Limited consensus around ARM information protection practices[1]

Fred Cohen
Management Analytics
Webster University
Email: fc@all.net

Mel Leverich; Meghan Whyte; Eng Sengsavang & Grant Hurley
Graduate Research Assistants
Schol of Library, Archival and Information Studies, University of British Columbia, Vancouver, Canada

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 and practice is consistent with or divergent from IP literature and practice. This paper compares IP and ARM information protection through the lens of a Standard of Practice (SoP). An existing enterprise IP SoP was adapted to ARM through literature analysis and produced a draft ARM SoP. The draft ARM SoP was applied in a rote fashion to a small sample of government-operated archives to identify likely areas of consensus and lack of consensus surrounding the various elements of the SoP. This resulted in some areas of strong consensus and other areas of strong divergence. A horizontal element was also used to identify whether and to what extent learning and thinking about the issues caused changes in evaluation. Increased consensus was found after a delay between initial exposure to the SoP and subsequent review of SoP elements. While this is a small sample study, it points toward both the need and the value of larger and more comprehensive studies in order to afford a clear consensus around reasonable and prudent practices for ARM IP and the value of additional awareness, training, and education in IP issues within the ARM community.

Key words: archives and records management, consensus, government archives, information, protection, standard of practice

Background and introduction

Information protection (IP) and archival theory are ancient disciplines traceable to the beginning of recorded time and critical to legal and governance in much of the world. 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 (Gnanadesikan, 2009, p. 14). Archival theory concerns preservation of authentic records while IP foci surround limiting harm from symbolic representations. In the digital age, IP was applied to information technology (IT) and archival theory was applied to records management, producing the field of archives and records management (ARM). IP focused largely on confidentiality and integrity via physical and logical access control and encryption-related methods. Military approaches diverged from business approaches and, as the Internet emerged, ease of transmission and global access increased information-related risks. IP progressed at a rapid pace (Canadian System Security Centre, 1993, Commission of the European Communities, 1991, Department of Defense, 1986, Information Systems Security Association, 2005, International Standards Organization, 2005, International Standards Organization, 2009, International Standards Organization, 2010, ISACA, 2007, National Institute of Standards and Technology, 2000, National Institute of Standards and Technology, 2001, National Institute of Standards and Technology, 2006a, National Institute of Standards and Technology, 2006b, National Institute of Standards and Technology, 2013). The ARM literature in the same time frame produced

[1] This research was supported in part by the InterPARES Trust Project of the University of British Columbia, Webster University, and Management Analytics, Inc.

apparently independent approaches. Early attention focused on longevity of physical media as opposed to records (Waters and Garrett, 1996). Early digital ARM content was largely administrative, statistical, or survey data of short-term value (Cook, 1991, p. 203). Files were viewed as data with informational value, and not records with evidential value, and therefore not perceived as ARM responsibility (Cook, 1991, p. 204). Preservation of digital records become an ARM specialty in the 1990s (Cook, 1991, p. 204, Duff, 1996, p. 28-45, Duranti, 2001, Duranti and MacNeil, 1996, p. 46-67, Waters and Garrett, 1996). In the 2000's, the ARM field developed models, standards, guidelines, and tools with respect to long-term digital preservation (Consultative Committee for Space Data Systems, 2004, Consultative Committee for Space Data Systems, 2012, National Library of Australia, 2003, Nestor Working Group on Trusted Repositories Certification, 2006, PREMIS Working Group, 2005).

ARM and IP diverged. IP's focus became limiting information-related harm (Cohen, 1995) while ARM focused on archival creation, management, and preservation of digital records. In ARM, IP is typically considered a necessary component of archival management, not an integral part of preservation. IP and ARM are both concerned with controlling persistence of content with certain qualities. IP qualities typically include confidentiality, integrity, availability, use control, and accountability. ARM's SPOT model lists availability, identity, persistence, renderability, understandability, and authenticity (Vermaaten et al., 2012). The OAIS Reference Model mandates "fixity, reference, provenance, context, understandability and availability of content" over time (International Standards Organization, 2012). The InterPARES Project focuses on authenticity, "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 (InterPARES 2 Project, 2007). The fields also tend to diverge with respect to longevity. Becker et al. describe digital preservation as "information management with a long-term mission" compared to the "medium-term vision" of IP (Becker et al., 2011, p. 1-10). IP frameworks tend to ignore technology change over time and accessibility issues associated with long-term usability, while ARM tends to ignore the costs and complexities of the real-time ongoing struggle between attackers and defenders in modern highly connected information technology systems.

