

Guidelines for Managing Records Created in the Investigative and Litigation Process:
A White Paper

Donald C. Force
University of British Columbia
May 2011

Table of Contents

Acknowledgements.....	3
About the Author.....	3
Executive Summary.....	4
Introduction.....	5
Definitions of Key Terms.....	6
Legal Context.....	8
Guidelines and Best Practices.....	9
Research Questions.....	10
Methodology.....	11
Literature Review.....	12
Statutes & Regulations.....	13
Case Law.....	13
Benchmarking Practices.....	13
Investigative Record.....	14
Recordkeeping Systems.....	14
Tracking Evidence.....	14
Physical Evidence.....	15
Electronically Stored Information.....	15
Retention & Disposition.....	15
Preservation of Evidence.....	16
Findings.....	16
Question 1.....	16
Question 2.....	18
Question 3.....	20
Question 4.....	21
Question 5.....	22
Question 6.....	22
Recommendations.....	23
Summary.....	26
Bibliography.....	28
Appendix 1 – Questions for External Organizations.....	32
Appendix 2 – Standards, Guidelines, and Best Practices (Annotated).....	33
Appendix 3 – System Map Example.....	35

Acknowledgements

This project was made possible by funding from Mathematics of Information Technology and Complex Systems (MITACS) and its Accelerate program. MITACS is a Canadian federally and provincially funded research network with offices located throughout Canada, which brings together academia, industry and the public sector through research and training initiatives to develop cutting-edge tools vital to the knowledge-based economy. This project was funded as part of the MITACS-Accelerate program, “a national internship program which connects companies and other organizations with the vast research expertise in Canada’s universities from applied sciences, engineering, social sciences and business to arts, life sciences” and other domains.¹

This project could not have been completed without the assistance from a number of individuals. Foremost, I would like to thank the project’s academic advisor Dr. Victoria Lemieux, Assistant Professor at the School of Library, Archival and Information Studies at the University of British Columbia, without her guidance, support, and expertise, this project would not have succeeded. A special thank you must also be given to all the anonymous contributors who took the time to complete the questionnaire and discuss this research project with the author. I would also like to thank Dr. Luciana Duranti, Professor at the School of Library, Archival and Information Studies at the University of British Columbia for providing access to bibliographic information from the Digital Records Forensics and International Research on Permanent Authentic Records in Electronic Systems (InterPARES) projects.

About the Author

Donald C. Force is a Ph.D. candidate in the Library, Archival and Information Studies program at the University of British Columbia (UBC). His current research interests focus on the relationship between archival science and law, specifically, the relationship between recordkeeping standards, e-discovery, and the admissibility of records as evidence. In addition to this project, he has been involved in several international research initiatives at UBC, including the InterPARES (International Research on Permanent Authentic Records in Electronic Systems), Digital Records Forensics, and Digital Economy projects. He has given numerous presentations on the topic of e-discovery and its relationship to records professionals and in 2010 his article “From Peruvian Guano to Electronic Records: Canadian E-Discovery and Records Professionals” appeared in *Archivaria* #69. Prior to studying at UBC, he received his Master of Library Science and Master of Information Science degrees from Indiana University (Bloomington, IN), holds an MA in history from Southern Illinois University Carbondale, and a BA in English from Millserville University (Millserville, PA).

¹ “About MITACS-Accelerate,” MITACS (2011). Available online at http://www.mitacs.ca/index.php?option=com_content&view=article&id=243&Itemid=6&lang=en.

Executive Summary

Financial and securities regulators must properly manage and maintain investigative records to meet their legal requirements. Increasing amounts of evidence in physical and digital formats place growing strains on these organizations to satisfy their legal obligations. Lack of sufficient controls over the management of investigative records may ultimately result in unfavorable legal actions and/or negative publicity for the organization.

Based on a research project that aimed to develop guidelines for financial and securities regulators with regards to how they manage their investigative records, this white paper:

- Articulates the importance of the proper management of investigative records;
- Discusses the management practices of different financial and securities regulators; and
- Establishes a baseline of recommendations for how financial and securities regulators may improve their case management practices.

This paper discusses the key findings of the research project which include the following observations:

- There are no established best practices for the proper management of investigative records for securities regulators;
- The management of investigative records depends largely on the context of the organization and its specific legal requirements;
- Regulatory and securities organizations must be consistent when documenting acquired evidence to ensure its chain of custody and legal admissibility; and
- Regulatory and securities organizations rely on a combination of recordkeeping systems to manage the variety of evidence they acquire.

Based on the findings, this paper recommends that financial and securities regulator should:

- Create a case management unit that documents acquired evidence and tracks the use of evidence throughout the organization;
- Defines the purposes and authorities of its records and evidence management systems;
- Establish concise documentation for logging, tracking, and using evidence in litigation;
- Educate staff, investigators and litigators, in identifying evidential materials that are high at risk for degradation;
- Train staff, investigators and litigators, in the processes they should take when they identify materials high-at-risk for degradation;
- Create a preservation policy/plan to ensure the long-term access of electronically stored information (ESI) at high-risk of degradation; and
- Review their positions toward outsourcing the scanning of evidentiary documents within a risk management framework on a routine basis.

By adopting these recommendations, financial and security regulators will strengthen the management of their investigative records. These practices will enable such organizations to more effectively and efficiently respond to legal challenges.

Introduction

According to the International Organization of Securities Commissions (IOSCO), the “securities and derivatives markets are vital to the growth, development and strength of market economies. They support corporate initiatives, finance the exploitation of new ideas and facilitate the management of financial risk.”² Financial and securities regulators are responsible for safeguarding the fair and efficient operation of financial services, capital markets, exchanges, and firms. Financial and securities regulators ensure that investors have timely, accurate information on which to base investment decisions while promoting confident and informed participation by investors and consumers in the financial system and protecting them against fraud. To maintain confidence in these markets, financial and securities regulators have the legal authority to propose new statutes, laws, and regulations, issue new policy initiatives and projects, and pursue administrative or criminal prosecutions.

Financial and securities regulators must properly manage and maintain the paper, digital, and other records created and received in the fulfillment of the investigative and litigation process. Enforcement staff within these organizations need to be able to access all of the records related to a particular case in order to perform their work functions effectively. Consequently, there are concerns that these organizations may be limited in their abilities to conduct their work effectively and efficiently evaluate and process cases due to the growing amount of evidence required that must be properly managed to ensure its chain of custody and authenticity.

The issue of balancing legitimate business needs, records management requirements, and evidentiary requirements of the legal system is a common problem experienced by financial and securities regulators. These organizations face the challenge of managing and preserving records that they create or receive in non-traditional software formats, some of which are not compatible with any document management systems currently in place.

This paper proposes a new set of benchmark practices that financial and securities organizations may use to gauge their current case record management processes. These recommendations are based on a research project, conducted by the author, which investigated how several financial and securities organizations manage their investigative records. The author also reviewed international and national standards on records management. Combined, this collective body of knowledge led to the practices outlined in this white paper, which are designed to meet current business needs and satisfy regulatory and statutory requirements, while ensuring the proper protection of evidentiary and organizational records so as to maintain their authenticity and reliability over time.

² International Organization of Securities Commissions (IOSCO). “Objectives and Principles of Securities Regulations.” (May, 2003), p. iv. Available online at: <http://www.iosco.org/library/pubdocs/pdf/IOSCOPD154.pdf>.

Definitions of Key Terms

Admissibility: The quality or state of being allowed to be entered into evidence in a hearing, trial, or other official proceeding.

Admissible: Capable of being legally admitted in a hearing, trial, or other official proceeding.

Admissible Evidence: Evidence that is relevant and is of such a character (e.g., not unfairly prejudicial, based on hearsay, or privileged) that the court should receive it.

Authenticity: The trustworthiness of an entity as the entity; i.e., the quality of an entity that is what it purports to be and that is free from tampering or corruption. The quality of being authentic or entitled to acceptance.

Discovery: The process of identifying, locating, securing, and producing information and materials for the purpose of obtaining evidence for utilization in the legal process.

Documentary Standard: A document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities as their results, aimed at the achievement of the optimum degree of order in a given context.

Electronically Stored Information (ESI): Information that is stored electronically, regardless of the media or whether it is in the original format in which it was created, as opposed to kept in hard copy (i.e., on paper).

Evidence: All records, documents, or materials (regardless of form or format) collected or created during the investigation and litigation processes.

Evidence Document Log (EDL): A document or database used to account for and track evidence in an organization.

Financial and Securities Regulator: An organization responsible for safeguarding the fair and efficient operation of financial services, capital markets, exchanges, and firms.

Investigation Process: The process by which a person of legal authority (e.g., police or securities officer) identifies a possible financial or securities violation, obtains and creates information about the violation, and acquires evidence from the alleged violator. If an investigator determines there is evidence of wrongdoing then the case will be submitted to litigation for evaluation and, possibly, prosecution.

Investigative Record: The collective whole of evidence obtained and created during the investigative and litigation processes and which may be used in a legal investigation.

Litigation Process: The process by which an authorized legal professional (e.g., lawyer) evaluates the evidence collected by the investigators and conducts legal proceedings based on his/her findings. Actions may result in the non-prosecution of a case, a settlement before the case reaches court, or a trial.

