Presented to the Interdisciplinary Studies Program:

UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Applied Information Management
and the Graduate School of the
University of Oregon
in partial fulfillment of the
requirement for the degree of
Master of Science

Employing the Generally Accepted Recordkeeping Principles® (GARP®) to Identify Practices for Efficient and Compliant Electronic Records and Information Management

CAPSTONE REPORT

Jason C. Stearns, CRM
Corporate Vice President
Corporate Records Manager
New York Life Insurance Company

University of Oregon
Applied Information
Management
Program

July 2010

Continuing Education
1277 University of Oregon
Eugene, OR 97403-1277
(800) 824-2714

Approved by

_____

Dr. Linda F. Ettinger
Senior Academic Director, AIM Program

Employing the Generally Accepted Recordkeeping Principles® (GARP®) to Identify Practices for Efficient and Compliant Electronic Records and Information Management

Jason C. Stearns, CRM

New York Life Insurance Company

Abstract

Information Technology (IT) and Records and Information Management (RIM) professionals must work together to manage the expansion of electronic records and information (ARMA International, 2009e). This study, based on literature published between 2005 and 2010, employs the *Generally Accepted Recordkeeping Principles® (GARP®)* to identify 23 practices for effective and compliant electronic RIM. Practices, framed in relation to eight GARP® principles, are presented as a comprehensive guide for RIM and IT professionals tasked with recordkeeping responsibilities.

Keywords: electronic records, GARP®, recordkeeping, records management, RIM

Table of Contents

List of Tables

Introduction to the Literature Review

Purpose

The purpose of this study is to conduct a preliminary examination to identify practices for efficient and compliant electronic records and information management (RIM). The approach is to first extrapolate a set of recordkeeping requirements from the Generally Accepted Recordkeeping Principles® (GARP®) and then use these as a framework within which to identify practices from selected literature. For the purposes of this study, requirements are defined as the various constraints, necessities, needs, or parameters that must be met or satisfied for the creation and maintenance of records by an organization.

GARP® was developed with "all of the major ANSI/ISO/ARMA standards playing a foundational role" (ARMA International, 2009a, para. 3) and is intended to set forth the characteristics of an effective recordkeeping program (ARMA International, 2009d). As a result, this researcher believes that GARP® can play a significant part in the identification of practices for the management of electronic records and information.

For Information Technology (IT) departments, RIM practices are typically not a priority and they frequently lack the methodology and expertise needed to address the issues (Stephens, 2009). RIM managers too often cling to the idea that paper will be around forever and address their efforts there (Stephens, 2009). Like it or not, these disciplines are being forced to work together due to the rapid and expanding growth of electronic records and information (ARMA International, 2009e). As a result, RIM professionals need to extend their knowledge of IT practices, and IT professionals need an understanding of the relevant RIM requirements and methodologies (ARMA International, 2009e).

The assumption underlying this study is that with the growing need to manage information correctly, recordkeeping practices are no longer a skill set exclusive to RIM professionals (ARMA International, 2009d). All members of the organization involved with the information lifecycle are in need of an understanding of key recordkeeping requirements, skills and practices (ARMA International, 2009d).

Problem/Significance

Records and recordkeeping are essential to the operation of organizations (ARMA International, 2009d). According to Marcella (2008) greater than 90% of all business information originates in electronic forms. In response, organizations commonly invest significant human and economic resources in attempts to manage the millions of electronic documents and email they create and maintain (Mattox, 2007).

Though the overall growth and significance of electronic records and information has been dramatic in recent years (Stephens, 2009), fewer than 40% of respondents to a 2003 survey indicate that they address electronic records and information in their records management strategies, policies or procedures (Launchbaugh, 2004). The failure to adequately address electronic RIM issues represents a disconnect between those responsible for the application of RIM practices, the RIM professionals, and those responsible for the day-to-day management of electronic records and information and the systems that create and maintain them, the IT professionals (Launchbaugh, 2004).

Since the late 1980s, the pressure to address the challenges associated with the management of electronic records has been growing (Saffady, 2009). More recent events have had an even greater impact on the need to address these challenges:

- The Sarbanes-Oxley Act of 2002 requiring corporate boards and executives to set policies to ensure, and attest to, the accuracy of their records (Stephens, 2009; ARMA International 2002)
- Judge Scheindlin's rulings in *Zubulake v. UBS Warburg LLC* reinforcing the importance of proper record retention practices and the need for record and information preservation when litigation arises (Interwoven, Inc., 2004)
- The fallout from *Arthur Andersen v. United States* (2005) and the other corporate scandals of the early 2000s (Stephens, 2009)
- The 2006 amendments to the Federal Rules of Civil Procedure (FRCP) that incorporate and normalize the concept of electronically stored information (ESI) and establish requirements for the search and production of electronic records and information in the federal courts (AXS-One, Inc., 2007)

These events and others, combined with the ever-increasing volume of electronic records and information, are resulting in RIM and IT professionals becoming increasingly involved in the management of the information lifecycle (ARMA International, 2009e).

