The majority of the requirements are considered by elements in the SoP.

The SoP contains elements regarding A1 "Expression of Record Attributes and Linkage to Record,"[52] A2 "Access Privileges,"[53] and A3 "Protective Procedures: Loss and Corruption of Records"[54] of the *Benchmark Requirements Supporting the Presumption of Authenticity*. Benchmark Requirement A4 concerns record integrity through media deterioration and technological change. Integrity is an SoP protection objective and the issues of deterioration and change are implicit in elements that concern changes over time such as "Technical Security Architecture: Lifecycles: What aspects of lifecycles are considered in the protection program and its processes?," "Risk Management: Changing systemic risks: How is changing systemic

[50] "Archival information not demonstrably properly controlled; Inability to produce output in usable form; Inability to consume input to proper effect; Inability to properly process content with proper results; Loss of trust in the system or its services." Ibid.

[51] InterPARES 2 project: Authenticity Task Force, "Appendix 2: Benchmark Requirements Supporting the Presumption of Authenticity and Baseline Requirements Supporting the Production of Authentic Copies of Electronic Records," InterPARES 2, (2002), pp. 1-11, http://www.interpares.org/book/interpares_book_k_app02.pdf.

[52] Fred Cohen, "TechArch: Metadata: What Metadata should be ingested, created, retained, and presented?" *Archive Information Protection Standard of Practice*, All.net, accessed August 25 2014, available at http://all.net/SoP/Archives/index.html

[53] Ibid. "Control Architecture: Access Controls: What access control model is used?"

[54] Ibid. "Content control: Version control: How are versions of data over time protected?", "Incidents: Malicious Alteration Detection: How is malicious alteration detected?" and the Redundancy elements among others.

risks managed?," and "Control Architecture: Control Architecture: When is a systematic security architecture created and updated?" The SoP does not contain elements that specifically concern Requirements A5-A8 regarding documentary forms, procedures and rules controlling records authentication, identification of authoritative records, and removal and transfer of relevant documentation. Some or all of these requirements may be identified in "Business modelling: What are the business functions and what information do they depend on for what?" and will be more explicitly covered in the near future.

Unbroken custody is the first of the *Baseline Requirements Supporting the Production of Authentic Copies of Electronic Records* and custody is one of the fundamental protection objectives in the SoP. The SoP's consideration of security issues is much more extensive and specific than Baseline Requirement B1.2, which broadly requires that "Security and control procedures are implemented and monitored." B1.3 requires that "The content of the record and any required annotations and elements of documentary form remain unchanged after reproduction," in other words, that record instances have integrity, which is a fundamental SoP protection objective. Specific elements that concern control and documentation of record reproduction are "Content Control: Version Control" and "Technical Security Architecture: Metadata." B3 "Archival Description" and B2 "Documentation of Reproduction Process and its Effects" were elaborated by InterPARES 3 in the Application Profile for Authenticity Metadata which has been included in the metadata element of the SoP.

DRAMBORA: Digital Repository Audit Method Based on Risk Assessment toolkit[55]

Digital Repository Audit Method Based on Risk Assessment (DRAMBORA) was developed by Digital Curation Centre (DCC) and Digital Preservation Europe (DPE) in 2006-2007. DRAMBORA is a self-assessment online tool and audit methodology that encourages users to do a full survey of the their organizational systems and context before developing a unique risk profile. The 2007 public draft of the DRAMBORA method includes an appendix with example risk descriptions with an area on technical infrastructure and security.

Unlike the SoP, DRAMBORA does not differentiate between threat actors (heretofore "threats"),[56] vulnerabilities, attack mechanisms and consequences: security vulnerability, exploitation of a security vulnerability, and loss of confidentiality (a potential consequence of the previous) are each identified in DRAMBORA as risks.[57] Vulnerabilities, threats, attack mechanisms and consequences are addressed separately in the SoP as elements of risk. Within the more extensive Risk Management section of SoP, organizations are asked to identify specific threats and attack mechanisms that could pose harm to the organization and there is an element regarding how the organization assesses vulnerability, a decision that is based on risk

---

55 Digital Curation Centre (DCC) and DigitalPreservationEurope (DPE), "Digital Repository Audit Method Based on Risk Assessment," Version 1.0 (draft), February 28 2007, p. 1-221, http://www.repositoryaudit.eu/download/.

56 Many dictionaries define 'threat' as something like "a person or thing that threatens," and 'to threaten' as "to be a menace or source of danger to" (Dictionary.com, "threat."). The term "threat actor" is used here to differentiate threat from the more common usage which is imprecise and usually nebulous.