Recordkeeping Standard: A type of documentary standard that provides rules, guidelines, or characteristics for records professionals to assist in the management of organizational records throughout their lifecycles.

Records Management: The systematic and administrative control of records throughout their life cycle to ensure efficiency and economy in their creation, use, handling, control, maintenance, and disposition.

Records Management Program: The activities, policies, and procedures within an organization to implement records management.

Records Professional: Any individual who is qualified, as opposed to simply responsible, for managing records at any stage of their life-cycle and in any environment, regardless of the actual title of the position held.

Reliability: The quality of being dependable and worthy of trust.

Sedona Conference: A group of judges, lawyers, and scholars (primarily from the United States) dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, and intellectual property rights.

Weight of Evidence: The persuasiveness of some evidence in comparison with other evidence.

Legal Context

According to the IOSCO's "Objectives and Principles of Securities Regulations" report, financial and securities regulators should have the "power to impose administrative sanctions and / or to seek orders from courts or tribunals."³ In a later report, the IOSCO states that the "scope of the investigative and enforcement powers conferred on the regulator and/or on other authorities, including public prosecuting authorities, depends on the conduct under investigation and the legal system applicable in the jurisdiction."⁴ The legal bodies that provide financial and securities regulators their power and ensure that these organizations do not abuse their power vary from country to country and jurisdiction to jurisdiction. For example, there are substantial differences between those organizations operating in common law jurisdictions versus those in civil law jurisdictions;⁵ and research has indicated that "civil law jurisdictions seem to adopt a more intrusive and regulatory stance toward securities regulation, but place less emphasis on enforcement."⁶

The project on which this paper is based focused solely on organizations in common law countries. In these instances, financial and securities regulators process legal cases through administrative or criminal tribunals or criminal trials.

The following section discusses the role of administrative law as it exists within the Canadian context. While the section makes some distinctions between administrative law and criminal law, the paper discusses the nuances of the latter in the Findings section.

In common law countries, financial and securities regulators, such as the Australian Securities and Investments Commission (ASIC), the British Columbia Securities Commission (BCSC), or the Financial Securities Authority (FSA) of the United Kingdom, operate within the legal framework of administrative law, a component of public law which involves public interests. Administrative law has been defined as:

the law that governs public officials and tribunals who make decisions that affect the interests of individual persons and whose authority to make those decisions is derived from statute. Administrative law prescribes the rules by which these authorities are expected to operate and, when these rules are not complied with, provides the complaint procedures and the remedies.⁷

Administrative law consists of three components: 1) actual by-law, rules and regulations and other forms of subordinate legislation made by administrative tribunals; 2) principles of law governing the actions of administrative tribunals and their decisions; and 3) legal remedies available to those affected by unlawful administrative action or improper decisions of administrative tribunals.⁸ These tribunals function as a part of government, not independent of it like civil and criminal courts, and their primary

³ *Ibid.*, p. 15.

⁴ International Organization of Securities Commissions (IOSCO). "Methodology for Assessing Implementation of the Iosco: Objectives and Principles of Securities Regulation," (February, 2008), p. 44. Available online at: <http://www.iosco.org/library/pubdocs/pdf/IOSCOPD266.pdf>.

⁵ John C. Coffee, Jr., "Law and the Market: The Impact of Enforcement," *University of Pennsylvania Law Review* 156, no. 2 (December, 2007), p. 294.

⁶ *Ibid.*

⁷ Sara Blake, *Administrative Law in Canada*, 4th ed. (Markham, Ontario: LexisNexis, Butterworths, 2006), p. 4

⁸ Lisa Braverman, *Administrative Tribunals: A Legal Handbook* (Ontario: Canada Law Books, 2001), p. 19.

objective is not to punish wrongdoers; rather they aim to protect the public.⁹ In 1992, the Supreme Court of Canada defined the role of administrative tribunals in *Newfoundland Telephone Co. v. Newfoundland (Board of Commissioners of Public Utilities)*:

Administrative boards play an increasingly important role in our society. They regulate many aspects of our life, from beginning to end. Hospital and medical boards regulate the methods and practice of the doctors that bring us into this world. Boards regulate the licensing and the operation of morticians who are concerned with our mortal remains. Marketing boards regulate the farm products we eat; transport boards regulate the means and flow of our travel; energy boards control the price and distribution of the forms of energy we use; planning boards and city councils regulate the location and types of buildings in which we live and work. In Canada, boards are a way of life. Boards and the functions they fulfill are legion.¹⁰

Administrative law rests on two primary legal principles: the principle of natural justice and the principle of fairness. As Gall explains, there are two rules of natural justice: *audi alteram partem* (hear the other side) and *nemo iudex in causa sua debet esse* (no one ought to be a judge in his own cause). The former requires that there must be a fair hearing, the parties must receive proper notice of the hearing, and each party must be allowed to challenge the evidence presented. The latter rule requires the removal of bias from tribunal proceedings.¹¹ The principle of fairness, one of the central rules of natural justice,¹² requires that the administrative tribunal process be fair to “ensure that individuals are given an opportunity to participate in the decision-making process.”¹³ This allows for a flexible judicial process and a tribunal which exercises discretion to make its rulings. Unlike civil or criminal courts, these tribunals are not bound by legal precedent, though they have “an interest in maintaining a pattern of consistent and perhaps predictable rulings.”¹⁴ Overall, though the boundaries between tribunals and other courts may not always be clear, the tribunal system has been established “to prevent the ordinary courts of law from being overburdened by cases, but a tribunal is still subject to judicial review on the basis of breach of natural justice, or where it acts in an ultra vires manner, or indeed where it goes wrong in relation to the application of the law when deciding cases.”¹⁵

Despite their differences from civil or criminal proceedings, organizations responsible for prosecuting individuals in violation of securities-related laws still require proper records management to ensure they fulfill the principle of fairness. Proper records management enhances any organization’s ability to meet disclosure standards while ensuring the chain of custody of its records.

Guidelines and Best Practices

According to the Sedona Conference, a nonprofit legal think tank dedicated to the advanced study of law and policy, “[a]ppropriate management of information and records is driven by two primary

⁹ Blake, p. 42.

¹⁰ *Newfoundland Telephone Co. v. Newfoundland (Board of Commissioners of Public Utilities)*, [1992] SCR 623, CanLII 84 (SCC).

¹¹ Gerald L. Gall, *The Canadian Legal System*. 3rd ed. (Toronto: Carswell, 1990), pp. 360-361.

¹² *Ibid.*, p. 362.

¹³ Braverman, p. 33.

¹⁴ *Ibid.*, p. 25 (citing R.W. Macaulay and J.L.H. Sprague, *Practice and Procedure Before Administrative Tribunals* (Scarborough: Carswell Thomson Professional Publishing, 1997), pp. 1-2 to 1-2.1).

¹⁵ Slapper and Kelly, p. 399.

sources: (a) statutory, regulatory and other legal principles (“law”), and (b) professional standards.”¹⁶ In records management, the “field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records,”¹⁷ recordkeeping standards function as tools records managers may use to enhance the efficiency and effectiveness of organizations by improving the procedures by which organizations create, access, preserve, and dispose of their records.

Guidelines and best practices help ensure records maintain their authenticity, thereby increasing the likelihood that they will be admitted as evidence. For example, section 31.5 of the *Canada Evidence Act*, R.S.B.C. 1996, c. 124 states:

For the purpose of determining under any rule of law whether an electronic document is admissible, evidence may be presented *in* respect of any standard, procedure, usage or practice concerning the manner in which electronic documents are to be recorded or stored, having regard to the type of business, enterprise or endeavour that used, recorded or stored the electronic document and the nature and purpose of the electronic document.

While this provision may be unique to the Canadian context, the Sedona Conference, a nonprofit legal think tank that has gained resounding support and recognition from the courts, stipulates that best information management practices result from two sources: the law (i.e., judicial decisions and statutes) and professional standards. According to the Sedona’s “Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age” (2007) there “is no single standard or universal policy that can be applied as a talisman to guide future conduct or judge the wisdom of prior practices for any given organization” (p. 5). While any organization should use multiple standards to address specific issues, any organization should be able to turn to at least one standard that addresses the most relevant issues of that industry or area of expertise and facilitates the organization’s ability to manage those issues. Currently, there are no standards or best practices designed or intended for securities regulators.

While issues of admissibility and ensuring authenticity may not be paramount for financial and securities regulators, these matters coincide with proper records management and the ability of the organization to ensure that case file information and evidence may be produced for disclosure and hearings. As will be explained in the Methodology section of this report, this research project turned to recordkeeping standards and legal best practices to fill this gap; but even in this case, the standards do not cover all evidentiary issues and there remains a growing need for a comprehensive standard for handling evidence in these types of organizations.

Research Questions

At the outset of the research project on which this paper is based, several research questions were proposed to guide the work to be undertaken for this project. The answers to these questions are addressed in the Findings section of this report.

¹⁶ Sedona Conference Working Group on Electronic Document Retention & Production (WG 1), “The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age,” (November 2007).