Archives Information Protection Standard of Practice

The InterPARES Trust ARM-SoP effort developed a draft ARM-SoP. An SoP is a decision-making methodology used to help professionals determine "reasonable and prudent" (RaP) courses of action for a given institutional circumstance. The concept of "reasonable and prudent" originates in English tort law with the "reasonable man."(Vaughan vs Menlove, 1837). An action is RaP if it is what a prudent person with reasonable amount of expertise or knowledge might have done given the same circumstances. ARM institutions use the ARM-SoP to identify current and develop RaP future practices. Current and anticipated SoPs do not uniquely identify RaP practices, as there may be RaP practices for situations the SoP fails to identify. Without an ARM-SoP, decisions are likely dependent on the knowledge of individuals directly involved in institutional IP efforts, rather than a broadly studied analysis based on community consensus. The ARM-SoP is "open-source" and available at http://all.net/SoP/Archives/index.html This paper describes the beginning of the work toward consensus. See the Appendix for specifics.

The ARM-SoP studied contains 111 elements (i.e., factual information about the institution or

status of a particular decision nexus), each with has four component parts. The "Title" is phrased as a question (e.g., "How are real-time interdependency risks managed?"). The "Options" contain a non-exhaustive set of alternative answers to the question. The "Decision" contains a decision-making process to determine RaP Option(s) for a given situation. The "Basis" provides the underlying definitions and rationale for the Decision. In application, the current situation is collected and codified, and a RaP future state is developed by applying the Decisions in context. The basis is included so the reasoning behind the decisions is documented. The Decision methodology can be applied by rote, however it is intended for application by an expert analyst understanding the subject's circumstances and in a group process involving parties with relevant knowledge. A depiction of the areas of coverage of the ARM-SoP is provided in Figure 1. Further details are available from the standards itself as referenced above.

