

# Project NA03: Standard of Practice

## **A Comparison of ARM Literature and Information Protection Standards of Practice**

Grant Hurley, University of British Columbia

on behalf of Dr. Fred Cohen, Webster University

# Outline

---

1. Background & Introduction
2. Introduction to the Standard of Practice (SoP)
3. Development of the Draft ARM SoP
4. Standards & Literature Compared
5. Conclusions
6. Current Steps & Outcomes

# 1. Background & Introduction

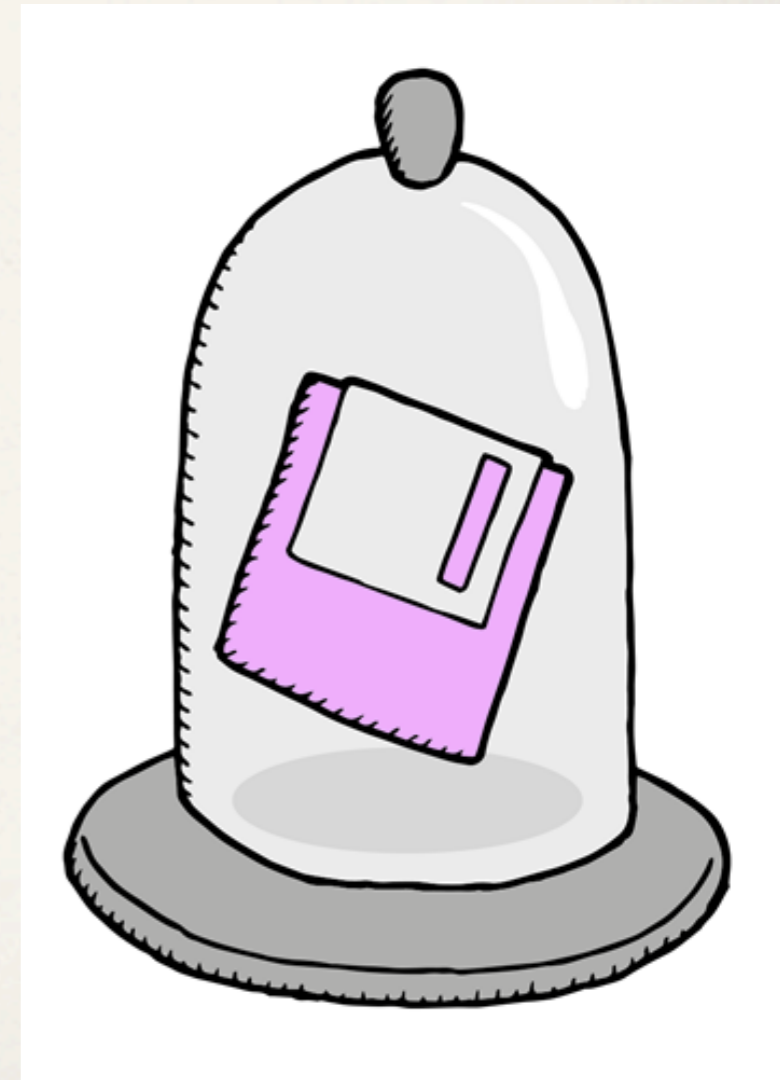
---

## Information Protection (IP)

- ❖ Historical concern with protecting information from unauthorized access, manipulation, use, and denial of use; ensuring transmission integrity and secrecy, and authentication (Salzer & Schroeder, 1975; van Biene-Hershey, 2007)

## Archives and Records Management (ARM)

- ❖ Historical focus on trusted preservation of authentic records for the purposes of evidence and memory (Duranti, 2013; InterPARES2, 2014)



# 1. Background. Becker et al.

---

“Digital Preservation is an operational activity with a **long-term vision**, which can lead to difficulties in structuring effective and efficient processes.”

“The discipline of IT Governance has a **medium-term vision**: it strives to ensure business continuity by detecting changes early, assessing their impact proactively, and ensuring strategic alignment of technology with business goals.”