Unfortunately, IT professionals and RIM professionals rarely work together in pursuit of electronic RIM (Chosky, 2008). A 2008 study indicates that fewer than 15% of RIM and IT professionals share a reporting relationship to the same senior executive (Chosky, 2008). Further, many RIM professionals complain that IT staff are unwilling to give up control to records management (Chosky, 2008).

Audience

The intended audiences for this study are RIM and IT professionals tasked with the responsibility of managing electronic records and information. While immediately applicable to Corporate Records Managers, Chief Record Officers (CRO) and Chief Information Officers (CIO) responsible for developing the programs and structures for the delivery and management of information and records (ARMA International, 2008), other members of the IT organization also have a role to play (ARMA International, 2009d).

Electronic information and records are only as usable and reliable as the system used for their creation and maintenance (ARMA International, 2009d). As a Certified Records Manager (CRM) and RIM professional at a Fortune 100 company, this researcher is painfully aware of the need to manage electronic records and information. The volume of electronic information created and managed at my company, and others its size, is typically measured in terabytes and petabytes; the sheer volume of information is staggering. As the appointed officer in the organization responsible for developing the corporate strategy for the management of company records, practices that address the challenges of electronic records and information management throughout the enterprise are of particular interest. As a result, system administrators, application developers, information security professionals, network administrators and other members of the IT organization must be involved (ARMA International, 2009d). As noted by ARMA International (2009e), when it comes to the management of electronic records and information, RIM and IT professionals need to collaborate proactively. For the collaboration between RIM and IT professionals to be effective, each group should be familiar with the requirements of their respective discipline. This study is not intended to provide an exhaustive review of either discipline or the identified practices. Additionally, this study does not address organizational

issues such as reporting structures or the internal placement of records management functions within the enterprise.

Outcome

The outcome of this study is a guide that presents an initial set of practices for use by RIM and IT professionals, as they work together in pursuit of efficient and compliant electronic records and information management. The guide is arranged in two main sections: (1) an overview of the GARP® principles and the recordkeeping practices derived from them, and (2) a listing of practices that meet the identified requirements.

Delimitations

Literature collection. Resources that provide literature for use in this study include academic indexes and databases, publications of ARMA International, general searches of the World Wide Web, and this researcher's personal collection of periodicals, standards and texts related to records and information management. Searches of online resources use keywords derived from the GARP® principles, the various standards and guidelines used in their development, and from the analysis of literature from this researcher's personal collection.

GARP® foundational references. As GARP® was developed with "all of the major ANSI/ISO/ARMA standards playing a foundational role" (ARMA International, 2009a, para. 3) the publications of ARMA International are a key resource available for review in this study. These publications are considered relevant and credible due to ARMA International's status as a not-for-profit professional association known worldwide for setting standards and best practices, and for providing comprehensive education, publications, and information on records and information management (ARMA International, 2009c).

The standards and guidelines used in the development of the GARP® principles constitute a significant number of the literature resources referenced in this study. These resources are not explicitly listed in the GARP® principles or in the various publications addressing GARP®. These standards and guidelines are identified through direct communication with representatives from the publisher of GARP®, ARMA International, and members of the GARP® development committee.

According to ARMA International President-elect and GARP® committee member Galina Datskovsky, Ph.D., CRM (personal communication, May 13, 2010) and GARP® committee member Lenore Greenburg, CRM (personal communication, May 12, 2010), of the multitude of standards, guidelines and other materials referenced during the development of GARP®, four were particularly influential:

- **ISO 15489** – *Information and documentation – records management part 1 & part 2* published by the International Organization for Standardization.
- **DoD 5015.2 –** *DoD5015.2-STD, Electronic records management software applications design criteria standard* published by the U.S. Department of Defense.
- **MoReq2** – *Model requirements for the management of electronic records, Update and extension, 2008,* published by the DLM Forum.
- **Current litigation trends and precedents** – GARP® was not influenced by a specific precedent or case, but rather by the general trends in litigation observed over the last several years (G. Datskovsky, personal communication, May 13, 2010). As a result, the publications and guidance provided by The Sedona Conference® are referenced for the following reasons: the organization's role as a, "research and educational organization that focuses on complex litigation issues and intellectual property rights" (The Sedona

Conference®, 2005, p.106); their expert ability to summarize, comment and provide guidance on litigation trends and issues (G. Datskovsky, personal communication, May 13, 2010); and the participation in The Sedona Conference® by GARP® committee members and subject matter experts consulted during its development (G. Datskovsky, personal communication, May 13, 2010).