57 Digital Curation Centre (DCC) and DigitalPreservationEurope (DPE), "Digital Repository Audit Method Based on Risk Assessment," Version 1.0 (draft), February 28 2007, , p. 169-170, 186.

level and maturity level. Specific vulnerabilities are not addressed in one element, however the SoP implicitly anticipates numerous areas of potential vulnerability, both human and technological, throughout its 111 elements. Under “Risk Management: Threats: What attack mechanisms are considered?,” the SoP identifies scores of “attack mechanisms,” each representing a class of potential vulnerabilities, and supports use of an automated tool to rank these. In the “Risk Management: Vulnerabilities: How and when are information-related vulnerabilities assessed?” SoP element, decisions about vulnerability assessment are included as well. In addition to the risk management analysis, the SoP includes elements regarding the ways in which the organization may fail to protect the integrity, availability, confidentiality, use-control, accountability, transparency and custody of the content it manages in the Control Architecture.[58]

A major difference between DRAMBORA and the SoP is the value used to measure “risk.” The term “risk” is one that is commonly debated in the relevant communities, and metrics surrounding risk are often poorly defined and used. The consequence metrics used throughout the SoP include potential wasted time and effort (inefficiency), substantial negative publicity, acts viewed as gross negligence, substantial enterprise value reduction, serious bodily harm, environmental damage, societal harm, loss of (human) life, enterprise collapse, and other dire consequences, as detailed in the “Overarching: Content: What content does the enterprise have and what are the consequences of protection failures?” element. The SoP analysis is oriented to the institution as a holistic whole, not only risks that seem to directly affect the content. At a conceptual level, this is because the SoP takes the perspective that the job of Information Protection is to “assure the utility of content.”[59] DRAMBORA asks users to consider risk with respect to potential loss of authenticity and understandability of the repository's holdings, the “ultimate practical expression of failure for repositories that are auditable using this toolkit.”[60] DRAMBORA's focus on archival loss seems to overlook the ways in which other types of loss, such as financial loss, might have a collateral effects on the sustainability of the archives, and perhaps more importantly, the larger potential effects of archival failures on the rest of society. The term “risk” in the SoP is somewhat unclear, but it notionally identifies risk as a combination of consequences and threats in which risks are higher as each of these increase.

SPOT (Simple Property-Oriented Threat) Model for repository risk assessment[61]

The SPOT model is a lightweight, outcomes-based risk assessment for digital preservation. Based on a review of digital preservation literature, the SPOT model identifies six principles of digital preservation, characterized as properties of a well-preserved object: availability, identity,

---

[58] Fred Cohen, “Overarching: Content: What content does the enterprise have and what are the consequences of protection failures?” *Archive Information Protection Standard of Practice*, All.net, accessed August 25 2014, available at http://all.net/SoP/Archives/index.html.

[59] Fred Cohen, *Enterprise Information Protection*, All.net, accessed August 25 2014, available at http://all.net/SoP/SecDec/index.html.

[60] Andrew McHugh, Raivo Ruusalepp, Seamus Ross, and Hans Hofman, "Digital Repository Audit Method Based on Risk Assessment," *Digital Curation Centre (DCC) and DigitalPreservationEurope (DPE)* (2007), p. 84F.

[61] Sally Vermaaten, Brian Lavoie, and Priscilla Caplan. "Identifying Threats to Successful Digital Preservation: the SPOT Model for Risk Assessment." *D-Lib Magazine* 18, no. 9 (2012): 4.

persistence, renderability, understandability, and authenticity. The repository applying the SPOT risk assessment is asked to identify possible threats to each property and mitigation strategies. The SPOT model encourages users to focus on the part of the preservation management process in which each property is most vulnerable and includes suggestions "regarding the parts of the digital preservation process most relevant to a particular property-threats combination."

There are some differences between the SPOT model's principles and the SoP's protection objectives. The SoP is based on the seven following protection objectives: integrity, availability, confidentiality, use control, accountability, transparency, and custody. The conceptual fields of identity, persistence and authenticity in the SPOT model overlap with those of integrity and custody in the SoP. However, the SPOT model does not specifically include concepts of accountability, transparency and confidentiality. The SoP does not specify the concept of renderability as a protection objective, although it is implicit in the concepts of use control and availability. In particular, availability is identified with "Access," which in the "Control Architecture: Access facilitation: How is access facilitated once identity is adequately established?" section is defined as "access: the granting of capabilities to examine, modify, delete, add to, or otherwise apply content to gain utility." It is the last part that encompasses renderability. Additional consideration is given under "Technical Security Architecture: Lifecycles: What aspects of lifecycles are considered in the protection program and its processes?" which includes content and within content includes "Use," "Presentation," and "Disposition" elements. Under "Use," it states "When in use, data must be in usable form." Under "Presentation," it states, among other things, "It is critical that the presentation accurately represent the intent of the application." Under "Disposition," "Migration" is considered and includes "accessibility in a useful form for content from systems that are obsolescent or obsolete," and similar language. In SPOT, "The concept of renderability was an important addition to the canon, as it encapsulated to some extent the discussion of content in the Waters report as the "knowledge or ideas the object contains," recognizing that it might be necessary to transform the original bits of an object in order to ensure that its content can be rendered (delivered) with current technologies."[62]

The SoP includes a protection objective analysis that is similar to the SPOT model, but much more demanding.[63] The repository is asked to estimate the consequences in the event of a failure to maintain each protection objective for every major type of content stored by the institution. Examples are provided, such as "Confidential or proprietary financial data."

The SoP's Risk Management section takes risk analysis far beyond the scope of the SPOT model. The Risk Management section includes elements on the risk management process; the avoidance, acceptance and transfer of risks; threats (actors), attack mechanisms, and vulnerabilities; risk aggregation; separation of duties; interdependencies; costs; surety matching; failsafes; changing systemic risks and changing subsystem risks.

---

[62] Ibid.