¹⁷ International Organization for Standardization (ISO), “ISO/TR 15489-1: Information and Documentation – Records Management – Part 1: General” (2001), p. 3.

- What are the expectations and requirements for maintaining records within a legal context, including civil procedure, criminal, and administrative law?
- Within the specific context of administrative law, for tribunals...
 - should the same disclosure standards as civil or criminal law cases be met?
 - should the same admissibility standards as civil or criminal law cases be met?
- How to best support staff and investigators for e-evidence requirements, in terms of management and preservation?
- What are the issues of chain of custody, authenticity, and the admissibility of e-evidence?
 - What are the best practices for managing all types of documentation for an investigation (i.e., the ERMS stores some, but not all, evidentiary records and administrative records)?
 - What are the best practices for keeping all the documentation and evidence of a case connected?
- What are the best practices for the retention, disposition and preservation requirements for evidence (traditional and electronic)?
- What are the issues (i.e., processes and quality) involved in meeting required expectations for scanned documentation?

Methodology

To answer the research questions, the research project initially set out to determine the methods investigators and litigators of financial and securities regulators use to manage evidence. The project sought to map these processes and identify ways in which they may be enhanced or used to establish a set of best practices. Upon further discussion with the project team, the project took a slightly different approach to data collection and analysis. The researcher contacted staff from several regulatory bodies and had willing participants complete a short questionnaire (Appendix 1). After returning the questionnaire, the researcher conducted follow-up interviews with the participants.

The project also evaluated major recordkeeping standards, guidelines, and best practices. It synthesized this set of documentation in order to develop a new set of best practices that may be used for securities organizations. The researcher reviewed a variety of documents such as international recordkeeping standards, legal guidelines and best practices, and enforcement manuals publicly accessible. This analysis aimed to identify common themes among the documentation and deduce a set of best practices for managing investigative records.

Currently, there are several sets of best practices available for investigators who are required to collect and examine evidence, especially ESI. There include the:

- Association of Chief Police Officers' (ACPO), "Good Practice Guide for Computer-Based Electronic Evidence";
- International Association of Chiefs of Police's, "Best Practices for Seizing Electronic Evidence";
- International Organization on Computer Evidence's, "Guidelines for Best Practice in the Forensic Examination of Digital Technology"; and

- U.S. Securities and Exchange Commission’s, “Enforcement Manual.”

Yet, these documents do not address the management or preservation of evidence once it has arrived at the investigative agency.

This paper attempts to fill this gap by turning to recordkeeping standards and legal practices (see Appendix 2 for an annotated list of the documentation reviewed for this project), such as the:

- International Standards Organization’s (ISO) 15489: “Information and Documentation for Records Management”;
- Canadian General Standards Board’s, “Electronic Records as Documentary Evidence”;
- Sedona Conference’s, “Best Practices Recommendations & Principles for Addressing Electronic Document Production” and “Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age”; and
- International Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2 Project’s, “Preserving Digital Records: Preserver Guidelines for Organizations.”

Literature Review

Digital technology poses many challenges for organizations. As they adjust from handling paper records to managing digital records, they must adapt new workflow processes and procedures facilitating their identification, maintenance, and preservation of these records which helps to ensure their authenticity and reliability.¹⁸ Legal scholars have acknowledged that ESI creates challenges for locating, retrieving, identifying, and producing relevant documentation for legal proceedings.¹⁹ The lack of proper controls (i.e., policies, procedures, technological resources, training of staff, etc.) may influence an organization’s ability to ensure the reliability of the systems from which they are produced, as well as their identification, provenance, integrity, and originality.²⁰ Furthermore, financial and securities organizations must ensure that they meet the constantly evolving standards by which the Canadian Courts address ESI. For example, in Canada, Prince Edward Island (*Electronic Evidence Act*, R.S.P.E.I. 1988, c. E-4.3) and the Yukon Territories (*Electronic Evidence Act*, R.S.Y. 2002, c. 67) have enacted legislation specific to electronic records and most other provinces and territories have amended their Evidence Acts to address digital information, such as Ontario (*Evidence Act*, ss. 34.1, 1990) and British Columbia (*Evidence Act*, ss. 41.1-41.4, 1996).

From a regulatory perspective, there is a literature void regarding the requirements, best practices, and procedures financial and regulatory organizations should follow when managing investigative records within the administrative law context. The existing literature, typically aims to inform lawyers about the nuances and procedures of administrative law and administrative tribunals, offering guidance and

¹⁸ Luciana, Duranti, “Reliability and Authenticity: The Concepts and Their Implications.” *Archivaria* 39 (Spring, 1995): 5-10 and Heather MacNeil, “Providing Grounds for Trust: Developing Conceptual Requirements for the Long-Term Preservation of Authentic Electronic Records,” *Archivaria* 50 (Fall, 2000): 52-78.

¹⁹ Todd J. Burke, et al. *E-Discovery in Canada* (Markham, Ontario: LexisNexis, 2008).

²⁰ Rosemary Pattenden, “Authenticating ‘Things’ in English Law: Principles for Adducing Tangible Evidence in Common Law Jury Trials,” *International Journal of Evidence & Proof* 12, no. 4 (2008): 273-302 and George Paul, *Foundations of Digital Evidence* (Chicago: American Bar Association, 2008) and Kenneth L. Chasse, “Electronic Records as Documentary Evidence,” *Canadian Journal of Law and Technology*, 6, no. 3 (2003): 141-162.

recommendations for navigating the system.²¹ From the records professional's perspective, there is an established body of research devoted to the proper management of records (traditional and non-traditional), and their long-term preservation,²² though only a limited number of publications that explicitly address the relationship between law and records management.²³

Due to the scant body of literature available, the researcher relied on the methodology previously explained to provide recommendations for how financial and securities regulators may best address these issues.

Statutes & Regulations

Financial and securities regulators must confirm to the relevant statutes, laws, and regulations of their respective jurisdictions. In some situations, amendments to laws, statutes, or regulations may affect operational duties and actions. Staff must be knowledgeable of relevant legislation and regulations and be informed of changes to any applicable laws. Staff should be instructed how these changes may affect their work processes.

Case Law

In common law countries, such as the United States, Canada, UK, and Australia, the courts typically rely on judicial precedent to resolve new cases; and oftentimes, cases establish the binding interpretation of statutes. Relevant case law, or judicial decisions, varies from jurisdiction to jurisdiction. Staff should be made aware of how rulings effect the organization and work processes. Even in civil law countries, legal precedent is not entirely irrelevant because the judges aim to maintain an "element of predictability in the law."²⁴

Benchmarking Practices

This project contacted and interviewed several financial and securities agencies. As stated in the methodology section, an initial contact message was sent to these and several other organizations to solicit feedback about their recordkeeping practices related to the handling of evidence. Responses came from different positions within the organizations, including records managers, investigators, and lead enforcement officers. Upon acknowledging a willingness to participate in the project, the researcher submitted a short questionnaire to be completed (Appendix 1). Once this questionnaire was completed, the researcher conducted follow-up telephone interviews with each of these organizations;

²¹ Lisa Braverman, *Administrative Tribunals: A Legal Handbook* (Ontario: Canada Law Books, 2001); Sara Blake, *Administrative Law in Canada*, 4th ed. (Markham, Ontario: LexisNexis, Butterworths, 2006); and to a lesser extent Gerald L. Gall, *The Canadian Legal System*, 5th ed. (Toronto: Carswell, 2004).

²² Luciana Duranti and Heather MacNeil, "The Protection of the Integrity of Electronic Records: An Overview of the UBC-MAS Research Project," *Archivaria*, 42 (1996): 46-67; Luciana Duranti and Kenneth Thibodeau, "The Concept of Record in Interactive, Experiential and Dynamic Environments: The View of InterPARES," *Archival Science*, 6 (2006): 26-33

²³ For example see: Heather MacNeil, *Trusting Records: Legal, Historical, and Diplomatic Perspectives* (Dordrecht: Kluwer Academic Publishers, 2000); Maria Guercio, "Principles, Methods, and Instruments for the Creation, Preservation, and Use of Archival Records in the Digital Environment," *American Archivist*, 64, no. 2 (2001): 238-269; Donald C. Force, "From Peruvian Guano to Electronic Records: Canadian E-Discovery and Records Professionals," *Archivaria*, 69 (2010): 49-75; and Luciana Duranti, Corrine Rogers and Anthony Sheppard, "Electronic Records and the Law of Evidence in Canada: The *Uniform Evidence Act* Twelve Years Later," *Archivaria*, 70 (2010): 95-124.

²⁴ Gall, p. 29.

these conversations helped clarify responses and obtain additional information about that organization's practices. This section summarizes the practices these organizations follow when managing their investigative records. The section is divided into the key areas addressed in the survey and expressed by the participants in the follow-up interviews. Additional information from the participants has also been included in the Findings section of this paper.