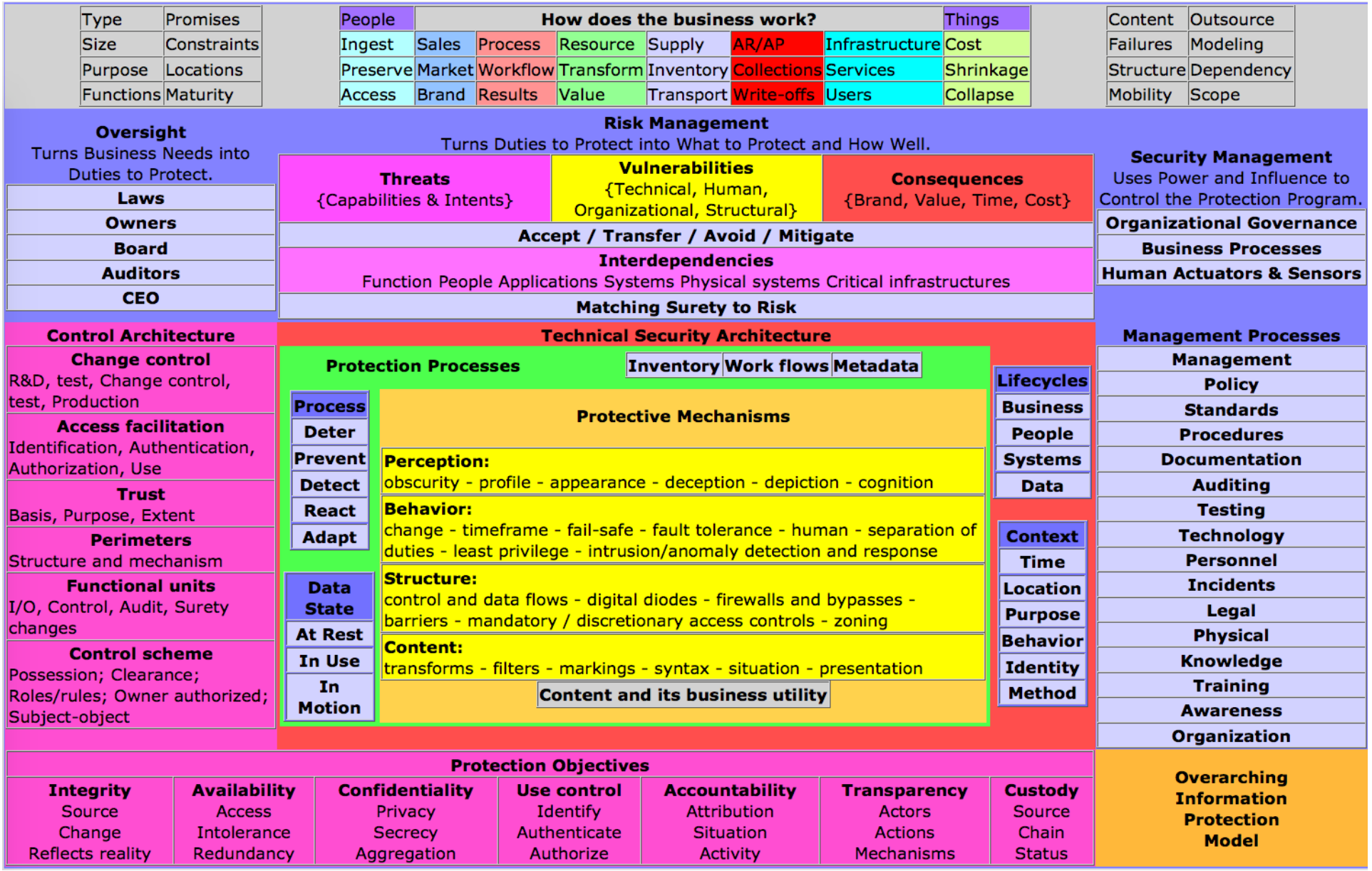

Figure 1: The SoP in the context of an overall protection mode

To develop the ARM-SoP, researchers compared ARM standards and literature to information security recommendations using a pre-existing enterprise SoP, and adapted it producing a draft ARM-SoP. The ARM-SoP was applied to a notional low-risk low-consequence archive to test utility in context and validate it conceptually.

The development process led to notionally understanding many issues relating to divergence of the fields. For example, while transparency is a core principal of archives, it was completely missing in IP. ARM literature places methodological risk management and information protection secondary to archival management and does not take maturity, risk, and differing requirements of institutions into account. ARM literature is prescriptive with respect to professional responsibilities, but permissive regarding implementation. The ARM-SoP makes recommendations about issues that impact long-term preservation planning and content management, but allows the institution to define specific requirements. The ARM-SoP collects information about institutional mandate and responsibilities, but takes purpose from the institution. The SoP is more granular, making practical recommendations about specific operations and processes based on the circumstances and context of the institution.

An initial study of consensus

- Methodology

In 2014-2015, the *draft* ARM-SoP was studied using 5 volunteer government operated archives from Canada. IRB approval (H14-01059) was attained and each subject participated in a 1-day or less online video-session in which an expert presents and asks each question of the draft and answers are codified on-screen as given and corrected to meet subject's specifications. When questions of meaning of words are asked, the "Basis" section is used to provide details, and to the extent that answers are of known sorts, wording is suggested to help clarify presentation (e.g., if the subject indicates that they don't know something, the suggested answer might be "unknown" rather than an extended explanation of the fact they subject does not know). Subjects responded to elements of the draft with current state information to the best of their knowledge. Subjects were chief archivists or equivalent, and some had a co-worker present. Information gathered was anonymized at collection, and at end of day of collection, a copy was provided for review and confirmation of anonymization adequacy. A survey was provided related to the information gathered, and responses collected before the next phase proceeded. Survey 1 questions:

- Was this an element of information protection that you were aware of? (Y/N)
- Did this element identify alternative information protection methods that you were unaware of? (Y/N)
- Are there additional elements of information protection you use that were not provided? (Y/N)

Within 10 days of current state collection, and after collection of survey data, a "future state" report was provided based on rote application of the draft. In rote application, the draft "Decision" sections are applied without added judgment or expertise. Upon providing results, subjects are surveyed asking if each future state element is RaP and taking comments. Survey 2 question:

- Do you think the "future state" recommendations are reasonable and prudent? (Y/N or Other)

At least 60 days later, each subject was asked to review results of two other subjects and indicate whether each future state element was RaP in the context of the other anonymized archive. Survey 3 questions:

- Do you think the "future state" recommendations are: Reasonable? (Y/N or Other) Prudent? (Y/N or Other)