To limit the scope of this study, the standards and guidelines reviewed in conjunction with GARP® in an effort to derive recordkeeping requirements for electronic RIM are mostly limited to these references. Additional ARMA International standards and publications used in the development of GARP® are referenced to provide supporting information, background material, detailed requirements, and standardized definitions as needed.

Selection and evaluation criteria. For a resource to be deemed appropriate to this research it must produce relevant and credible results. For the purposes of this study, relevant resources are those that directly address topics and issues related to the general practices of records information management, those specifically addressing topics and issues of electronic records and information management, and/or those that detail IT practices addressing issues related to electronic records and information management. The criteria used to establish a resource as credible include: (a) references that include the full text and are published in a peer-reviewed journal; (b) references written by a recognized expert in their field; (c) references published by a recognized industry trade organization, standards organization, university or academic institution, or governmental body; and/or (d) whitepapers published by a recognized industry leader in their respective field (Bell & Smith, 2009).

Time frame. While the need to address the challenges of managing electronic records and information has been growing since the late 1980s (Saffady, 2009), more recent events have raised this need to new levels of importance (Stephens, 2009). The concepts of records management are not new (Stephens, 2009); however, with the exception of technology independent best practices and standards, references for this study are limited to the last five years to ensure that the information in this study is relevant to current challenges.

Topic Focus. According to the International Organization of Standardization (ISO) (2001a), the field of records and information management addresses the efficient and systematic control of the records and information through all aspects of the information lifecycle independent of media or format. As a result, records management practices impact a wide range of disciplines including physical file management, forms management and creation, database management, information security, mail services, reprographics and others (Robek, Brown, & Stephens, 1995). This study does not address these multiple facets of RIM nor the related technologies and supporting practices. This study is limited to recordkeeping requirements for the management of electronic records and information identified from an analysis of the GARP® principles. Additionally, while this study does address areas of commonality where RIM and IT professionals can work together to address the challenges associated with electronic records and information management, it does not address organizational issues such as reporting structures or the internal placement of records management functions within the enterprise.

Search strategy. The search for practices related to electronic RIM is limited to those that are relevant to the recordkeeping requirements extrapolated from the GARP® principles. RIM programs and practices cover a number of other related topics (Robek et al., 1995); unless

directly related to electronic RIM practices and related to the recordkeeping requirements extrapolated from the GARP® principles, these have been excluded.

Intended audience. This literature review is intended to serve as a guide for RIM and IT professionals tasked with addressing the challenges of managing the growing volume of electronic records and information. When it comes to the management of electronic records and information, RIM and IT professionals need to collaborate proactively (ARMA International, 2009e). This study is not intended to assist general business managers in their pursuit of RIM goals.

Exclusions. This study does not provide an exhaustive review of records management practices, RIM technologies, or the detailed application and implementation requirements of the identified practices.

The concept of "requirements." A requirement is defined as the "constraints, demands, necessities, needs, or parameters that must be met or satisfied" (BusinessDictionary.com, 2010h, para. 1). Specific to Records and Information Management, ARMA International (2007a) defines recordkeeping requirements as the "statutory or regulatory requirements, or administrative directives, that define obligations for the creation and maintenance of records by an organization" (p. 4). For the purposes of this research, a hybrid of these definitions will be used: Constraints, demands, necessities, needs, or parameters that must be met or satisfied for the creation and maintenance of records by an organization.

The concept of "practices." Though this study identifies practices for the management of electronic records and information, it is important to note that the practices identified herein may not be appropriate for all organizations or situations (BusinessDictionary.com, 2010c). It is the responsibility of the reader to understand the business, legal, regulatory or other factors that

may impact recordkeeping requirements and the applicability of any practice to the circumstances faced by his/her organization.

Data Analysis Plan Preview

The data analysis process in this study is designed to examine a variety of standards, guidelines, best practices, and academic and professional publications in an effort to identify practices for electronic RIM. The overall data analysis goal is to identify meaningful relationships (Busch, De Maret, Flynn, Kellum, Le, & Meyers, 2005) between the GARP® principles and methods and techniques for electronic RIM in an effort to identify related practices. A *practice* is defined as the "methods, procedures, processes and rules used in a particular field or profession" (BusinessDictionary.com, 2010g, para 1). A *best practice* is defined as the "methods and techniques that have consistently shown results superior than those achieved with other means" (BusinessDictionary.com, 2010, para. 1). For the purposes of this research, a hybrid of these terms is used to create a stricter definition for practice: methods, procedures, processes and rules used in a particular field that have shown superior results.

To accomplish this goal, the selected data analysis approach is content analysis as described by Busch, De Maret, Flynn, Kellum, Le, and Meyers (2005). This approach provides a research tool that can be used to verify the presence of certain words or concepts within texts or sets of texts through a process known as coding.