Investigative Record

All organizations agree that the "investigative record" constitutes all the information and evidence obtained and created by investigators and litigators that is relevant to a particular case. Such information and evidence may include hardcopy documentation such as business records, digital information such as hard drives or portable media containing electronic files in all types of formats, or other physical evidence such as white boards, computer monitors, CDs, DVDs, laptops, etc. Additionally, internally created administrative records, such as reports and e-mails exchanged between investigators and/or litigators, may become part of the investigative record. Despite the ongoing growth of ESI being produced by organizations and individuals, the nature of the organization being investigated determines the size, shape and format of the investigative record for any one investigation.

Recordkeeping Systems

For most organizations, no single recordkeeping system is capable of managing all types and forms of evidence. Organizations that handle small amounts of investigative records in limited ranges of formats may not require multiple recordkeeping systems. For example, one organization in this study relied primarily on a shared network drive to manage its investigative records. But most organizations use a combination of systems to help manage all the information that is collected and generated for investigations.

Organizations with multiple systems typically implement a combination of shared network drives, records management systems, and other databases. Regardless of the number of different systems being used, there is clear delineation about their purposes. For example, one organization uses Searchlight to store the scanned versions of all the paper documents and Enterprise Document Asset Management databases to track what documents are in use and to keep relevant notes about the case. While most of the interviewees implied that using different systems sufficed for their needs, one interviewee remarked that it was becoming problematic. The interviewee said his/her organization would be implementing new software designed to facilitate the retrieval of information by centralizing searching across the different recordkeeping systems.

Tracking Evidence

Accounting for evidence from the time it arrives at the organization, so it may be tracked as it moves throughout the organization among investigators, litigators, and records managers, is a vital component to financial and securities regulators. The organizations that participated in this research project used varying processes to ensure that their evidence (traditional and electronic) remains trustworthy (i.e., authentic and reliable) with unbroken chains of custody, though all of them use some type of an evidence document log (EDL) to account for incoming evidence and its movement throughout the organization.

While all the organizations make every effort to log every document, in many instances it is simply not feasible, such as with boxes containing documents that may only be questionably relevant. In these situations, the organizations initially account for the files at the box level but log individual documents on an as-needed basis.

The importance of consistently recording evidence in and updating the EDL is of paramount importance for these organizations. Instances where evidence is inconsistently accounted for in the EDL increases the likelihood that important evidence may be misplaced in the organization or needlessly delaying legal proceedings when staff “revise” the EDL or must search for documentation. Two of the study’s participants regulate the use of this log by having designated staff enter the evidence into the organization’s system and EDL. For example, one participant said that within his/her organization only one person has the authorization to log evidence, and in the event of this person’s prolonged absence (e.g., he/she goes on vacation), a temporary hire is not allowed to log new evidence into the EDL. Another organization also uses Excel sheets to track logged evidence but uses printed copies of the sheet to serve as place holders when investigators need to temporarily remove evidence from the exhibit room.

Physical Evidence

All organizations that participated in this research study maintain their physical evidence in secured, facilities within the confines of the organization. Officers or staff are responsible for monitoring these areas and keeping track of what physical evidence enters, who has access to these rooms, and what evidence investigators use. Access to exhibit rooms is monitored in various ways from electronic cardkey access to hardcopy sign-in and sign-out sheets. What evidence is access may be accounted for in the sign-in and sign-out sheets (typically a printed Excel document), but one participant said that his/her organization was aiming to implement an electronic signature system using barcodes to track the movement of evidence.

Electronically Stored Information

Once any hardcopy evidence is scanned and an electronic image is saved in a database or recordkeeping system, most of the organizations have procedures to ensure that only authorized personnel have access to the evidentiary records. This practices drastically reduces the risk of unauthorized deletion of them and protects the records’ chain of custody. At least one organization stated it has quality control procedures in place that checks the accuracy and/or degradation or deletion of digital information, thus ensuring its authenticity.

Retention & Disposition

There are no guiding standards or best practices for the retention and disposition of investigative records. All the participants stated that they have devised their own set of best practices and guidelines for the management of investigative records. One participant said his/her organization devised their schedules with the assistance of an outside consultant involved with the Sedona processes. Another participant pointed to relevant guiding statutes which stipulate that the agency is required to ensure the integrity of anything it stores for 25 years. Another participant stated that his/her organization retains their investigative records on site until after the appeal period, where after, the government archives receives the materials for permanent retention. In this instance, the challenges of transferring ESI is moot because the archives only accepts paper, therefore all investigative records are printed. One other participant stated that his/her organization retains enforcement files for 15 years (3 years onsite; 12 years offsite) after the case closes. Following this period the documentation is destroyed. Yet, even in this circumstance, only the paper records and correspondence located on the shared drive are destroyed; any case files located in the records management system or another database are permanently retained. Finally, other organizations have designed their policies and procedures in consultation with regional enforcement authorities, relevant statutory provisions, and through the experiences of their own institutions.

Preservation of Evidence

None of the organizations that participated have policies and procedures in place for the long-term preservation of evidence, though one participant mentioned that in his/her organization's ESI is migrated forward as systems evolve. Another participant summarized the lack of concern toward preservation matters by saying that it "is not that big of an issue because it has not been a factor to date." Another person remarked that his/her agency typically only deals with copies of copies (e.g., bank cheques), so even if an electronic files of those records becomes corrupt it is not a problem because it is easy to replace the documentation.

Findings

Based on the previous sections, this section lists the project's findings. The findings are presented in a way to reflect the research questions outlined at the beginning of this report. The first two questions are primarily questions of law. Statutes, relevant case law, and secondary legal literature form the basis for their answers. The remaining questions address best practices for managing disparate pieces of the investigative record. Answers to these questions are based on findings from the responses to the surveys, follow-up interviews, and examination of the standards, best practices, case law and secondary literature (primarily, though not exclusively, from the Canadian context).

Question 1

1. *What are the expectations and requirements for maintaining records within a legal context, including civil, criminal, and administrative law?*

The expectations and requirements for maintaining records within a legal context are implicit in statutes and judicial rulings. Although there are differences between civil, criminal, and administrative law, the judicial system holds parties to a high level of judicial fairness. Within an administrative context, this fairness arises, in part, from parties being able to fully account for and disclose relevant evidence. This process plays a vital role in judicial fairness, "ensuring that a participant in an administrative proceeding is fully informed of the case [he/she] has to meet, and ensuring that he is provided with a proper opportunity to meet that case."²⁵ For example, section 173 of the British Columbia *Securities Act*, RSBC 1996, c. 418 reads:

The person presiding at a hearing required or permitted under this Act:

- (a) has the same power that an investigator appointed under section 142 or 147 has under section 144,
- (b) must receive all relevant evidence submitted by a person to whom notice has been given and may receive relevant evidence submitted by any person, and
- (c) is not bound by the rules of evidence.

Disclosure of the relevant evidence hinges on the agency being able to locate this information. Such a process may prove difficult in organizations that rely on multiple systems to help manage and store their records (paper and electronic). Investigators or litigators who take personal liberties to manage

²⁵ Alice Woolley, "The Devil is in the Disclosure: The Role of *R. v. Stinchcombe* in Establishing Appropriate Disclosure Rules for Administrative Tribunals," *Alberta Law Review*, 40, no. 3 (2002), p. 722.

investigative records outside the defined policies and procedures of the organization potentially jeopardize case proceedings by being unable to meet disclosure requirements.²⁶

Furthermore, proper recordkeeping does not conclude for a case once the tribunal has made its decision. Once again turning to the British Columbia *Securities Act*, it allows for a person “directly affected by a decision of the commission” to appeal the ruling. Furthermore subsections (2)-(4) state:

(2) The commission or the Court of Appeal may grant a stay of the decision appealed from until the disposition of the appeal;

(3) If an appeal is taken under this section, the Court of Appeal may direct the commission to make a decision or to perform an act that the commission is authorized and empowered to do;

(4) Despite an order of the Court of Appeal in a particular matter, the commission may make a further decision on new material or if there is a significant change in the circumstances, and that decision is also subject to this section.

A case file may be required to be left open for a prolonged period of time. Following the initial decision, proper management of the investigative record is necessary to ensure a fair appeal, especially when new evidence may be introduced on appeal and required to be maintained with the original case file.

Within the criminal and civil law frameworks, and at least in Canada, there are some indications that the courts are paying more attention to parties’ recordkeeping practices. Increasingly some civil courts appear to be specifically looking at retention and disposition schedules to determine the extent to which a party may be held accountable for not being able to disclose information. One of the leading cases in Canada regarding these policies is *Ontario v. Johnson Controls Ltd.*, [2002] OJ No. 4725 (SCJ) (Quick Law), OTC 950. In this case, a box of records had gone missing which may or may not have supported the defendant’s case. The defendants argued that its absence caused prejudice to their case and the application against them should be dismissed. Justice Cameron disagreed. He argued that:

Johnson [Controls] bears substantial responsibility for any loss of its documents. There is no evidence of any document retention or destruction policy. A policy with a short retention period might offer some justification to dispose of “smoking guns” and other prejudicial evidence ... The absence of a document retention policy also constitutes a failure to recognize the court’s ability to draw an adverse inference in certain circumstances for failure to produce a document and a failure to address the practical need to retain documents once notice of a proceeding has been received.²⁷

The records management practices of Crown bodies have been scrutinized by the courts in several criminal cases. For example, in *R. v. Sivasubramaniya*, [2002] OJ No. 195 (SCJ) (Quick Law), 92 CRR (2d) 130, the police could not produce video tapes of the defendant’s arrest because their retention policy stipulated that the tapes be destroyed after one month, unless required for court, a policy based on those of other police forces.²⁸ Justice Douglas found this completely unreasonable. He ruled that there “was no sound basis for the determination of a 30-day retention period...”²⁹ This case and others

²⁶ Blake, p. 41 (citing *Kane v. University of British Columbia*, [1980] 1 SCR 1105).