Agreement was measured by yes/no answers and averaged across responses based on the number of "yes" votes. As in Hererra and Herrera-Viedma (1996, p. 73-87), consensus was determined as the "maximum possible consensus" for each given SoP element in contrast to "maximum consensus" (100% for all questions), which would be difficult to achieve and less informative in such a situation. The series of questionnaires created a "dynamic process" where participants were invited to learn from their experiences of the SoP and the experiences of other participants to "update their opinions" and move towards greater consensus. The approach also resembles the Delphi technique [35] in use since the 1960s and developed by the United States military (Dalkey and Helmer, 1963). The key components of the Delphi technique, such as anonymity of participants, structured information flow in the form of questionnaires, ability to give feedback on prior opinions, the role of experts (in this case, ARM professionals), and a mediator were all present in the SoP process. As Dalkey and Halmer (1963, p. 458-467) describe, the technique uses a "series of intensive questionnaires interspersed with controlled opinion feedback" and "the repeated individual questioning of the experts". The result is expressed as a "numerical quantity" that is then compared across surveys to see if there is a tendency for consensus "to converge as the experiment continues".

- Limitations and hypotheses

As a small-sample study, statistical results are essentially meaningless. In addition, the number of elements (110) and the number of alternatives per element (varying between 3 and various combinations of up to 20 sets of 10 selections in sequence) is such that no practical study could reasonably provide meaningful data at a detailed level. Rather, results are intended to indicate areas of likely consensus and divergence for further study.

Hypotheses surrounded three basic areas; (H1) there is consensus and divergence between the IP and ARM communities surrounding specific areas of information protection; (H2) practicing ARM specialists are unfamiliar with many aspects of IP, and (H3) governance problems well know in information protection are also present in ARM. Evidence of consensus and divergence is directly shown by agreement or lack thereof between RaP of SoP elements by ARM participants.

Familiarity with concepts was identified as indicated by changes in RaP results and question comprehension over time. Governance problems are indicated by specific areas such as separation of duties, presence of codified duties to protect, and power and influence of the chief archivist. In more detail, respectively, (a) separation of duties is often inadequate elsewhere with the responsible party working for someone who can violate the requirements without recourse of inspection, (b) duties to protect are often inadequately or not specified, leading to poor decisions about what to protect and how well, and (c) it is common in other areas for those responsible for protection to lack the power and influence to affect the areas of their responsibility.

- Results

o Familiarity of concepts:

Familiarity with concepts was identified as indicated by changes in RaP results and question comprehension over time. The survey indicated levels of awareness with the elements of the SoP overall, with 62.7% of respondents in the 80-

100% range. No elements had zero awareness. The chart below gives percentage levels of awareness indicated by a "Yes" response (x) by the number of elements in the SoP (y).

0%	20%	40%	60%	80%	100%
0	2	8	31	36	31

Awareness of elements of the SoP at the start of the process

The following elements of the SoP had 20% to 40% awareness (first 2 are 20%):

- What model is used to understand information protection issues?
- Is an explicit business model used to support information protection decision-making?
- How duty to protect is analyzed?
- What design basis threat is used?
- How are risk and surety changes of a subsystem handled?
- How does the enterprise model information-related controls?
- How are technical controls structured?
- How is zone separation verified?
- How is intelligence gathering countered?
- What logical perimeters have what protection mechanisms?

IP methods (Options within elements) new to subjects were identified for 105 out of 110 elements (95%). Thus general knowledge was present but specific knowledge of alternatives was lacking.

o Evidence of consensus

Evidence of consensus and divergence is directly shown by agreement or lack thereof between RaP of SoP elements by ARM participants.

Results after the initial assessment in looking at their own institutions were rarely considered RaP. Out of a total of 110 elements considered, only 9 of ARM-SoP elements were considered RaP by all participants across all assessments and there was a significant lack of consensus.

20%	40%	60%	80%	100%
3	19	47	32	9

Post-Results elements with identified percentages of subjects asserting RaP

Full agreement was present on maturity level, use of consultants, outsourcing of things, oversight (form of duties and analysis) management influence and knowledge, version control, and redundant storage location. Nearly full disagreement with RaP practices was found for design-basis threat, vulnerability assessment, and management.

Reasonable and prudent views of other institutions after 2-4 months waiting times produced far higher consensus levels. The results for the post-assessment survey were averaged between reasonable and prudent results. 111 RaP questions answered Yes or No 110 had 80% or higher consensus.