[63] Fred Cohen, "Overarching: Content: What content does the enterprise have and what are the consequences of protection failures?" *Archive Information Protection Standard of Practice*, All.net, accessed August 25 2014, available at http://all.net/SoP/Archives/index.html.

Audit and Certification of Trustworthy Digital Repositories (ISO 16363)[64]

The *Audit and Certification of Trustworthy Digital Repositories Recommended Practice* was published by the Consultative Committee for Space Data Systems (CCSDS) in 2011 and adopted by the International Standards Organization (ISO) in 2012 with the identification ISO 16363. ISO 16363 is based on the Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC), developed by the Research Libraries Group (RLG) and the National Archives and Records Administration (NARA) in 2003. The original TRAC was itself based on the CCSDS OAIS Reference Model (ISO 14721).

Each requirement is followed by an explanation of how the repository could demonstrate compliance with the requirement, often in the form of documentation. Each of the Security Risk Management requirements recommend that the repository follow the codes of ISO 27000 and that it has documentation of completed analysis, controls in place and preparedness. It does not specify, however, how the analysis and controls that are documented should be technically performed or how often. The ISO 27000 series were among the standards consulted when the Enterprise Information Protection SoP was developed. In the Archives and Enterprise Information Protection SoP, "GAISP, COSO, ISO-27001, ISO-27002, and industry-specific standards" are recommended as the bases for application in large, commercial enterprises or institutions with a maturity level of Defined or higher.

The scope of the SoP does not include most of the criteria of the Digital Object Management section of ISO 16363 and does not prescribe financial sustainability, preservation planning, or the definitions and controlled transformations of the repository's Submission Information Packages (SIP), Archival Information Packages (AIP) and Dissemination Information Packages (DIP). Criteria that the repository designates its primary users and that the repository monitor the designated community and make digital content available and usable based on community needs are also beyond the scope of the SoP. The SoP is a neutral evaluative tool rather than a certification criteria with regards to the institution's core responsibilities. In the Overarching: Promises element, the institution must describe the promises it makes, to whom and why, while in the Oversight section, the institution describes how it prioritizes, documents and analyses its duties to protect.[65] The SoP was augmented to include a simplified form of the OAIS model, but generally does not advise on specifics to the level of ISO 16363.

Nestor Seal for Trustworthy Digital Archives[66]

---

[64] Consultative Committee for Space Data Systems (CCSDS), "Audit And Certification Of Trustworthy Digital Repositories," CCSDS 652.0-M-1, *Recommended Practice*, 1 (2011), pp. 1.1-B.1 http://public.ccsds.org/publications/archive/652x0m1.pdf.

[65] Fred Cohen, "Overarching: Promises: What promises does the archive make, to whom, and why? How do they relate to information?" *Archive Information Protection Standard of Practice*, All.net, accessed August 25 2014, available at http://all.net/SoP/Archives/index.html.; Ibid "Oversight: How are different sorts of duties prioritized in determining what to protect and how well?"

[66] Henk Harmsen, Christian Keitel, Christoph Schmidt, Astrid Schoger, et al., "Explanatory notes on the nestor Seal for Trustworthy Digital Archives," nestor Certification Working Group, (2013), p. 1-40, http://files.d-nb.de/nestor/materialien/nestor_mat_17_eng.pdf.

The nestor (Network of Expertise in long-term STORage and accessibility of digital resources in Germany) Catalogue of Criteria for Trusted Digital Repositories are based on DIN 31644 and the OAIS Reference Model. The nestor criteria are available in German and English and are designed for self-assessment of memory institutions, including archives, libraries, and museums. After a positive review from the nestor working group, a compliant repository may be awarded with the nestor Seal for Trustworthy Digital Archives.

In order to be compliant with nestor, a repository must identify the characteristics of the digital objects that must be preserved. The documentary and functional characteristics that are selected as essential to preserve is inevitably balanced between the technical possibilities and needs of user community. Similarly, the repository must define its SIPs, AIPs and DIPs with regard to their structure, format and metadata, and it must control and document any transformations performed. The digital repository must also provide representation information through documentation, software, format transformation, emulation, instructions, or other means. Nestor points to IT infrastructure and security of the digital repository in the last two criteria (C33 and C34) and requires documentation for the IT infrastructure “in abstract terms, [and] its operation need not be comprehensively tested.”[67] The SoP fills this gap in nestors' applicability to IP by turning the lens of IP to the ARM institution as a whole rather than as one of the less emphasized criteria.

Many of the nestor criteria are addressed in the SoP framework, including criteria C1 to C3, and C6 to C11 in the Overarching sections on the ARM institution's mission, promises, and legal duties. C13 on evaluating the institution's assets is a requirement for the process of risk management that the SoP uses to evaluate risk within the organization. C14 on integrity and ingest is addressed in the control architecture section of the SoP as well as being an explicit part of the protection objectives within the SoP. C15 to C19 concerning authenticity are also addressed in the SoP control architecture. C27 on identifiers are addressed through the Zone section of the SoP in detail. C28 to C32 concerning specific metadata are addressed in the metadata table provided for in the Technical security architecture – metadata section.