²⁷ *Ontario v. Johnson Controls Ltd.*, [2002] OJ No. 4725 (SCJ) (QL) at para. 51.

²⁸ *R. v. Sivasubramaniya*, [2002] OJ No. 195 (SCJ) (QL) at para. 44–45, 92 CRR (2d) 130.

²⁹ *Ibid.*, at para. 47–48.

indicate that the courts are increasingly scrutinizing not only the records management practices and procedures of organizations but the rationale behind these actions as well. This becomes even more apparent when considering the requirements that a party must meet when introducing electronic records as evidence under the *Canada Evidence Act*. Section 31.1 of the *Act* reads:

Any person seeking to admit an electronic document as evidence has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic document is that which it is purported to be.

This is followed by the “best evidence” requirements stipulated in section 31.2(1) which are satisfied:

- (a) on proof of the integrity of the electronic documents system by or in which the electronic document was recorded or stored; or
- (b) if an evidentiary presumption established under section 31.4 applies.

According to these sections, the proponent must ensure that the recordkeeping system used to produce the records is functioning properly and did so at the time the records in question were produced. Section 31.5 of the *Act* states:

For the purpose of determining under any rule of law whether an electronic document is admissible, evidence may be presented in respect of any standard, procedure, usage or practice concerning the manner in which electronic documents are to be recorded or stored, having regard to the type of business, enterprise or endeavour that used, recorded or stored the electronic document and the nature and purpose of the electronic document.

Based on the *Canada Evidence Act*, an organization has some flexibility in how it authenticates the records it intends to submit as evidence. Despite this leeway, recordkeeping standards, such as the Canadian General Standards Board’s “Electronic Records as Documentary Evidence” and the International Organization for Standardization’s “ISO/TR 15489-1: Information and Documentation – Records Management,” stress a *higher* standard to the maintenance of records. For example, section 8 of the “Electronic Records as Document Evidence” standard focuses on the importance of audits and audit trails which account for the movement of information throughout the system; this monitoring helps safeguard their integrity and the authenticity of the records within them. In other words, an organization that relies on a centralized electronic document management system may, in fact, contain more trustworthy records than an organization that relies solely on shared drives or another type of decentralized storage system, but only when regular audits of the system occur and when security measures are in place to reduce unauthorized access to organizational documents and evidence.

Question 2

2. *Within the specific context of administrative law, for tribunals, should the same disclosure standards as civil or criminal law cases be met? Should the same admissibility standards as civil or criminal law cases be met?*

There are indications that, at least within the Canadian context, financial and securities organizations should be held to a high standard of disclosure, similar to what was established in the criminal case of *R.*

v. Stinchcombe, [1991] 3 SCR 326.³⁰ In *Stinchcombe* the Supreme Court of Canada ruled that full disclosure is necessary for judicial fairness and advances the search for truth. *Stinchcombe* has permeated into the administrative tribunal mindset and it may be difficult to convince a tribunal that any disclosure short of the *Stinchcombe* standard may be justifiable.³¹

Such a demand for disclosure may result in the prolonging of cases as litigators comb through boxes, files, and growing amounts of ESI to determine what is relevant and should ultimately be produced. Placing the *Stinchcombe* standard on organizations that fall under the administrative tribunal umbrella may negate one of the reasons tribunals were initially established, that is, to expedite the judicial process in areas of the law not covered by civil or criminal courts.³² One means to facilitate the high expectation for disclosure would be for the better education of investigators about the need to obtain only relevant documentation through disclosure orders—an approach used by at least one of the organizations interviewed for this project. The goal is to reduce the amount of evidence (hardcopy and ESI) collected by enforcement officers; this lessens the strain on litigators required to determine which evidence needs to be disclosed. A regular and formalized training program would formally establish the importance and methods of obtaining less evidence.

Despite the expectations courts may have for disclosure, there is a fairly low threshold for the admissibility of records. In fact, Judge Grimm of the U.S. District Court of Maryland in his ruling of the admissibility of ESI in *Lorraine v. Markel Insurance Co.*, 2007 U.S. Dist. LEXIS 33020 (D. Md. 2007) (Quicik Law), 241 F.R.D. 534³³ stated that when proving the authenticity of records counsel should be “creative in identifying methods of authenticating electronic evidence when the facts support a conclusion that the evidence is reliable, accurate, and authentic[....]”³⁴ In Canada, as has already been discussed, section 31 of the *Canada Evidence Act* stipulates that the proponent of the evidence must show that the system that produced it was operating properly at the time of the record’s creation. Yet, to prove the integrity of the system, the courts offer a variety of methods as stated in section 31.5 of the Act. There is no reason that financial and securities organizations should not be expected to meet these expectations. Simply because a tribunal court is not required “to apply criminal law standards to the conduct of investigations under the [*Securities Act*],”³⁵ does not mean regulatory agencies should not hold themselves to these higher standards.

By meeting criminal and civil judicial standards, financial and securities regulators will only increase the likelihood that relevant evidence proffered for any case retains its maximum weight value when assessed by the court. Furthermore, this may assist these organizations to meet the high standard of proof required of them when litigating fraud cases. Having clear policies and procedures in place to

³⁰ *Fernback (Re)*, 2004 BCSECCOM 378 (CanLII) and readdressed in *Fernback (Re)*, 2004 BCSECCOM 622 (CanLII).

³¹ In Ontario *Stinchcombe* has become the accepted standard for discovery with respect to proceedings initiated by Commission staff. The tribunal affirmed *Stinchcombe* in *YBM Magnex International Inc.*, (2000) OSCB 623 and by the Ontario Court of Appeal and the Supreme Court of Canada in *Deloitte & Touche LLP v. Ontario (Securities Commission)*, [2003] 2 S.C.R. 713.

³² Braverman, p. 20.

³³ *Lorraine v. Markel Insurance Co.*, 2007 U.S. Dist. LEXIS 33020 (D. Md. 2007) (QL), 241 F.R.D. 534. Additional commentary about the case may be found at: Paul W. Grimm, Michael V. Ziccardi, and Alexander W. Major. “Back to the Future: *Lorraine v. Markel American Insurance Co.* and New Findings on the Admissibility of Electronically Stored Information,” *Akron Law Review* 42, no. 2 (2009): 357-418.

³⁴ *Lorraine v. Markel*, 2007 U.S. Dist. LEXIS 33020 (D. Md. 2007) (QL) at *553.

³⁵ *Fernback (Re)*, 2005 BCSECCOM 80 (CanLII), para. 29.

account for the management of evidence throughout the organization that assists with proving the integrity of the electronic recordkeeping systems, which ease the burden of litigators required to present “clear and convincing proof of the elements of fraud” if only by reassuring both investigators and the courts that the evidence is authentic and reliable.³⁶

Question 3

3. *How to best support staff and investigators for e-evidence requirements, in terms of management and preservation?*

An evidence document log (EDL) is a vital component to any organization required to manage evidence. The EDL should allow investigators and litigators to track the movement of evidence throughout the organization, effectively establishing the evidence’s chain of custody. The log should facilitate the composition of disclosure packages, but organizations must protect against inconsistencies of its use, which may, in fact, hinder the litigation process. Depending on the structure of the organization, inconsistencies in using an EDL may result from investigators and litigators using it according to their own needs and interpretations of the EDL’s fields. These inconsistencies may prolong cases as staff update or edit the log to accommodate their personal preferences and position needs.

Some of this pressure may be alleviated by creating a Case Management Unit responsible for the management of investigative records throughout their lifecycle, that is, from the time they arrive at the organization or are created by staff until the time the records need to be permanently preserved or destroyed. Several financial and securities regulators already rely on such a position, whether it be in the form of a single person or a departmental unit with several staff. The Unit and its staff functions as a liaison between the enforcement, litigation, and records management units, collaborating closely with each operation but independent of them. This position should ensure that all the evidence acquired by enforcement is properly entered into the EDL and handled throughout its lifecycle. This unit’s staff may also ensure the proper access to evidence and that it is properly and efficiently handled after the case is closed. This position would ease the burden from enforcement and litigators who may be reluctant to fulfill administrative duties, such as updating the EDL. The Case Management Unit would also enable the records management unit to concentrate primarily on the proper management, retention, and disposition of administrative and other operational records.