0%	20%	40%	60%	80%	100%
0	0	0	1	83	27

Post-delay elements with identified percentages of subjects asserting others are RaP

Governance problems are indicated by specific areas such as separation of duties, presence of codified duties to protect, and power and influence of the chief archivist. In more detail, respectively, (a) separation of duties is often inadequate elsewhere with the responsible party working for someone who can violate the requirements without recourse of inspection, (b) duties to protect are often inadequately or not specified, leading to poor decisions about what to protect and how well, and (c) it is common in other areas for those responsible for protection to lack the power and influence to affect the areas of their responsibility.

- Regarding the hypotheses of the study

H1: There is apparent consensus and divergence between the IP and ARM communities surrounding specific areas of information protection when first introduced, but exposure leads to very high levels of consensus regarding RaP for other institutions given time to digest the issues. Specific areas of each are identified above.

H2: Practicing ARM specialists are unfamiliar with some aspects of IP, particularly in areas where classical ARM educational lacked in-depth coverage. However, the basic understandings of ARM apply broadly and given time to consider these issues, they come to the view that IP issues are valid and apply to ARM situations.

H3: Governance problems well known in IP are also present in ARM. Most particularly while responsible for information protection, chief archivists were, in some cases, inadequately empowered, resourced, or knowledgeable to meet those responsibilities. However, this varies substantially by organization. This appears to be an organizational issue that is not universal.

WARNING: This is a small sample study and as such, generalizations such as these should be examined with further studies and statistical inferences should not be drawn from these results.

Summary, conclusions, and recommendations

The effort to formulate a standard of practice for archives and records management identified areas in both fields where they were lacking and strengthens them both by integrating their critical concepts and viewpoints. The resulting ARM-SoP is a valuable tool to self-examination.

While this study reports only on a very small sample, it points toward both the need and the value of (1) larger and more comprehensive studies to gain consensus around reasonable and prudent practices for ARM IP and (2) the value of additional awareness, training, and education on IP issues within the ARM community. The change over a very short time frame in views on reasonable and prudent protection implies the potential for substantial improvement in protection for relatively little investment.

Appendix: The elements of the ARM-SoP's

Who are the interviewees?	
Overarching	How does the archive describe itself and why this effort is being undertaken?
	Protection model: What model is used to understand information protection issues?
	Business: What is the purpose of the archive?
	Promises: What promises does the archive make, to whom, and why? How do they relate to information?
	Scope: What is the scope of this security architecture?
	Maturity level: What maturity level does the information protection program have?
	ARMA maturity model: What GARPM maturity levels do different aspects of the archive have?
	Content: What content does the enterprise have and what are the consequences of protection failures?
	Location: Where are content and work located?
	Organization: What is the structure of the organization?
	Security consultants: When are information security consultants used?
	Mobility: What part and portion of the workforce is mobile?
	Outsourcing people: What part and portion of the workforce is outsourced?
	Outsourcing things: When is information technology outsourced?
Business modeling	How does the enterprise model itself and its business?
	Is an explicit business model used to support information protection decision-making?
	What are the business functions and what information do they depend on for what?
	What does enterprise oversight provide to the protection program to define duties to protect?
Oversight:	How are different sorts of duties prioritized in determining what to protect and how well?
	Form of duties: What form are duties defined in?
	Duties analysis: How is duty to protect analyzed?
Risk Management	How does the enterprise do risk management?
	Risk management process: What risk assessment processes are used?
	Risk definition: How are risk levels for the protection program defined?
	Threats: How are information-related threats assessed?
	Threats: What threats have been identified, what are their characteristics and relevant history?