Nestor criteria C4 requires the institution to provide suitable search capacity for users to access the material which the SoP does not address explicitly outside of assuring access to different levels of users as necessary. Criteria C12 on crisis or successor management is not explicitly developed in the SoP, but left to the institution to address within its own documentation. Criteria C20 recommends that ARM institutions retain the right to migrate digital content into accessible formats. The SoP does not recommend this tactic specifically but rather, in addressing the issues of access and migration throughout the framework, provides for the process for ARM institutions to assure access and migration capabilities for records created and ingested. Criteria 21-26 address SIPs AIPs and DIPs which, as previously discussed, are not included in the scope of the framework.

The nestor criteria explicitly require that the repository monitor changes in technology and the user knowledge base and conduct long-term preservation planning. The SoP references preservation planning under OAIS, but really deals with the long term issues under “Technical

[67] Ibid., p 39.

Security Architecture: Lifecycles: What aspects of lifecycles are considered in the protection program and its processes?“ and in issues related to backup storage media. Lifecycles in the SoP include business, people, systems, and content, each of which involves a “womb to the tomb” or longer chain of issues. It does not contain recommendations regarding the total scope of the long-term vision of the institution. Rather, the SoP relies on the institution to provide its own long-term vision for the institution during the application of the SoP and review process, and use of the SoP will likely inform the long-term vision by revealing gaps in the current IP approach and practices as well as alternative approaches. Based on the long-term vision of the institution, the SoP recommends lifecycle issues to be addressed, and provides reasonable and prudent alternatives for how each should be addressed in any particular situation.

Nestor specifically recommends use of digital signatures for both ingest and dissemination for the purposes of authentication on receipt, not confidentiality. It requires that the repository provide ways for users to be sure of technological integrity of the disseminated objects through the application of metadata and digital signatures. While the SoP includes elements regarding when data at rest and in motion should be encrypted, it does not specify the type of encryption, as this is not really the issue for preservation. Rather, the use of digital signatures in the SoP is related to integrity. For example, 'Modification' under 'Content' in the Lifecycles element in the SoP states: “Malicious modification of data is highly undesirable and protection typically involves the use of cryptographic checksums for detection and access controls for prevention.”[68] Other references to integrity include logically secured infrastructure in “Overarching: Location: Where are content and work located” and the notion of freedom from alteration in “Control Architecture: Objectives: What are the protection objectives and how are they applied,” along with which is noted “cryptography has serious limitations in integrity protection.”[69] However, cryptographic protocols and checksums on traffic and/or content are included as part of “connection controls” and digital signatures is included as a type of checksum under one of the options. Cryptographic protocols used in conjunction with normal access controls or microzone controls to prevent interception and/or alteration of control and data en-route as part of microzoning strategy is also noted in the SoP. In any case, beyond cryptography and digital signatures for integrity in transfer, a more encompassing application of the principle of integrity includes aspects of securing the ARM infrastructure. Nestor criteria 6.3 notes “The [digital repository] should ensure that no unauthorised user can obtain rights over digital objects, metadata or other system elements,”[70] while the SoP asks the ARM institution “What access control model is used?”[71] within the larger Control Architecture element in order to address the need for both the integrity of the records in the system, as well as access by intended users.

Much of the nestor criteria are specifically addressed in the SoP framework and in greater depth than simple documentation. The SoP provides the ARM institution with reasonable and prudent alternatives based on the circumstances and from an Information Protection perspective. For

---

[68] Fred Cohen, *Archive Information Protection Standard of Practice*, All.net, accessed August 25 2014, available at http://all.net/SoP/Archives/index.html.

[69] Ibid.

[70] Nestor Working Group on Trusted Repositories Certification, *Catalogue of Criteria for Trusted Digital Repositories,* Version 1, Frankfurt am Main: nestor c/o Deutsche Nationalbibliothek 2006. July 12, 2014. http://edoc.hu-berlin.de/series/nestor-materialien/8en/PDF/8en.pdf. p. 21.

[71] Fred Cohen, *Archive Information Protection Standard of Practice*, All.net, accessed August 25 2014,

the criteria addressed in the Overarching elements, the process of using the SoP tool will provide the institution the opportunity to begin documentation if they have not done so already.

Aboriginal and Torres Strait Islander Library, Information, and Resource Network Protocols (ATSILIRN)[72]

The protocols are not intended as IP directives but rather a guide for libraries, archives, and information services in appropriate ways to interact with communities as well as handle content. In circumstances where material related to aboriginal groups is held by the archival institution, the protocols point to an additional concern with copyright. Aside from the rights of the creator, the community considers itself owners of the culture, and as such possessing the moral rights to protect their cultural and intellectual property. In Canada, moral rights include the author's right to the integrity of the work, as well as the right to be associated with the work, and cannot be assigned, only waived. The SoP folds issues like moral rights into intellectual property. Intellectual property is a factor in risk management and moral rights are included in that consideration. SoP requires institutions to state what promises they are required to uphold as an institution and in terms of important relationships between groups, the ATSILIRN provides greater insight as to how that might be negotiated between an ARM institution and local aboriginal communities. Rights are also covered in the SoP under legal elements. Specifically, legal mandates are identified as part of the “duty to protect” area, and process by which legal mandates are fulfilled are identified in the SoP in a variety of places, ranging from workflow controls to governance. However, because of the large number and high rate of change associated with laws on a global basis, the SoP does not address individual laws on a case by case basis.