Furthermore, most financial and securities regulators are in a unique position with regard to digital preservation. Not only do these organizations create and manage their own digital records, but they also acquire ESI. This is an important distinction. It is widely accepted among archival professionals that digital preservation starts at creation. As stated in the International Organization for Standardization’s *Digital Records Preservation: Where to Start Guide*: “the earlier in the process that the preservation activities start, the greater the assurance that the records will meet the requirements of reliability, completeness, authenticity and usability.”³⁷ Yet, when evidence is acquired, investigators oftentimes do not have the luxury of knowing the circumstances which created the ESI. To ensure the long-term survival of evidence, especially ESI, investigators and litigators need to be properly educated and trained to be able to identify materials that are high at risk for degradation. The EDL should account for these items. Such information could become important in prolonged cases and be used to facilitate identifying evidence that needs to be accessed over an extended period of time. In situations where evidence

³⁶ *Anderson v. British Columbia Securities Commission*, 2004 BCCA 7 (CanLII) at para. 29.

³⁷ International Organization for Standardization, *Digital Records Preservation: Where to Start Guide* (Geneva: International Standards Organization, 2010), p. 2.

needs to be migrated to a new medium, a policy should be implemented outlining the procedures that must be followed in the event evidence needs to be migrated to a new medium or system to ensure its continual access. This documentation will assist in defending the evidence in the event that its authenticity is challenged.³⁸

Question 4

4. *What are the issues of chain of custody, authenticity, and the admissibility of e-evidence?*
- *What are the best practices for managing disparate pieces of documentation for an investigation (i.e., some evidentiary records and administrative records are stored in the EDRMS but not all documentation for investigation is ingested into the EDRMS)?*
 - *What are the best practices for keeping all the documentation and evidence of a case connected?*

Most financial and securities organizations require multiple recordkeeping systems to manage all the different components of the investigative record. Only organizations that handle small amounts of evidence in a limited range of formats may not require multiple recordkeeping systems. But most organizations use a combination of systems to help manage all the information that is collected and generated for investigations. Such a practice may be a necessary evil.

As organizations accumulate more and more evidence in both hardcopy and digital formats, they must expand their capacity to incorporate and handle all the components of the investigative record, resulting in extra storage space (onsite and offsite) and expanding the capabilities of electronic recordkeeping systems. The further an organization moves away from a concise centralized recordkeeping structure, the greater the likelihood that evidence within that structure may be lost or mishandled if the proper management controls are not in place and regularly reviewed.

As noted in the Benchmarking Practices section of this paper, though organizations rely on different systems, in most cases, there is a clear understanding of their individual purposes. For example, one organization uses Searchlight to store the scanned versions of all the paper documents and Enterprise Document Asset Management databases to track what documents are in use and to keep relevant notes about the case. Another participant stated that his/her organization uses shared drives to only store e-mails and other correspondence. While most of the interviewees implied that using different systems sufficed for their needs, one interviewee remarked that it was becoming problematic. The interviewee said his/her organization would be implementing new software designed to facilitate the retrieval of information by centralizing searching across the different recordkeeping systems.

Each financial and securities regulator would benefit from clearly defining the purposes and authorities of its different systems. Policies should stipulate what each system is designed and designated for and who within the organization has the authority to use the different systems. Furthermore, all policies should be accompanied by a set of procedures outlining the steps staff should take in using the systems. In addition to this documentation, recordkeeping standards and best practices all emphasize the need to train staff in proper records management procedures; the organization should also include in their educating practices how the different systems should be used.

³⁸ Stephen Mason, "Proof of the Authenticity of a Document in Electronic Format Introduced as Evidence," *The ARMA International Education Foundation* (2006).

This is also an area where the Case Management Unit or position would be of value to the organization. They could ensure that all components of an investigative record are accounted for throughout its lifecycle. Personnel from this unit would have first-hand knowledge of where different materials for any given case reside among the different electronic and physical storage systems in the organization. This unit would also serve a regulatory role, ensuring that staff properly use the different electronic storage systems.

Question 5

5. *What are the best practices for the retention, disposition and preservation requirements for evidence (traditional and electronic)?*

Based on the researcher's findings, there are no standard retention, disposition and preservation periods for evidence (traditional and electronic) for financial and regulatory organizations. Scheduling investigative records depends largely on the context of the organization. For example, from the interviews, one organization maintains their case files 15 years after the case closes, another for 25 years, and another keeps them permanently.

In all cases financial and securities regulators should have an explicit definition of the term "evidence" defined in their retention and disposition schedules. Such a definition may help to manage the investigative record, in particular, what happens with evidence that is collected or created but does not become part of a legal case. A clearly articulated definition of "evidence" should clarify the distinction between what evidence goes forward and what evidence is not used. This report recommends that a broader definition be incorporated. Evidence should be defined as *all records, documents, or materials (regardless of form or format) collected or created during the investigation and litigation processes.*

Question 6

6. *What are the issues (i.e., processes and quality) involved in meeting required expectations for scanned documentation?*

Many financial and securities organizations currently out-source scanning of evidentiary documents. While some scanning occurs in-house, it must be determined if this is the proper ratio. The researcher learned that costs and turnaround time have been the primary factors for outsourcing the scanning process. Such reasons cannot be dismissed especially in light of the judicial preference seemingly in favour of electronic copies of records over the original paper records. For example, in *R. v. Jarvie*, 2003 CanLII 64366 (ONSC), the Honorable Justice Templeton wrote that "in many cases involving voluminous paper material, electronic disclosure may be the format of choice for all parties. The search capabilities afforded by electronic storage of information may well be superior in other cases to the search capabilities afforded to counsel by way of paper disclosure."³⁹ Furthermore, Master MacLeod of the Superior Court of Justice of Ontario in *Logan v. Harper*, 2003 CanLII 15592 (ONSC) ruled that even in those instances where poor copies of the documents have been disclosed, the receiving party may request a better version.⁴⁰ As these are valid justifications for outsourcing this process, they should not be the sole factors for determining if an organization should continue to rely on a third-party vendor for handling this type of evidence.

³⁹ *R. v. Jarvie*, 2003 CanLII 64366 (ONSC), at para. 37.

⁴⁰ *Logan v. Harper*, 2003 CanLII 15592 (ONSC), at para. 32.

On a periodic basis, organizations need to review their position toward outsourcing the scanning of evidentiary documents in the context of a risk-based assessment framework. Each organization needs to ensure the trustworthiness of any of the digitized documents; and be able to assess the vendor's staff's skill-base and the technologies it uses. In order to maintain the chain of custody of any of the records, it is vital to know the vendor's policies and procedures for handling evidence. These practices should indicate the security measures the vendor has in place to protect the records from wrongful tampering or spoliation and what quality control measures it employs to ensure the reliability of the digital records. Only if all these criteria satisfy the organization's needs should it continue to outsource the scanning of documentary evidence.

In the event that the organization increases the amount of documentation it scans in-house, organizations may consult the Canadian General Standards Boards' CAN/CGSB-72.11-93: "Microfilm and Electronic Images as Documentary Evidence" (1993; amended in 2000), which "provides rules and guidelines for organizations to establish and operate a credible image management program with the ability to demonstrate that the resulting captured images are accurate reproductions of source records." Additional standards and guidelines that may be of assistance include the CAN/CGSB-72.34: "Electronic Records as Documentary Evidence" (2005) which specifies principles and procedures for creating all forms of electronic records to enhance their admissibility as evidence in legal proceedings, and the ANSI/AIIM Technical Report (TR31) "Legal Acceptance of Records Produced by Information Technology Systems" (2004), which provides "performance guidelines and self-assessment checklists to help ensure admissibility and trustworthiness of the printouts" within an American context.

Adherence to these standards becomes important in light of the "best evidence" as established in the *Canada Evidence Act*. As previously discussed in the answer to Question #1 (pp. 15-17), the *Act* emphasizes a party's ability to show the system which maintained the documents in question. Thus, the organization must ensure its scanning policies and procedures are clearly articulated and account for what happens to the "original" documents when they are no longer needed.

In light of these arguments, the process by which documents are scanned and the quality of the scans remains an open question and is an area that requires further investigation.

Recommendations

Based on the project's findings, this section summarizes the recommendations made in this report. These recommendations intend to guide financial and securities regulators in the future management of their investigative records, regardless of form or format.