	Threats: What design basis threat is used?
	Threats: What attack mechanisms are considered?
	Vulnerabilities: How and when are information-related vulnerabilities assessed?
	Risks: When does the enterprise avoid, accept, transfer, and mitigate information-related risks?
	Risk aggregation: What process is used to identify and control the aggregation of risks?
	Separation of Duties: How should duties be separated?
	Interdependencies: How are supply chain risks managed?
	Interdependencies: How are real-time interdependency risks managed?
	Costs: How is security budgeted?
	Surety matching: How is surety matched with risk?
	Failsafes: When failsafes are required and how are they determined?
	Changing systemic risks: How is changing systemic risks managed?
	Changing subsystem risk and surety: How are risk and surety changes of a subsystem handled?
Management:	How does the enterprise manage the information protection program?
	CISO: Is there an enterprise information protection (IP) Lead, and where are they placed?
	Duties: What duties does the information protection lead have?
	Influence: What power and influence does the IP Lead have?
	Security Metrics: What security measurements are taken and when?
	Policy: What information security policies are needed and used?
	Standards: Which widely used control standards are best suited to the enterprise?
	Procedures: What procedures are implemented and how?
	Documentation: How are security-related issues documented?
	Auditing: How are audits managed within information protection?
	Testing: What does the testing function do and cover?
	Personnel: How are personnel issues with information protection managed?
	Background checks: When are which background checks done on which workers?
	Incident handling: How are incidents managed?
	Legal issues: How do legal issues interact with protection management?
	Physical security: How is physical security integrated with information protection?

	Knowledge: How is the knowledge program integrated with information protection?
	Security awareness: What sort of enterprise security awareness program does the enterprise have?
Control Architecture:	How does the enterprise model information-related controls?
	Establishment: Is a control architecture formally established?
	Objectives: What are the protection objectives and how are they applied??
	Access Controls: What access control model is used?
	Identification: How are individuals originally identified and their identities verified?
	Identity proofing: How are asserted identities proofed after originally identified?
	Authentication: How are identities authenticated to support authorized access?
	Access facilitation: How is access facilitated once identity is adequately established?
	Trust model: How is trust assessed and managed?
	Change management: How are changes to information technology managed?
	Control Architecture: When is a systematic security architecture created and updated?
Technical Security Architecture:	How are technical controls structured?
TechArch:	Inventory: What information protection-related inventory is kept and in what form(s)?
	Workflows: How are workflows used, controlled, and assured?
	Metadata: What Metadata should be ingested, created, retained, and presented?
	Lifecycles: What aspects of lifecycles are considered in the protection program and its processes?
Zones:	How does the enterprise separate parts (zone) its network(s)?
	Placement: What systems, data, and people go in which zones and subzones?
	Firewalls: What mechanisms are used to separate communicating zones and subzones?
	Zone separation verification: How is zone separation verified?
	Physical separation: How are zones and subzones physically separated and controlled?
	Connection controls: How are connections between devices controlled?
	Microzones: How is virtualization and encryption used to for microzones and when?
	Remote access: How is access to internal zones from distant locations (including wireless) facilitated?
	Endpoint protection: What protective mechanisms are used to harden which endpoints?
	Zone to zone access: How is communication facilitated and controlled to areas outside a zone/subzone?
Incidents:	Detection: Are intrusions detected, and if so, how?

	Malicious Alteration Detection: How is malicious alteration detected?
	Response: Who controls and executes responses to information-related attacks?
	Detection and response: What are the process requirements for detection and response?
	Deception: When are deceptions used to defend networks and systems?
Content control:	How is harmful and useless content controlled in my computing environments?
	What mechanisms keep control over content with business utility?
	Data in use: How is data in use protected?
	Data in motion: When is content in transit encrypted?
	Data at rest: What is stored encrypted?
	Version control: How are versions of data over time protected?
	How is intelligence gathering countered?
	How is intellectual property protected?
Human factors:	How are human factors considered in the protection program?
	Protection load: How is security load managed?
	User decision-making: What decisions do users make and how do they make them?
	Disruption: How is disruption of work controlled?
Redundancy:	Fault model: What fault model is assumed for analysis of redundancy?
	Backups: What is backed up and how often?
	Backup retention: How long are backups retained and how are they disposed of?
	Storage location: Where and in what sort of containers are backups stored?
	Data center redundancy: How many data centers are required?
	Redundant facility distance: How far apart are redundant data centers and people to assure continuity?
	Business continuity and disaster recovery: What information resources are where?
	Interdependencies: How is redundancy applied to interdependent mechanisms?
Technology:	Logical Perimeters: What logical perimeters have what protection mechanisms?
	Physical Perimeters: What physical perimeters have what protection mechanisms?
	Physical/Logical Nexus: How do physical and logical controls interact and integrate?

References

Becker, C., Antunes, G., Barateiro, J., Vieira, R. and Borbinha, J. (2011), "Control objectives for dp: Digital preservation as an integrated part of it governance", *Proceedings of the American Society for Information Science and Technology,* Vol. 48 No. 1, pp. 1-10.