Data Seal of Approval Guidelines (DSA)[73]

The Data Seal of Approval (DSA) is a self-assessment tool based on sixteen guidelines and five criteria measuring quality characteristics in the creation, (re-)use and storage of digital research data. It was created by the Data Archiving and Networked Services (DANS), itself a product of two Dutch science organizations, and focuses on the potential for research data to be reused by other researchers after its final disposition. DSA gives guidelines for three groups of stakeholders: data producers, data repositories, and data consumers and focuses on the data repository as a support for the creators and (re)users of the records. The five criteria, which determine whether or not the digital research data may be qualified as “sustainably archived,” are as follows:

• The research data can be found on the Internet.
• The research data are accessible, while taking into account relevant legislation with regard to personal information and intellectual property of the data.
• The research data are available in a usable format.
• The research data are reliable.

---

[72] *The Protocols*, Aboriginal and Torres Strait Islander Library, Information and Resource Network Inc. http://aiatsis.gov.au/atsilirn/protocols.php.

[73] Data Seal of Approval Board, “Data Seal of Approval Guidelines,” Version 2, (July 19, 2013), http://www.datasealofapproval.org/media/filer_public/2013/09/27/guidelines_2014-2015.pdf.

• The research data can be referred to.[74]

DSA notes interoperability with the above mentioned standards: nestor, TRAC, and DRAMBORA, as well as others. While DSA is designed specifically with scientific and scholarly data in mind, it can be applied to all types of digital data or digital objects. DSA *Guidelines* are generally addressed by the SoP in the areas of metadata provision; legal and contractual compliance; documentation of processes and procedures; workflows and data lifecycles; access controls and regulations; technical infrastructure; and maintenance of data authenticity and integrity through chain of custody, audit, and version control mechanisms.

While the first 3 guidelines are directed at data producers rather than repositories and institutions, Guideline 1 also suggests that information about the methods and techniques of data creation and collection should be made explicit to users to facilitate assessment of legal and ethical compliance of the data collection. This methodological information could be incorporated as metadata.[75] The SoP has been augmented to include transparency as a protection objective, and as such, this is covered.

Guideline 4 of the DSA requires that repositories establish an explicit mission for digital preservation, including having a succession plan in place for digital assets and ensuring compliance by third party service providers with DSA, DIN, or ISO standards. The SoP model provides for DSA compliant institutions by asking organizations to describe their mission as well as any promises they make and their purpose. The Management and Risk Management sections of the SoP address standards compliance and personnel, while the issues attendant to using third party service providers, including regulatory compliance and archival control, are found in the section “Overarching: Outsourcing Things” as well as under interdependencies and related areas.

DSA Guidelines 2, 7 and 10 address the concerns of file formats and obsolescence issues, which may be mitigated by long-term digital preservation planning (Guideline 7) and the use of preferred formats for digital objects (Guideline 2 and 10). Preferred formats are not given, but assumed to be developed within the context of the repository and the research discipline preferences and needs. Preferred formats for ingest, storage and access are not addressed in such terms in the SoP, however the issues of system obsolescence and content transforms and presentation are referenced as medium-risk aspects of lifecycle control and migration in the Lifecycles element.[76]

Guidelines 11 and 12 note integrity and authenticity, which are included in the SoP protection objectives. Guideline 13, on technical infrastructure, is addressed in much more depth in the

---

[74] Data Seal of Approval Board, “Data Seal of Approval : Quality guidelines for digital research data” Version 2, (2013) https://assessment.datasealofapproval.org/media/files/DSA_booklets/DSA-booklet_1_June2010_1.pdf.

[75] Fred Cohen, “Techarch: Metadata: What Metadata should be ingested, created, retained, and presented?” *Archive Information Protection Standard of Practice*, All.net, accessed August 25 2014, available at http://all.net/SoP/Archives/index.html.

[76] Ibid. “TechArch: Lifecycles: What aspects of lifecycles are considered in the protection program and its processes?”

SoP technical security architecture section, which folds aspects of Guideline 8: workflows and lifecycles of information objects into the architecture of the institution as a whole. While guideline 13 presumes use of the OAIS model, both the SoP and the Guidelines allow for other standards and institutional requirements to take priority.

The final three guidelines are directed at users rather than the ARM institutions, however it is also a reminder for institutions to document access rules, codes of conduct, and applicable licenses for the material accessible to its users. The SoP presumes as well that each institution will produce its own policies and documentation based on its previously described legal and other obligations within the Overarching section of the framework. Users who do not follow access rules and codes of conduct are addressed in the SoP sections on risk management and specifically the potential human vulnerabilities in the system as well as potential threats.

Overall, the *Guidelines* focus on publicly available data in data repositories, while the SoP broadly focuses on being applicable to a variety of material and institutional circumstances. The expectation that all documentation will be available on the Internet to aid transparency is addressed in the SoP protection objectives framework in order to respect the balance with other IP concerns for ARM records.

ICA Principles of Access to Archives: Technical Guidance on Managing Archives with Restrictions[77]

The International Council on Archives (ICA) *Technical Guidance on Managing Archives with Restrictions* was published in 2014. The document provides guidance on how to implement restrictions on holdings in archival repositories. The *Guidance* was written to integrate with the ICA's 2012 *Principles of Access to Archives*, which address "the legal authority to consult archives."[78]. While the Principles are general, the Guidance is more specific, offering practical advice on the "legitimate withholding of materials in an archival institution."[79] Whether that be "as required by laws and other authorities, ethics, or donor requirements"[80] The *Guidance* covers activities such as the development of an access policy; setting access restrictions at the time of materials acquisition; control of access to restricted materials; description of restricted materials; decision-making, implementing, and documenting access restrictions; requests for restricted materials; and the release of formerly restricted materials.