1. Financial and securities regulators must hold themselves to a high records management standard. This will ensure the integrity of evidentiary and business records and may be done by adhering to some of the following practices and principles:
 - Recordkeeping policies need to be regularly updated to address organizational changes and meet the emergent requirements of the organization;
 - Recordkeeping procedures need to be regularly updated to address organizational changes and meet the emergent requirements of the organization; and

- Staff should properly use and rely on the organization’s document management system for the creation, storage, or tracking (e.g., of physical evidence such as a hard drive) of investigative records.
2. Each financial and securities regulator should have a Case Management Unit, or person responsible for the duties outlined below. This unit/individual needs to be independent of enforcement, litigation, and records management. The unit’s/individual’s responsibilities would include but not be limited to:
 - Logging evidence that arrives at the organization;
 - Accounting for evidence created by the organization;
 - Managing evidence (physical and digital) throughout the organization;
 - Ensuring the proper access to investigative records;
 - Monitoring the evidence storage rooms (i.e., who has access to them, what is deposited, what is removed, etc.);
 - Ensuring the needs of enforcement, litigation, and records management are met in terms of the handling of investigative records; and
 - Conducting audits of case files (i.e., accounting for all pieces of evidence for the case) upon the closure of a case.
 3. Organizations need to investigate using technology (e.g., barcode or RFID) to track evidence. This technology will:
 - Strengthen the chain of custody of the evidence;
 - Track the movement of evidence throughout the organization; and
 - Establish staff accountability for handling evidence.
 4. For ESI that is at high-risk of degradation, financial and securities regulators need to create a preservation policy/plan. This policy should include, but not be limited to the following components:
 - Identification of the scope and objectives of any digital preservation activities (i.e., what will be preserved);
 - Identify file formats and storage media capabilities of the organization;
 - Establish procedures for handling evidence when it needs to be transferred to a more stable media, converted to new software/hardware, or for emulating (i.e., recreating) the original environment;
 - Determine how the evidence will be upgraded (e.g., will it be converted into new formats/platforms, migrated to new media, or will the original environment be emulated). Note: Different types of evidence may require different methods;
 - Establish procedures for how staff should proceed when they identify ESI at high-risk for degradation; and

- Establish a policy and/or procedures that account for the original evidence—where it may be stored and how it may be handled after it has been transferred to a more stable media or converted to new software/hardware.
5. Each financial and securities regulator must define the purposes and authorities of its records and evidence management systems. The purposes and authorities (i.e., permissible access) may be incorporated into existing policies and procedures or may result in the creation of new policies and procedures. This documentation should clearly articulate the roles these systems have within the organization and how they facilitate the management of investigative records.
 6. Each financial and securities regular must clearly define what it means by “evidence” in its retention and disposition schedules. This definition may help manage the investigative record, in particular, what happens with evidence that is collected or created but does not become part of a legal case. A clearly articulated definition of “evidence” should clarify the distinction between these two evidentiary issues. This report recommends that a broader definition be incorporated. Evidence should be defined as *all records, documents, or materials (regardless of form or format) collected or created during the investigation and litigation processes*.
 7. When tracking evidence, organizations should consider using at least three different documents. These documents may be incorporated into one database or centralized tracking system. The three documents include:
 - **Evidence receipt log.** This document would account for the receipt of evidence at the financial and securities regulator. This log should contain, but be not limited to, the following fields:
 - Date the investigator collected the evidence;
 - Name of investigator who collected the evidence;
 - Description of the evidence;
 - Notes about the evidence;
 - Identification number;
 - Location of the evidence (i.e., storage room number);
 - Name of person responsible for logging the evidence; and
 - Date the evidence was logged.
 - **Evidence room tracking log.** All evidence must be stored in the secure evidence rooms. This document would account for the removal of evidence from these areas and it should contain, but not be limited to, the following fields:
 - Identification number of the box/item;
 - Name of person who checked out the material; and
 - Date & time it was checked out.
 - **Exhibit log.** This sheet would account for any necessary in-house scanning of exhibits, and disclosure information of the exhibits. It should contain, but not be limited to, the following fields:
 - A note if the item needs to be scanned;
 - Date it was scanned;
 - Name of person who scanned it;

- A note if the item is to be disclosed;
 - The disclosure number;
 - A note if the item is to be used as an exhibit in court;
 - A note if the item was used as an exhibit in court; and
 - The exhibit number.
8. Evidence tracking documentation proposed in Recommendation #7, should become the responsibility of a “neutral” unit within the financial and securities regulator, such as the Case Management Unit (see Recommendation #2). Staff in this unit would be responsible for the consistent receipt of evidence, its entry into the relevant documentation, and tracking throughout the organization.
9. Relevant staff within financial and securities organizations, in particular, investigators and litigators, need to be properly educated and trained in identifying evidential materials that are high at risk for degradation. This information needs to be accounted for in evidence tracking documentation.
10. Each financial and securities organization should periodically review its position on outsourcing the scanning of evidentiary documents in light of a risk-based assessment framework. Factors that need to be considered should include but not be limited to:
- Does the vendor’s staff have the appropriate skill-base?
 - Is the financial and securities regulator able to communicate its requirements for scanned materials?
 - How does the vendor manage the original evidence?
 - What documented policies and procedures does the vendor have in place to ensure the chain of custody of the evidence?
 - Does the financial and securities regulator have access to the original records when they are in the vendor’s possession?
 - What are the quality control measures of the vendor?
 - How quickly is the vendor able to scan and return the records?
 - What security controls does the vendor employ for safeguarding both the original and electronic records?
 - What is the risk of the vendor’s business failing?

Summary

The proper management of investigative records is a serious concern for financial and securities regulators. The volume of these records, both paper and digital, threatens any organization’s ability to maintain their chain of custody, be able to produce them for litigation purposes, and properly handle them at the completion of a case. Currently, there are no standards or best practices designed for securities regulators to manage their investigative records. These practices occur in accordance with each organization’s own environmental, cultural, and regulatory needs.

This report discusses how several financial and securities regulators manage their investigative records. Organizations responsible for the management of evidence must maintain tight control over their records. This may be accomplished by instituting policies and procedures for logging and tracking evidence, properly securing evidence, and documenting when investigators or litigators access the evidence. Most organizations must use a combination of electronic recordkeeping systems to help manage the different pieces of legal case files; there is no single electronic system capable of handling all the various types of evidential materials.

Since some legal cases may take extended periods of time to be resolved or decided, organizations need to be prepared to handle digital evidence that is at high-risk for deterioration. Digital preservation is not currently a major priority for financial and securities regulators. To avoid not being able to access digital records or produce authentic digital records five or ten years after the acquisition of evidence, these organizations need to create policies and procedures that outline how the organization will ensure the continued accessibility and authenticity of these records. Staff must be educated in the identification of digital evidence that is susceptible to degradation and initiate the process to ensure its long-term survival. Inaction jeopardizes the organization's ability to use the evidence in court.

By adopting the recommendations proposed in this report, these organizations will strengthen the management of investigative records. These practices will help ensure that financial and securities regulators may continue to effectively and efficiently respond to legal challenges in order to promote and safeguard a dynamic and fair securities market.

Bibliography

Monographs

- Arkfeld, Michael R. (2006). *Electronic Discovery and Evidence*. Phoenix, AZ.: Law Partner Publishing, LLC.
- Blake, Sara. (2006). *Administrative Law in Canada*. 4th Edition. Markham, Ontario: LexisNexis, Butterworths.
- Braverman, Lisa. (2001). *Administrative Tribunals: A Legal Handbook*. Ontario: Canada Law Books.
- Daft, Richard L. (2001). *Organization Theory and Design*. 7th Edition. Cincinnati, OH: South-Western College Publishing, 2001.
- Dee, Dwight D. (2009). *A Basic Overview of Securities Regulations in British Columbia*. Vancouver: Legal Education Society of British Columbia.
- Ewart, J. Douglas. (1984). *Documentary Evidence in Canada*. Ontario: Carswell Legal Publications.
- Gall, Gerald L. (1990). *The Canadian Legal System*. 3rd edition. Toronto: Carswell.
- Paul, George L. (2008). *Foundations of Digital Evidence*. Chicago: American Bar Association.
- Paciocco, David M. and Lee Stuesser. (2005). *The Law of Evidence*. Toronto: Irwin Law.
- Rice, Paul R. (2005). *Electronic Evidence: Law and Practice*. Chicago: ABA Publishing.

Articles

- Blue, Ian A. (1989). "Administrative Law Hearings: A Comparison of U.S. and Canadian Practice." *Administrative Law Review*, 41(4): 481-490.
- Casswell, Donald G. (1991): "Through the Admissibility of Evidence Maze: An Attempt at a Purposive Structuring." *Alberta Law Review*, 29(3): 584-616.
- Coffee, Jr., John C. (2007). "Law and the Market: The Impact of Enforcement." *University of Pennsylvania Law Review*, 156(2): 229-311.
- Duranti, Luciana. (2001). "The Impact of Digital Technology on Archival Science." *Archival Science* 1(1): 39-55.
- _____. (1995). "Reliability and Authenticity: The Concepts and Their Implications." *Archivaria*, 39: 5-10.
- Giannelli, Paul C. (1983). "Chain of Custody and the Handling of Real Evidence." *American Criminal Law Review*, 20(3): 527-568.
- Hoffman, Norton and Robert Klepper. (2000). "Assimilating New Technologies: The Role of Organizational Culture." *Information Systems Management*, 17, no. 3 (2000): 1-7.

Lynch, Clifford. (2000). "Authenticity and Integrity in the Digital Environment: An Exploratory Analysis of the Central Role of Trust." In *Authenticity in a Digital Environment*, 1-20. Washington, DC: Council on Library and Information Resources.

MacNeil, Heather. (2000). "Providing Grounds for Trust: Developing Conceptual Requirements for the Long-Term Preservation of Authentic Electronic Records." *Archivaria*, 50: 52-78.

Weiler, Paul C. (1976). "The Administrative Tribunal: A View from the Inside." *University of Toronto Law Journal*, 26(2): 193-214.

Winklhofer, Heidemarie. "Organizational Change as a Contributing Factor to IS Failure." *Proceedings of the 34th Hawaii International Conference on System Sciences (HICSS-34)*, 8 (2001): 1-9.