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

Cohen, F. (1995), "Introductory Information Protection": ASP Press, available at: http://all.net/edu/curr/ip/index.html (accessed 29th December 2015).

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

Consultative Committee for Space Data Systems (2004), "Producer-Archive Interface Methodology Abstract Standard", Washington DC, Consultative Committee for Space Data Systems

Consultative Committee for Space Data Systems (2012), "Reference Model for an Open Archival Information System", Washington DC, Consultative Committee for Space Data Systems

Cook, T. (1991), "Easy to byte, harder to chew: the second generation of electronic records archives", *Archivaria,* Vol. 33 No. Winter, pp. 202-216.

Dalkey, N. and Helmer, O. (1963), "An experimental application of the Delphi method to the use of experts", *Management Science,* Vol. 9 No. 3, pp. 458-467.

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

Duff, W. M. (1996), "Ensuring the preservation of reliable evidence: a research project funded by the NHPRC", *Archivaria,* Vol. 41 No. 1, pp. 28-45.

Duranti, L. (2001), "The long-term preservation of authentic electronic records", in Apers, P. M. G., Atzeni, P., Ceri, S., Stefano Paraboschi, Ramamohanarao, K. and Snodgrass, R. T. (eds), *Proceedings of 27th International Conference on Very Large Data Bases*, Roma, Italy, Morgan Kaufmann pp. 625-628.

Duranti, L. and MacNeil, H. (1996), "The Protection of the Integrity of Electronic Records: An Overview of the UBC-MAS Research Project", *Archivaria,* Vol. 42, pp. 46-67.

Gnanadesikan, A. E. (2009), *The writing revolution: Cuneiform to the internet,* Wiley-Blackwell, Malden, MA.

Herrera, F. and Herrera-Viedma, E. (1996), "A model of consensus in group decision making under linguistic assessments", *Fuzzy sets and Systems,* Vol. 78 No. 1, pp. 73-87.

Information Systems Security Association (2005), "Generally Accepted Information Security Principles v3. 0", Information Systems Security Association.

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

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

International Standards Organization (2010), "ISO 9798-1:2010 Information

Technology—Security Techniques—Entity Authentication", Geneva, International Standards Organization.

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

InterPARES 2 Project. (2007), "Terminology Dictionary: Authenticity", available at: http://www.interpares.org/ip2/ip2_term_fdisplay.cfm?tid=189&pageID=2 (accessed 12th July 2014).

ISACA. (2007), "COBIT 4.1: Framework for IT Governance and Control", available at: http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx (accessed 26th December 2015).

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

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

National Institute of Standards and Technology (2006a), *Minimum Security Requirements for Federal Information and Information Systems 200,* Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD

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

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

National Library of Australia. (2003), "Guidelines for the preservation of digital heritage", available at: http://unesdoc.unesco.org/images/0013/001300/130071e.pdf (accessed July 12 2014).

Nestor Working Group on Trusted Repositories Certification. (2006), "Catalogue of Criteria for Trusted Digital Repositories", available at: http://edoc.hu-berlin.de/series/nestor-materialien/8en/PDF/8en.pdf. (accessed July 12th 2014).

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

Vaughan vs Menlove (1837), "3 Bing N.C. 467, 132 E. R. 490", Court of Common Pleas.

Vermaaten, S., Lavoie, B. and Caplan, P. (2012), "Identifying threats to successful digital preservation: The SPOT model for risk assessment", *D-Lib Magazine,* Vol. 18 No. 9.

Waters, D. and Garrett, J. (1996), *Preserving Digital Information. Report of the Task Force on Archiving of Digital Information,* The Commission on Preservation and Access, Research Libraries Group, Washington DC.

Biography

Dr Fred Cohen is best known as the person who defined the term "computer virus" and the inventor of most of the widely used computer virus defense techniques, the principal investigator whose team defined the information assurance problem as it relates to critical infrastructure protection, as a seminal researcher in the use of deception for information protection, as a leader in advancing the science of digital forensic evidence examination, and as a top flight information protection consultant and industry analyst. He is CEO of Fred Cohen & Associates, a firm that does research and advisory services exclusively for the US government, CEO of Management Analytics, a firm specializing in research and advisory services and litigation support for non-US Federal government customers, and a Senior Partner at Fearless Security, LLC, a firm specializing in examination and specification of information protection. He is also acting director of the Webster University CyberLab.