---

[77] International Council on Archives Committee On Best Practices And Standards Working Group On Access, "ICA Principles of Access to Archives: Technical Guidance on Managing Archives with Restrictions," 2014, p. 1-23, http://www.ica.org/15369/toolkits-guides-manuals-and-guidelines/technical-guidance-on-managing-archives-with-restrictions.html.

[78] ICA Committee on Best Practices and Standards Working Group on Access "Principles of Access to Archives : a Success for Transparency and Right to Information," 2012, p. 3.

[79] International Council on Archives Committee On Best Practices And Standards Working Group On Access, "ICA Principles of Access to Archives: Technical Guidance on Managing Archives with Restrictions," February 01 2014, p. 1-23, http://www.ica.org/15369/toolkits-guides-manuals-and-guidelines/technical-guidance-on-managing-archives-with-restrictions.html, p. 3.

[80] Ibid. p 2.

The SoP provides guidance on what access control method to use, but is agnostic with regard to the purpose of access controls and the circumstances of implementation. Consequently, it anticipates a larger number of access control types than the *Guidance*, including “clearances, classifications, and compartments” as one of the approaches. The activities of decision-making, implementing, and documenting access restrictions are broadly covered and abstracted in the SoP in the areas of Business Modelling, Content Control, Technical Architecture and Management. The SoP does not specifically address topics such as redaction methods, requests for restricted materials and the reclassification of materials.

The SoP provides a more detailed consideration of some of the issues addressed by the Guidance, for example in the physical and internal (i.e. staff access) and control of archival holdings (D and E). On the subject of the description of restricted materials (F), one notable difference between the SoP and the Guidance is that in the former, description is addressed through metadata, while in the latter, the focus is on the production of finding aids.

Within the Overarching element, the SoP addresses certain duties the ARM institution may be cognizant of, for example: Legal and regulatory duties, Contractual duties, Chief Executive defined duties. Board defined duties, Owner-defined duties, Auditor or other external source duties, Line management defined duties and/or by conduct. In contrast the *ICA Principles of Access to Archives* points to the awareness of donor agreements (7) in access policies specifically. The duties created by donor agreements can be seen under “Contractual duties” and “are also addressed by the SoP requirement that ARM institutions spell out all promises and related duties under Overarching element “What Promises Does The Archive Make, To Whom, And Why?”[81]

The SoP provides more in the way of security implementation possibilities for thinking through the specific circumstances of access and restriction to records or data within an ARM institution. Guidance provides more information from an ARM policy and procedures perspective while the SoP presumes restricted material will be one aspect of the concerned ARM institution and provides reasonable and prudent options for securing the material.

ISO 15489:2001 Information and documentation -- Records management[82]

ISO 15489 was considered during the development of the SoPs and a sentence-by-sentence mapping was made between ISO 15489 and several other ISO standards. It appears that all of the elements of the mapped standards are present in the SoP. However, the structure of the SoP is significantly different than the structure of the ISO standard, and as such these are many-to-many mappings.

Conclusions

---

[81] Fred Cohen, *Archive Information Protection Standard of Practice*, All.net, accessed August 25 2014, available at http://all.net/SoP/Archives/index.html.

[82] IInternational Organization for Standardization, *ISO/IEC 15489:2001 Information and documentation -- Records management,* Geneva : International Organisation for Standardization, 2001.

Thus far, the initial literature review has been completed. Differences in scope between ARM literature and the SoP are apparent. The ARM literature places methodological risk management and computer security secondary to archival management. It typically does not take into account maturity and risk levels and other differing requirements of institutions. ARM literature is prescriptive with respect to the professional responsibilities of archives, while permissive as to how archives implements and achieves these responsibilities. The SoP makes recommendations about issues which impact long-term preservation planning and content management, but allows the institution to define its specific requirements in those areas. It collects information about the institution's mandate and responsibilities, but does not define the purpose of the institution for the institution. At the same time, the SoP is much more granular than most of the ARM literature reviewed, making practical recommendations about specific operations and processes in the IP systems based on the circumstances and context of the institution.

As mentioned previously, the next step in the SoP study is to apply the SoP in ARM environments. The team is in the process of soliciting the professional opinions of practicing ARM experts on whether the SoP's rote recommendations are reasonable and prudent for the interviewed institutions. This is necessary to ensure the SoP is both an accurate reflection of the target audience and a useful tool in evaluating IP practices. The InterPARES Trust research project represents a multi-national investment by the ARM community into these issues of IP and trust in digital records and data housed on the Internet. As can be seen from the long histories of both ARM and IP in society, the IP practices of ARM institutions are ever more important and intricate in a networked digital environment and the ARM SoP represents an important piece of work in developing the ARM community's sophistication in approach to information protection.

Acknowledgements

Dr. Fred Cohen is the principal researcher of Project NA03 of InterPARES Trust, the Archives Information Protection Standard of Practice (SoP) project. The project is also known as the ‘Standard of practice for trust in protection of authoritative records in government archives.’ In 2013-2014, three University of British Columbia School of Library, Archival and Information Studies graduate students -- Mel Leverich, Meghan Whyte, and Eng Sengsavang -- have assisted the project, and Corinne Rogers, Luciana Duranti, and Alexandra Bradley have advised.