Specifically, the data analysis process is designed to examine the GARP® principles and the foundational standards used in their development in order to identify recordkeeping requirements for the management of electronic records and information. Each principle, and the texts used in their development, is initially examined to develop a set of keywords that are representative of the recordkeeping requirements of each principle. These keywords are then

used to search for and code literature to identify themes related to the management of electronic records and information. Coding of the texts is used to establish relationships between the identified practices and the related GARP® principle in an effort to identify related practices.

The analysis process is organized in two stages:

1. Examination of the GARP® principles and the standards and guidelines used in their development to extrapolate a set of requirements for the effective management of electronic records and information.
2. Identification of practices for electronic RIM that meet the requirements developed from the GARP® principles through the coding of identified literature.

Writing Plan Preview

This study is structured as a review of literature that relates and extends the work of prior studies (Creswell, 2009) on the topic of electronic records and information management. Relevant and credible references are examined during the data analysis process in an effort to establish a set of recordkeeping requirements that are derived from the GARP® principles and to identify a preliminary set of practices for the management of electronic records and information that meet these requirements.

During the data analysis process, specific terms and concepts are identified in the selected literature. Results are then categorized to reveal related concepts, described and organized as themes for examination and presentation. Thematic organization allows for the examination and review of various perspectives, approaches and methodologies to aid the researcher in an analysis of previous research and study (Wesleyan University Library, 2009). In this case, themes are framed by the set of recordkeeping requirements derived from the GARP® principles.

Themes become the content for development of the final outcome of the study, designed in the form of a guide that summarizes the GARP® related practices for electronic RIM.

The guide is comprised of three components, related to the research questions for the study: (a) an overview of the GARP® principles and the foundational sources used in their development; (b) a listing of the recordkeeping requirements derived from the GARP® principles; and (c) a listing of practices for electronic RIM that meet the GARP® derived requirements. The guide is intended for use by RIM and IT professionals as they work together in pursuit of efficient and compliant electronic records and information management.

Definitions

Many of the terms included in this literature review are unique to the field of records and information management and/or have distinct meaning when used in the context of recordkeeping practices versus other disciplines. These terms include legal terminology, technical terminology, and various terms associated with RIM-specific concepts. Where appropriate, terms are defined within the body of the text when introduced. Sometimes it is not practical to provide these in text definitions, particularly when the term is embedded in quoted or excerpted text from source material. To establish a baseline understanding of these essential terms, this section provides definitions based on academic sources, reference materials and other cited texts. Definitions are recorded verbatim, as much as possible.

Accountability – The principle that individuals, organizations, and the community are responsible for their actions and may be required to explain them to others (ARMA International, 2004, p. 1).

Accuracy – Freedom from error (correctness), or closeness to truth or fact, resulting from exercise of painstaking care or due diligence. Accuracy depends on how the data is collected, and is usually judged by comparing several measurements from the same or different sources (BusinessDictionary.com, 2010a).

American National Standards Institute (ANSI) - The American National Standards Institute (ANSI), oversees the creation, promulgation and use of thousands of norms and guidelines that directly impact businesses in nearly every sector: from acoustical devices to construction equipment, from dairy and livestock production to energy distribution, and many more (American National Standards Institute, n.d., para. 2)

Archiving – (1) To back up electronic records or data to store such information offline yet available for future use.

(2) To conduct all activities related to caring for records of continuing value (ARMA International, 2009e, p.2).

ARMA International – ARMA International (www.arma.org) is a not-for-profit professional association and the authority on managing records and information. Formed in 1955, ARMA International is the oldest and largest association for the information management profession with a current international membership of more than 10,000. It provides education, publications, and information on the efficient maintenance, retrieval, and preservation of vital information created in public and private organizations in all sectors of the economy. It also publishes Information Management magazine, and the Generally Accepted Recordkeeping Principles® (GARP®) (ARMA International, 2010b, para. 4). Originally, ARMA was the acronym for the Association of Records Managers and Administrators. Over the past several years, however, we have seen a broadening of the profession as records management has become a recognized and integral part of information management which is key to doing business. To reflect the changing environment and this "expansion" of the profession, about four years ago the association's Board of Directors decided to discontinue using ARMA as an acronym and adopted "ARMA International" as a general descriptor of the association (ARMA International 2010b, para 1).

Audit – Independent review and examination of records and activities to test for compliance with established policies or standards, often with recommendations for changes in controls (ARMA International, 2009b, p. 2)

Authenticity – One of the four characteristics of a record that demonstrate that the record can be proven: (a) to be what it purports to be, (b) to have been created or sent by the person purported to have created or sent it, and (c) to have been created or sent at the time purported (International Organization for Standardization, 2001a).

Authority – An accepted source of information, advice, etc. (Dictionary.com, 2010)

Availability – Characteristic of a resource that is committable, operable, or usable upon demand to perform its designated or required function (BusinessDictionary.com, 2010b, para.1).