"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.

## 2. Intro. to Standards of Practice

---

- ❖ Neither a standard nor a practice,  
but a decision-making methodology used to help professionals determine reasonable and prudent courses of action
- ❖ Identifies whether someone acted with diligence or negligence
- ❖ Allows professionals to ask reasonably comprehensive questions

# 3. Development. Draft ARM SoP

Type	Promises	People	How does the business work?						Things	Content	Outsource				
Size	Constraints	Ingest	Sales	Process	Resource	Supply	AR/AP	Infrastructure	Cost	Failures	Modeling				
Purpose	Locations	Preserve	Market	Workflow	Transform	Inventory	Collections	Services	Shrinkage	Structure	Dependency				
Functions	Maturity	Access	Brand	Results	Value	Transport	Write-offs	Users	Collapse	Mobility	Scope				
<b>Oversight</b> Turns Business Needs into Duties to Protect.		<b>Risk Management</b> Turns Duties to Protect into What to Protect and How Well.									<b>Security Management</b> Uses Power and Influence to Control the Protection Program.				
<b>Laws</b>		<b>Threats</b> {Capabilities & Intents}			<b>Vulnerabilities</b> {Technical, Human, Organizational, Structural}			<b>Consequences</b> {Brand, Value, Time, Cost}			<b>Organizational Governance</b>				
<b>Owners</b>		<b>Accept / Transfer / Avoid / Mitigate</b>									<b>Business Processes</b>				
<b>Board</b>		<b>Interdependencies</b> Function People Applications Systems Physical systems Critical infrastructures									<b>Human Actuators &amp; Sensors</b>				
<b>Auditors</b>		<b>Matching Surety to Risk</b>									<b>Management Processes</b>				
<b>CEO</b>		<b>Technical Security Architecture</b>									<b>Management</b>				
<b>Control Architecture</b>		<b>Protection Processes</b>						<b>Inventory</b>			<b>Policy</b>				
<b>Change control</b> R&D, test, Change control, test, Production		<b>Protective Mechanisms</b>			<b>Work flows</b>			<b>Metadata</b>			<b>Standards</b>				
<b>Access facilitation</b> Identification, Authentication, Authorization, Use		<b>Process</b>	<b>Perception:</b> obscurity - profile - appearance - deception - depiction - cognition									<b>Lifecycles</b>	<b>Procedures</b>		
<b>Trust</b> Basis, Purpose, Extent		<b>Deter</b>	<b>Behavior:</b> change - timeframe - fail-safe - fault tolerance - human - separation of duties - least privilege - intrusion/anomaly detection and response									<b>Business</b>	<b>Documentation</b>		
<b>Perimeters</b> Structure and mechanism		<b>Prevent</b>	<b>Structure:</b> control and data flows - digital diodes - firewalls and bypasses - barriers - mandatory / discretionary access controls - zoning									<b>People</b>	<b>Auditing</b>		
<b>Functional units</b> I/O, Control, Audit, Surety changes		<b>Detect</b>	<b>Content:</b> transforms - filters - markings - syntax - situation - presentation									<b>Systems</b>	<b>Testing</b>		
<b>Control scheme</b> Possession; Clearance; Roles/rules; Owner authorized; Subject-object		<b>React</b>	<b>Content and its business utility</b>									<b>Data</b>	<b>Technology</b>		
		<b>Adapt</b>										<b>Context</b>	<b>Personnel</b>		
		<b>Data State</b>										<b>Time</b>	<b>Incidents</b>		
		<b>At Rest</b>										<b>Location</b>	<b>Legal</b>		
		<b>In Use</b>										<b>Purpose</b>	<b>Physical</b>		
		<b>In Motion</b>										<b>Behavior</b>	<b>Knowledge</b>		
												<b>Identity</b>	<b>Training</b>		
												<b>Method</b>	<b>Awareness</b>		
												<b>Organization</b>		<b>Overarching Information Protection Model</b>	
<b>Protection Objectives</b>															
<b>Integrity</b> Source Change Reflects reality		<b>Availability</b> Access Intolerance Redundancy		<b>Confidentiality</b> Privacy Secrecy Aggregation		<b>Use control</b> Identify Authenticate Authorize		<b>Accountability</b> Attribution Situation Activity		<b>Transparency</b> Actors Actions Mechanisms		<b>Custody</b> Source Chain Status			