Woolley, Alice. (2002). "The Devil is in the Disclosure: The Role of *R. v. Stinchcombe* in Establishing Appropriate Disclosure Rules for Administrative Tribunals." *Alberta Law Review*, 40(3): 717-742.

Wortzman, Susan and Susan Nickle. (2009). "Obtaining Relevant Evidence." *Advocates' Quarterly*, 36(2): 226-268.

Reports

British Columbia Securities Commission (BCSC). (2010). *Annual Report 09-10*. British Columbia Securities Commission.

Hume, Gavin, Robert Brun, Bruce LeRose, Glen Ridgway, and Kenneth Walker. (2009). "Report of the Mirror Imaging Working Group: Forensic Copying of Computer Records by the Law Society." Law Society of British Columbia.

Kitching, Andrew. (2009). "Securities Regulation: Calls for a Single Regulator." Parliamentary Information and Research Service of the Library of Parliament.

Standards / Best Practices / Guidelines

Association of Chief Police Officers. (n.d.). "Good Practice Guide for Computer-Based Electronic Evidence." 7Safe Information Security. Available online at http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf (last accessed 12 January 2010).

European Commission. (2010). "Document Management in the European Commission: Collected Decisions and Implementing Rules."

Financial Services Authority. (2005). "Records Management Policy and Standards – RMPS." United Kingdom, 2005.

Government of Canada. (2005). "CAN/CGSB-72.34-2005: Electronic Records as Documentary Evidence." Gatineau, Canada: Canadian General Standards Board.

International Association for Identification, Scientific Working Group on Imaging Technology (SWGIT). (2007). "Best Practices for Archiving Digital and Multimedia Evidence (DME) in the Criminal

Justice System.” Available online at <http://www.theiai.org/guidelines/swgit/index.php> (last accessed 14 October 2010).

_____. (2009). “Digital Imaging Technology Issues for the Courts.” Available online at <http://www.theiai.org/guidelines/swgit/index.php> (last accessed 14 October 2010).

International Association of Chiefs of Police Advisory Committee for Police Investigative Operations, PricewaterhouseCoopers, LLP, Technical Support Working Group, and U.S. Secret Service. (n.d.). “Best Practices for Seizing Electronic Evidence.” 2nd edition. United States Secret Service. Available online at <http://www.forwardedge2.usss.gov/pdf/bestPractices.pdf> (last accessed 12 January 2010).

International Organization on Computer Evidence. (2002). “Guidelines for Best Practice in the Forensic Examination of Digital Technology.” Available online at www.ioce.org/fileadmin/user_upload/2002/ioce_bp_exam_digit_tech.html (last accessed 14 October 2010).

International Organization on Computer Evidence. (2000). “Good Practices for Seizing Electronic Documents.” Available online at <http://www.ioce.org/core.php?ID=17> (last accessed 18 January 2010).

InterPARES Project. (2008). “Preserver Guidelines: Preserving Digital Records: Guidelines for Organizations.” Available online at http://www.interpares.org/ip2/ip2_documents.cfm?cat=pg (last accessed 23 February 2011).

International Organization of Standardization. (2010). “Digital Records Preservation: Where to Start Guide.” Available online at <http://www.archives.org.il/UserFiles/File/129041223446.pdf> (last accessed 18 January 2010).

_____. (2001). “ISO/TR 15489-1: Information and Documentation – Records Management – Part 1: General.”

_____. (2001). “ISO/TR 15489-2: Information and Documentation – Records Management – Part 2: Guidelines.”

Local Government Management Association. (2006). “Records Management Manual for Local Government in British Columbia.” 3rd Edition.

Mason, Stephen. (2006). “Proof of the Authenticity of a Document in Electronic Format Introduced as Evidence.” *The ARMA International Education Foundation*.

Sedona Conference Working Group on Electronic Document Retention & Production (WG 1). (2006). “ISO 23081-1: Information and Documentation – Records Management processes – Part 1: Principles.”

_____. (2008). “The Sedona Conference Commentary on ESI Evidence & Admissibility.”

_____. (2007). “The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production.” *The Sedona Conference*.

_____. (2007). “The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age.” *The Sedona Conference*, 2nd Edition.

Sedona Conference Working Group 7, Sedona Canada. (2008). “The Sedona Canada Principles: Addressing Electronic Discovery.” *The Sedona Conference*.

Task Force on the Discovery Process in Ontario. (2005). “Guidelines for the Discovery of Electronic Documents in Ontario.” ON: Commonwealth Legal.

Appendix 1 – Questions for External Organizations

- What technologies or information systems does your organization use to manage evidence?
 - Does your organization rely on an electronic document or records management system (EDRMS)?
 - What system controls are in place to prove the trustworthiness (i.e., authenticity and reliability) of the evidence?
 - If your organization relies on an EDRMS, does all evidence fit within this system?
 - For example, how would you handle a hard drive?
- Are investigative and litigation processes treated as one, or as separate processes handled by separate individuals and/or units?
- Does your organization make a distinction between administrative records made during the course of an investigation and evidence obtained by investigators?
 - If yes, how are administrative records linked to the evidence throughout the investigation and litigation processes?
- How do you ensure the chain of custody of evidence (electronic and/or traditional) from the time it is acquired to the time it is used in court?
 - When collecting/creating evidence how is it registered initially?
 - How is its location and custody tracked throughout the investigative and/or litigation process?
 - When evidence is handed off between individuals or work units how is the chain of custody maintained or tracked?
- What professional best practices or guidelines (e.g., Sedona) do you follow when managing evidence (electronic and/or traditional)?
 - Have you devised your own set of best practices or guidelines? If yes, are these based on any sets of professionally available best practices or guidelines?
- What guidelines or best practices does your organization follow for the retention and disposition of evidence?
- What guidelines or best practices does your organization follow for the long-term preservation of evidence?
 - Do you have any policies in place for the long-term preservation of evidence? If yes, are these based on any professionally published policies or guidelines?
- What recommendations would you have regarding best practices for handling of this type of evidence?
- Which, if any, legal rulings have influenced how you manage evidence?

Appendix 2 – Standards, Guidelines, and Best Practices (Annotated)

Electronic Records as Documentary Evidence (2005)

Published in 2005 by the Canadian General Standards Board and approved by the Standards Council of Canada, this standard specifies principles and procedures for creating all forms of electronic records to enhance their admissibility as evidence in legal proceedings. The document applies to organizations and individuals who receive, create, capture, maintain, use, store or dispose of records electronically.

ISO 15489: Information and Documentation – Records Management

Part 1: General (2001)

Part 1 of this standard provides guidance on managing records of originating organizations, public or private, for internal and external clients. The standard provides guidance on determining the responsibilities of organizations for records and records policies, procedures, systems and processes; and provides guidance on records management in support of a quality process framework to comply with other standards, such as ISO 9001: *Quality Management Systems* and ISO 14001: *Environmental Management Systems*. The elements outlined in Part 1 are recommended to ensure that adequate records are created, captured and managed.

Part 2: Guidelines (2001)

This component of ISO 15489 outlines the procedures that help to ensure the management of records according to the principles and elements covered in Part 1. Part 2 is an implementation guide to be used by record management professionals and those charged with managing records in their organizations. It provides one methodology that will facilitate the implementation of Part 1 in organizations that have a need to manage their records. It gives an overview of the processes and factors to consider in organizations wishing to comply with ISO 15489-1.

ISO Digital Records Preservation: Where to Start Guide (2010)

The intended audience is the person, groups or business units in an organization tasked with the development of plans for the preservation of digital records. This standard aims to provide its users with an understanding the issues specific to preservation of digital records; guide users in developing a preservation plan; provide users with the necessary knowledge so they may be able to safeguard their digital records asset over time with confidence; and offer additional resources to digital preservation projects and literature.

Preserving Digital Records: Guidelines for Organizations (2008)

Produced by the InterPARES 2 project (International Research on Permanent Authentic Records in Electronic Records), this document offers a series of recommendations for organizations responsible for the long-term preservation of authentic digital records. The guidelines cover a number of areas, such as appraisal, acquisition, storage, and access that should be considered when preserving digital records.

Records Management Manual for Local Government in British Columbia (2006)

This manual aims to “provide general records and information guidance to staff in the various local government organizations in the province of British Columbia.” The manual also includes the basic records management instruments including a records classification and retention schedule, a model bylaw, as well as samples of forms and practical tips for all aspects of records management.

Sedona Canada Principles: Addressing Electronic Discovery (2008)

This set of principles draws on those guidelines established in the United States as part of the Sedona Conference, a nonprofit legal think tank dedicated to the advanced study of law and policy, designed to address issues of electronic discovery (e-discovery) in the Canadian context. The document addresses issues raised by e-discovery and outlines principles, or best practices, by which legal counsel should operate to best confront these matters.

Sedona Guidelines for Managing Information & Records in the Electronic Age (2007)

This document establishes five primary principles that organizations should adhere to for the management of electronic information for its business, statutory, regulatory and legal needs. The document provides legal commentary on each of these principles, drawing on relevant U.S. case law and secondary legal sources.

Appendix 3 – System Map Example