Best practice – Methods and techniques that have consistently shown results superior than those achieved with other means, and which are used as benchmarks to strive for. There is, however, no practice that is best for everyone or in every situation, and no best practice remains best for very long as people keep on finding better ways of doing things (BusinessDictionary.com, 2010c, para.1).

Compliance – …confirmation that the doer of an action (such as the writer of an audit report), or the manufacturer or supplier of a product, meets the requirements of accepted practices, legislation, prescribed rules and regulations, specified standards… (BusinessDictionary.com, 2010d, para. 1).

Consistent – Being in conformity with a set of rules, guidelines or policies (BusinessDictionary.com, 2010e, para. 3)

Data – Groups of characters that represent a specific value or condition. Data provide the building blocks of information (ARMA International, 2005, p. 2)

Destruction – The definitive obliteration of a record, or information, beyond any possible reconstruction (ARMA International, 2009c, p. 2).

Discovery – (1) The process by which lawyers learn about their opponent's case in preparation for trial (ARMA International, 2007d, p. 2).

(2) The required disclosure of relevant items in the possession of one party to the opposing party during the course of legal action (ARMA International, 2009b, p. 3)

Disposition – The actions taken with regard to records as determined through appraisal. Actions might include transfer to storage, destruction, or preservation for archival purposes (ARMA International, 2004, p. 2).

DLM Forum – The DLM Forum was created through an initiative of the European Commission in 1997 with support from the public archives of European Union member states. Until 2002 the DLM Forum was an inter-disciplinary cooperative effort led by the EU member states and the European Commission. Subsequently, the DLM Forum has evolved to become a wider community of interested parties in archive, records, document and information lifecycle management throughout Europe.

From the third triennial conference in Barcelona in 2002 the DLM Forum has been an independent body and attracted members from both the public and private sector. It now includes suppliers, end users, consultants, regulatory bodies and associations. The DLM Forum is well established as an influential European centre, setting standards and guidelines within the disciplines of electronic information archiving and management (DLM Forum, 2009, para. 1-2).

Documentation – An organized set of information that explains the requirements needed to use and maintain a system, or project (ARMA International, 2007b, p 9.)

Encryption – The process of rendering plaintext unintelligible by converting it to ciphertext that can be read only by those with the knowledge to decode the plaintext from the ciphertext (ARMA International, 2007a, p. 3).

Generally Accepted Recordkeeping Principles® (GARP®) – The Generally Accepted Recordkeeping Principles® (GARP®) were created to assist organizations in implementing effective records systems and policies. Together, the eight principles set a standard of conduct and practice deemed by practitioners in the records and information management (RIM) field to represent sound policy and practice (ARMA International, n.d.).

Governance – Establishment of policies and the continuous monitoring of their proper implementation (BusinessDictionary.com, 2010f)

Information – Data that has been given value through analysis, interpretation, or compilation in a meaningful form (ARMA International, 2009c).

Information security – …the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes (International Organization for Standardization, 2010c, para. 4-6).

Information Technology (IT) – The infrastructure, processes, and technologies used to store, generate, manipulate, and transmit information to support an organization (ARMA International, 2009e, p.3).

Integrity – One of the four characteristics of a record that demonstrate that the record is complete and unaltered (International Organization for Standardization, 2001a).

International Organization for Standardization (ISO) – ISO (International Organization for Standardization) is the world's largest developer and publisher of International Standards. ISO is a network of the national standards institutes of 161 countries, one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system. ISO is a non-governmental organization that forms a bridge between the public and private sectors. On the one hand, many of its member institutes are part of the governmental structure of their countries, or are mandated by their government. On the other hand, other members have their roots uniquely in the private sector, having been set up by national partnerships of industry associations. Therefore, ISO enables a consensus to be reached on solutions that meet both the requirements of business and the broader needs of society (International Organization for Standardization, 2010a, para. 1-5). Because *International Organization for Standardization* would have different acronyms in different languages (“IOS" in English, "OIN" in French for *Organisation internationale de normalisation*), its founders decided to give it a short, all-purpose name. They chose ISO, derived from the Greek *isos*, meaning equal. Whatever the country, whatever the language, the short form of the organization's name is always ISO (International Organization for Standardization, 2010b, para. 1).

Keyword – A word or phrase taken from the title or text of a document that characterizes its content and facilitates retrieval (ARMA International, 2009c, p. 4).

Legal hold (also litigation hold) **–** (1) A communication issued as a result of current or anticipated litigation, audit, government investigation, or other such matter that suspends the normal disposition or processing of records (ARMA International 2009b, p.4).

(2) The process for preserving information and records that may be important to resolving a dispute (ARMA International 2007d, p. 3).

Metadata – (1) A characterization or description documenting the identification, management, nature, use or location of information resources (data) (ARMA International, 2007a, p. 3).