The Archival Information Protection Model

# 3. Example. Management: Policy

---

What information security policies are needed and used?

Question

Decision appropriate for given circumstance

Decision

- Option 1: No security policies at all.
- Option 2: Acceptable use policies.
- Option 3: Legal and regulatory related policies.
- Option 4: A wide array of standards-based and other policies.
- Option 5: A policy based on a single well-recognized standard.

Options

Basis:

Definitions of options and other pertinent information

Basis

# 4. Standards & Literature Compared

---

- ❖ *Aboriginal and Torres Strait Islander Library, Information, and Resource Network Protocols (ATSILIRN)*
- ❖ *Audit and Certification of Trustworthy Digital Repositories (ISO 16363)*
- ❖ *Data Seal of Approval Guidelines (DSA)*
- ❖ *DRAMBORA: Digital Repository Audit Method Based on Risk Assessment toolkit*
- ❖ *ICA Principles of Access to Archives: Technical Guidance on Managing Archives with Restrictions*
- ❖ *InterPARES 2: Benchmark Requirements Supporting the Presumption of Authenticity and Baseline Requirements Supporting the Production of Authentic Copies of Electronic Records*



# 4. Standards & Literature con't

---

- ❖ *ISO/IEC 14721:2012 Space data and information transfer systems -- Open archival information system (OAIS) – Reference model.*
- ❖ *ISO 15489:2001 Information and documentation -- Records management*
- ❖ *Nestor Seal for Trustworthy Digital Archives*
- ❖ *PREMIS Data Dictionary for Preservation Metadata*
- ❖ *SPOT (Simple Property-Oriented Threat) Model for repository risk assessment*

# 5. Conclusions

---

- ❖ Methodological risk management and computer security are generally secondary to archival management in the ARM literature
- ❖ Maturity (how processes are defined, documented and maintained) and risk levels are not currently taken into full account
- ❖ The SoP takes more granular approach than most of the ARM literature reviewed:
  - ❖ Practical recommendations about specific operations and processes in IP systems
  - ❖ Based on the circumstances and context of the institution

# 6. Current Steps & Outcomes

---

## Done:

- ❖ Literature review, SoP open source initial draft, report on which this presentation is based

## Ongoing:

- ❖ Application of the ARM SoP to organizations via interviews for identifying consensus (or lack thereof)

## Next:

- ❖ Use the study to adapt the SoP and build consensus around standards of practice

# Questions?

---

Please contact me at [gehurley@mta.ca](mailto:gehurley@mta.ca) if you'd like to participate!

Visit <http://all.net/SoP/Archives/> for the draft Archives SoP

# References

---

- ❖ Duranti, Luciana. "Historical Documentary Memory in the Cloud: An Oxymoron or the Inescapable Future?" *Revista D'arxius* (2013), p. 19-60.
- ❖ InterPARES. "Archives." *The InterPARES 2 Project Dictionary*. Oct. 16, 2014. [http://www.interpares.org/ip2/display\\_file.cfm?doc=ip2\\_glossary.pdf&CFID=5647158&CFTOKEN=31199803](http://www.interpares.org/ip2/display_file.cfm?doc=ip2_glossary.pdf&CFID=5647158&CFTOKEN=31199803)
- ❖ Saltzer, Jerome H., and Michael D. Schroeder. "The protection of information in computer systems." *Proceedings of the IEEE* 63, no. 9 (1975): 1278-1308.
- ❖ 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.