Bibliography

Becker, Christoph, Gonçalo Antunes, José Barateiro, Ricardo Vieira, and José Borbinha. "Control objectives for dp: Digital preservation as an integrated part of it governance." *Proceedings of the American Society for Information Science and Technology* 48, no. 1 (2011): 1-10.

Brenner, Susan W. ‘‘History of Computer Crime.’’ In *The History of Information Security: a Comprehensive Handbook.* Ed. Karl de Leeuw, Maria Michael, and Jan Bergstra, 705-721. Boston: Elsevier, 2007.

Canadian System Security Centre *Canadian Trusted Computer Product Evaluation Criteria*. Ottawa: Canadian System Security Centre, 1993.

Cohen, Fred. *Archive Information Protection Standard of Practice.* All.net, accessed August 15 2014 http://all.net/SoP/Archives/index.html.

Cohen, Fred. *Enterprise Information Protection Standard of Practice*. All.net, accessed July 7 2014, available at http://all.net/SoP/SecDec/index.html

Cohen, Fred. *Fearless Security.* All.net, accessed July 7 2014, available at http://courses.all.net/index.html

Commission of the European Communities. *Information Technology Security Evaluation Criteria*: P*reliminary Harmonised Criteria.* Luxembourg: Office for Official Publications of the European Communities, 1991.

Consultative Committee for Space Data Systems (CCSDS), “Audit And Certification Of Trustworthy Digital Repositories,” CCSDS 652.0-M-1, Recommended Practice, Issue 1, September 2011, pp. 1.1-B.1 http://public.ccsds.org/publications/archive/652x0m1.pdf

Consultative Committee for Space Data Systems. *Producer-Archive Interface Methodology Abstract Standard*. Washington: CCSDS Secretariat, 2002. July 12, 2014. www.ccsds.org/publications/archive//651x0b1.pdf.

Consultative Committee for Space Data Systems. *Reference Model for an Open Archival Information System*. Washington: CCSDS Secretariat, 2002. July 12, 2014. www.ccsds.org/publications/archive/650x0b1.pdf.

Cook, Terry. "Easy to Byte, Harder to Chew: The Second Generation of Electronic Records Archives." *Archivaria* 33, no. 1 (1991): 202-216. http://journals.sfu.ca/archivar/index.php/archivaria/article/view/11812/12763.

Data Seal of Approval Board, “Data Seal of Approval Guidelines,” Version 2, (July 19, 2013), http://www.datasealofapproval.org/media/filer_public/2013/09/27/guidelines_2014-2015.pdf

Data Seal of Approval Board, “Data Seal of Approval : Quality guidelines for digital research data” Version 2, (July 19, 2013) https://assessment.datasealofapproval.org/media/files/DSA_booklets/DSA-booklet_1_June2010_1.pdf

Department of Defense. *Department of Defense Trusted Computer System Evaluation Criteria.*Washington: Department of Defense, 1986.

Duff, Wendy. “Ensuring the Preservation of Reliable Evidence: A Research Project Funded by the NHPRC.” *Archivaria* 42, no. 1 (1996): 28-45.

Duranti, Luciana. “The Long-Term Preservation of Authentic Electronic Records.” In P*roceedings of the 27th VLDB Conference, Roma, Italy*. Ed. P.M.G. Aspers et al. Orlando, FL: Morgan Kaufmann, 2001. http://www.vldb.org/conf/2001/P625.pdf.

Duranti, Luciana and Heather MacNeil. “The Protection of the Integrity of Electronic Records: An Overview of the UBC-MAS Research Project.” *Archivaria* 42 no 1. (1996): 46-67.

Gnanadesikan, Amalia E. *The Writing Revolution: Cuneiform to the Internet.* Malden, MA: Wiley-Blackwell, 2009.

Gollman, Dieter. "Security Models.” In *The History of Information Security: a Comprehensive Handbook.* Ed. Karl de Leeuw, Maria Michael, and Jan Bergstra, 623-635. Boston: Elsevier, 2007.

International Council on Archives Committee On Best Practices And Standards Working Group On Access, “ICA Principles of Access to Archives: Technical Guidance on Managing Archives with Restrictions,” February 01 2014, p. 1-23, http://www.ica.org/15369/toolkits-guides-manuals-and-guidelines/technical-guidance-on-managing-archives-with-restrictions.html

International Council on Archives Committee On Best Practices And Standards Working Group On Access. “Principles of Access to Archives : a Success for Transparency and Right to Information,” (August 24, 2012)

InterPARES. “Authenticity.” *The InterPARES 2 Project Dictiona*ry. July 12, 2014. http://www.interpares.org/ip2display_file.cfmdoc=ip2_dictionary.pdf&CFID=4164403&CFTOKEN=69638790.

The InterPARES 2 Project, Authenticity Task Force. “Appendix 2: Benchmark Requirements Supporting the Presumption of Authenticity and Baseline Requirements Supporting the Production of Authentic Copies of Electronic Records.” InterPARES 2. March 2002, pp. 1-11. http://www.interpares.org/book/interpares_book_k_app02.pdf

The InterPARES 3 Project. "General Study 15 – Application Profile for Authenticity Metadata." InterPARES. February 1, 2012. Accessed July 7, 2014. http://www.interpares.org/ip3/display_file.cfm?doc=ip3_metadata_application_profiles_final_report.pdf.