(2) Data describing context, content, and structure of records and their management through time (International Organization for Standardization 2001a, p 3).

Migration – The transfer of digital materials from one hardware or software or database structure configuration to another or from one generation of computer technology to another for the purpose of assuring the preservation, usability, and integrity of the data in rapidly changing technology environments (ARMA International, 2007c, p. 3)

Policy – A high-level overall plan, containing a set of principles, embracing the general goals of the organization, and used to base decisions (ARMA International, 2007b, p19).

Practice – Methods, procedures, processes and rules used in a particular field or profession (BusinessDictionary.com, 2010g).

For the purposes of this study, this definition has been merged with the definition for *best practice* to create a stricter definition that defines the term as follows: methods, procedures, processes and rules used in a particular field that have shown superior results.

Practising Law Institute – Practising Law Institute (PLI) is a non-profit continuing legal education organization chartered by the Regents of the University of the State of New York, founded in 1933. PLI is dedicated to providing the legal community and allied professionals with the most up-to-date, relevant information and techniques which are critical to the development of a professional, competitive edge (Practising Law Institute, 2010, para. 1).

Preservation – The processes and operations involved in ensuring the technical and intellectual survival of authentic records through time (International Organization for Standardization, 2006, p. 3).

Privacy – Restriction on searching for or revealing facts that are unknown or unknowable to others (BusinessDictionary.com, 2010h).

Procedure – Instructions, exhibits, and/or other methodologies to follow in order to complete tasks in a predictable and orderly way (ARMA International, 2007b, p 19).

Protection – Ability to guard from attack, loss, harm, etc. (Dictionary.com, 2010).

Records – Information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business (International Organization for Standardization, 2001a, p. 3).

Records and information lifecycle – The span of time from the creation or receipt of records or information, through useful life, to final disposition (ARMA International 2004, p. 2).

Records and Information Management (RIM) (also Records Management or RM) - The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records (International Organization for Standardization, 2001a, p 3).

Reliability – One of the four characteristics of a record that identifies the record as having contents that can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities (International Organization for Standardization, 2001a).

Requirements (also Recordkeeping requirements) – (1) Constraints, demands, necessities, needs, or parameters that must be met or satisfied… (BusinessDictionary.com, 2010h, para. 1).

(2) Statutory or regulatory requirements, or administrative directives, that define obligations for the creation and maintenance of records by an organization (ARMA International, 2007a, p. 4).

For the purposes of this study, these two definitions have been combined and the term is defined as follows: Constraints, demands, necessities, needs, or parameters that must be met or satisfied for the creation and maintenance of records by an organization.

Retention – The period of time records or information must be kept to meet administrative, fiscal, legal or historical requirements (ARMA International, 2009c, p. 4).

Retrieval – The act of accessing information from stored data in a computer system (ARMA International, 2007b, p. 22).

Sarbanes Oxley (SOX) – The Sarbanes-Oxley Act of 2002 (PL 107-204), also known as the *Public Company Accounting and Investor Protection Act of 2002* and referred to as SOX, legislates financial reporting for U.S. public companies (ARMA International, 2009c, p. 5).

Secondary value (of a record) **–** The value of a record for future use versus the current use in an active environment. The term does not imply that the value is less or that the record is unimportant, but simply refers to the additional value(s) the record possesses beyond the reason(s) for its creation (Penn, Pennix & Coulson, 1994).

The Sedona Conference® – The Sedona Conference® is a nonprofit, 501(c)(3) research and education institute dedicated to the advancement of law and policy in the areas of antitrust, complex litigation and intellectual property rights (The Sedona Conference®, 2007, p.106).

Standard – A method, material, or practice developed through consensus by experts in the field, which leads to results that are consistent, predictable, and desirable (ARMA International, 2009c, p. 5).

Transparency – (1)…The availability of full information required for collaboration, cooperation, and collective decision-making (BusinessDictionary.com, 2010j, para. 1). (2) Minimum degree of disclosure to which agreements, dealings, practices, and transactions are open to all for verification (BusinessDictionary.com, 2010j, para. 2). (3) Essential condition for a free and open exchange whereby the rules and reasons behind regulatory measures are fair and clear to all participants (BusinessDictionary.com, 2010j, para. 3).

Usability – One of the four characteristics of a record that demonstrate that the record has the ability to be located, retrieved, presented, and interpreted (International Organization for Standardization, 2001a).

Research Parameters

This section explains the approach that is used to frame the research design of this study and includes the research questions. Results from initial research are used as a basis to guide continued search efforts and in the development of an approach for the evaluation of information sources. The strategy used to determine the credibility and relevance of selected references is described, as is the documentation approach.

Research Questions and Sub-questions

This research effort is guided by a series of research questions, each tied to one of the two stages that organize the data analysis coding process. The first set of questions is designed to extrapolate the recordkeeping requirements outlined by the GARP® principles. Once the recordkeeping requirements are defined, a second series of questions is designed to identify a preliminary set of electronic records and information management practices, in relation to the recordkeeping requirements for each of the GARP® principles.

1. What are the recordkeeping requirements outlined by the GARP® principles?
    a. What are the requirements related to the GARP® *Principle of Accountability*?
    b. What are the requirements related to the GARP® *Principle of Integrity*?
    c. What are the requirements related to the GARP® *Principle of Protection*?
    d. What are the requirements related to the GARP® *Principle of Compliance*?
    e. What are the requirements related to the GARP® *Principle of Availability*?
    f. What are the requirements related to the GARP® *Principle of Retention*?
    g. What are the requirements related to the GARP® *Principle of Disposition*?
    h. What are the requirements related to the GARP® *Principle of Transparency*?

2. What are the electronic records and information practices that meet the requirements extrapolated from the GARP® principles?
    a. What are the practices related to the requirements of the GARP® *Principle of Accountability*?
    b. What are the practices related to the requirements of the GARP® *Principle of Integrity*?
    c. What are the practices related to the requirements of the GARP® *Principle of Protection*?
    d. What are the practices related to the requirements of the GARP® *Principle of Compliance*?
    e. What are the practices related to the requirements of the GARP® *Principle of Availability*?
    f. What are the practices related to the requirements of the GARP® *Principle of Retention*?
    g. What are the practices related to the requirements of the GARP® *Principle of Disposition*?
    h. What are the practices related to the requirements of the GARP® *Principle of Transparency*?

Search Strategy

Though the focus of this study is to identify practices for electronic RIM, relevant information is regularly discussed within the general context of records and information management practices that do not specifically address electronic content. Using the results from initial research, an approach is developed to direct additional searches that include references

that specifically address electronic RIM issues and general RIM practices. The criteria used to evaluate literature sources are also described. Search results and the process used to identify pertinent and related references are then defined.

Search terms. References for the literature review are collected using the search terms below. Search terms are derived from the GARP® principles, the various standards and guidelines used in their development, and from the analysis of literature from this researcher's personal collection of periodicals, standards and texts related to records and information management.

Key search terms.

- Records management
- Best practice
- Electronic information
- Data
- Records
- Electronic records
- Recordkeeping

Subtopic search terms. Subtopic search terms are derived from the text of each of the GARP® principles, and the texts used in their development, and represent the essential concepts, components, and/or requirements that define each principle.

GARP® Principle of Accountability

- Accountability
- Responsibility
- Governance
- Audit
- Authority

GARP® Principle of Protection

- Protection
- Privacy
- Security
- Confidentiality

GARP® Principle of Integrity

- Integrity
- Authenticity
- Reliability
- Media migration
- Consistency
- Quality

GARP® Principle of Compliance

- Compliance
- Legal admissibility
- Data catalog/Data map
- Ethics
- Audit
- Policy/Procedure enforcement

GARP® Principle of Availability

- Availability
- Accuracy
- Retrieval
- Recovery

GARP® Principle of Disposition

- Disposition
- Deletion
- Destruction
- Data migration
- Legal hold

GARP® Principle of Retention

- Retention
- Information life cycle
- Archiving
- Preservation
- Secondary value

GARP® Principle of Transparency

- Transparency
- Documentation
- Compliance
- Audit

Literature resources. Literature resources for review in this study are identified by using the terms detailed above in combination, and are collected using the tools and literature sources outlined below. Literature resources reviewed in this study include: (a) the GARP® principles; (b) published standards and guidelines relating to records and information management; (c) studies and peer reviewed articles addressing electronic records and information management practices; (d) government publications detailing requirements and standards for electronic RIM and the systems that create and maintain them; (e) whitepapers and other articles published by recognized RIM and IT organizations and vendors; and (f) various articles, journal publications and other content sources that provide information, statistics and other contextual information related to this study.

Online indexes/databases. Literature resources for review are collected primarily by using Computer Source due to its focus on current issues and trends in technology and the high number of relevant results.

Search engines. Literature review sources are also collected using Google and Bing search engines. These search engines are most effective for identifying sources used to provide facts, statistics and other relevant information used to support key concepts and related assertions. These search engines are also used to locate articles and whitepapers listed in the bibliographies from texts used in the development of GARP®.

Additional literature resources. The standards and guidelines used in the development of the GARP® principles constitute a significant number of the literature resources reviewed in this study. These resources are not explicitly listed in the GARP® principles or in the various publications addressing GARP®. These standards and guidelines are identified through direct

communication with representatives from the publisher of GARP®, ARMA International, and members of the GARP® committee.