ISACA. *COBIT 4.1: Framework for IT Governance and Control.* 2007. July 14, 2014. http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx.

Information Systems Security Association. *Generally Accepted Information Security Principles* v. 3.0. ISSA, 2005.

International Organization for Standardization. *ISO/IEC 14721:2012 Space data and information transfer systems -- Open archival information system (OAIS) – Reference model*. Geneva : International Organisation for Standardization, 2012.

International Organization for Standardization. *ISO 9798-1:2010 Information Technology — Security Techniques—Entity Authentication*. Geneva : International Organisation for Standardization, 2010.

International Organization for Standardization. *ISO 15408-1:2009 Information Technology — Security Techniques—Evaluation Criteria for IT Security*. Geneva : International Organization for Standardization, 2009.

International Organization for Standardization. *ISO/IEC 15489:2001 Information and documentation -- Records management.* Geneva : International Organisation for Standardization, 2001.

International Organization for Standardization. *ISO 17799:2005 Information Technology—Security Techniques—Code of Practice for Information Security Management.* Geneva : International Organization for Standardization, 2005.

McHugh, Andrew, Raivo Ruusalepp, Seamus Ross, and Hans Hofman. "Digital Repository Audit Method Based on Risk Assessment." *Digital Curation Centre (DCC) and DigitalPreservationEurope (DPE)* (2007).

National Institute of Standards and Technology. *Advanced Encryption Standard FPS 197-12*. Gaithersburg, MD : Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 2001.

National Institute of Standards and Technology. *Digital Signature Standard (DSS) 186-2.* Gaithersburg, MD : Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 2000.

National Institute of Standards and Technology. M*inimum Security Requirements for Federal Information and Information Systems 200.* Gaithersburg, MD : Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 2006.

National Institute of Standards and Technology. *Personal Identity Verification (PIV) of Federal Employees and Contractors 201-1*. Gaithersburg, MD : Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 2006.

National Institute of Standards and Technology. *Security and Privacy Controls for Federal Information Systems and Organization Special Publication (SP) 800-53 Revision 4*. Gaithersburg, MD : Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 2013.

National Library of Australia. *Guidelines For The Preservation Of Digital Heritage.* Information Society Division United Nations Educational, Scientific and Cultural Organization, 2003. July 12, 2014. http://unesdoc.unesco.org/images/0013/001300/130071e.pdf.

The National Technical Authority for Information Assurance & Cabinet Office. "Good Practice Guide No. 45 Identity Proofing and Verification of an Individual." Issue 2.2, December 2013. Accessed July 14th 2014 from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/271266/GPG_45_Identity_proofing_and_verification_of_an_individual_-_issue_2.2_December_2013.pdf

Nestor Working Group on Trusted Repositories Certification. *Catalogue of Criteria for Trusted Digital Repositories.* Version 1. Frankfurt am Main: nestor c/o Deutsche Nationalbibliothek 2006. July 12, 2014. http://edoc.hu-berlin.de/series/nestor-materialien/8en/PDF/8en.pdf.

Perrin, Chad. *The CIA Triad*. (2008). July 14, 2014. http://www.techrepublic.com/blog/it-security/the-cia-triad/.

PREMIS Working Group. *Data Dictionary for Preservation Metadata: Final Report of the PREMIS Working Group.* Dublin, OH : OCLC and RLG, 2005. July 12, 2014. www.oclc.org/research/projects/pmwg/premis-final.pdf.

The Protocols. Aboriginal and Torres Strait Islander Library, Information and Resource Network Inc. http://aiatsis.gov.au/atsilirn/protocols.php

Ruiu, Dragos. "Learning from Information Security History." *IEEE Security and Privacy* 4 no. 1 (2006): 77-79.

Salzer, Jerome H. “Basic Principles of Information Protection.” In *The Protection of Information in Computer Systems*. July 14, 2014. http://web.mit.edu/saltzer/www/publications/protection/Basic.html.

van Biene-Hershey, Margaret. "IT security and IT Auditing Between 1960 and 2000." In *The History of Information Security: a Comprehensive Handbook.* Ed. Karl de Leeuw, Maria Michael, and Jan Bergstra, 665-680. Boston: Elsevier, 2007.

Vaughan v Menlove, (1837) 3 Bing. N.C. 467, 132 E.R. 490 (C.P.).

Vermaaten, Sally, Brian Lavoie, and Priscilla Caplan. "Identifying Threats to Successful Digital Preservation: the SPOT Model for Risk Assessment." *D-Lib Magazine* 18, no. 9 (2012): 4.

Waters, Donald and John Garrett. P*reserving Digital Information: Report of the Task Force on Archiving of Digital Information*. Washington: The Commission on Preservation and Access, Research Libraries Group,1996. http://www.clir.org/pubs/reports/pub63.

Yost, Jeffrey R. “A History of Computer Security Standards.” In *The History of Information Security: a Comprehensive Handbook.* Ed. Karl de Leeuw, Maria Michael, and Jan Bergstra, 595-621. Boston: Elsevier, 2007.