Resources from this researcher's personal collection of periodicals, standards and texts related to records and information management are also reviewed in this study. Bibliographies and references contained in these resources are also used to identify additional resources. The ARMA International website is also used to identify resources addressing or related to GARP®, and for resources related to records and information management.

Selection criteria. To identify practices for the management of electronic records and information that can be developed as a guide, literature selected for this review is chosen from a broad range of sources. Though multiple resources are used, literature is collected primarily from the following two sources: (a) this researcher's personal collection of standards, guidelines, texts, journals and other publications related to the field of records and information management; and (b) keyword searches from online indexes and databases. The majority of online sources are from the Computer Source database. "Computer Source provides researchers with the laterst (sic) information and current trends in high technology…" and, "…offers full text for more than 300 publications and indexing and abstracting for nearly 450 publications" (OneSearch, n.d.).

With the exception of technology independent best practices and standards, sources for this study are primarily limited to the last five years. This is to ensure that the information in this study is relevant to current challenges and reflective of recent events that have raised the importance of electronic records and information management (Stephens, 2009).

After the establishment of the date restrictions, bibliography reviews and keyword searches are conducted and the identified sources are reviewed to determine if the information identified should be included in the study. Source abstracts are reviewed and identified sources

are considered for inclusion based on their relevance to records and information management generally, and to electronic records and information management practices and the recordkeeping requirements extrapolated from the GARP® principles specifically.

Evaluation criteria. Sources that are determined to be relevant to this study are also assessed for credibility. Several factors are used to assess credibility to determine if the identified sources are appropriate for inclusion in this study (Smith, 2009). These factors include the author or publisher's level of knowledge and authority to address the topic (Smith, 2009). Credible authors are those that have relevant credentials including academic degrees in a related field, institutional affiliations, and/or that are frequently cited in related publications (Smith, 2009). Credible publishers include organizations that have a reputation for quality publications, professional organizations that specialize in the subject matter, and/or those that incorporate peer or other review process of the published works (Smith, 2009).

Documentation approach. Literature that is subjected to content analysis is manually coded. A table for each of the GARP® principles is used to tally the frequency of the coded concepts present in the literature.

Table 1 - Sample Coding Table

GARP® Principle of Accountability	**Coded Keywords**	**Article 1**	**Article 2**	**Article 3**
	Accountability			
	Responsibility			
	Governance			
	Audit			
	Authority			

The references selected for use in this study are a mix of electronic sources obtained using searches of the Computer Source database and the World Wide Web and hardcopy texts from this researcher's personal collection of materials related to RIM. Electronic sources are stored using Adobe PDF (Portable Document Format) and are named using the following convention: Author/Publisher Name_date of publication_Title. Each PDF file is saved to a folder named for one of the GARP® principles to which the source is deemed relevant based on the search and coding processes. If the source is relevant to more than one GARP® principle, the file is copied and placed in the folder for each principle to which it relates.

For physical sources, an index card is clipped to the cover of the publication and the following information is recorded on the card: (a) full APA citation and (b) relevant GARP® principle(s) identified through the coding process. If only a portion of the text is used (e.g. a specific chapter, a single article, etc.) the relevant pages are clipped together to facilitate access.

Data Analysis Plan

Data analysis proceeds in two larger stages. Literature selected for the first stage of the data analysis process includes the GARP® principles themselves and the sources used in their development that are identified through direct communications with the author of the GARP® principles, ARMA International, and members of the GARP® development committee. The GARP® principles are broad in scope and general in nature (ARMA International, 2009d) and as a result are not specific to issues relating to electronic RIM. To ensure that the content of the standards and guidelines are relevant to this study, only the portions that are format independent or that address electronic information and records directly are included in the analysis.

The primary goal during the first stage of the data analysis process is to extrapolate a set of requirements for the management of electronic records and information. A secondary goal is

to develop a series of coding terms that relate to the recordkeeping requirements identified. These coding terms are selected as being representative of the recordkeeping requirements identified from the GARP® principles and the sources used in their development. Coding terms are identified as selected keywords that characterize each document's content (ARMA International, 2009c) and represent the components that define requirements.

Requirements are defined as the constraints, demands, necessities, needs, or parameters that must be met or satisfied for the creation and maintenance of records by an organization (see Definitions for more detail). These terms serve as the initial set of coding terms, according to the description of the coding process provided by Busch et al. (2005). Keywords characterizing these recordkeeping requirements and that represent the essential concepts, components, and/or requirements that define each principle are determined for use in the content analysis process of the second stage of this study.

For the second stage of the data analysis, coding for each GARP® principle occurs independently. A total of four to six concepts/keywords are used to code for each principle in an effort to answer the question "What are the practices related to the requirements of the GARP® principle of ____." Literature is coded using the keywords associated with, and the recordkeeping requirements derived from, the GARP® principles in stage one. Coding results are analyzed based on context through the process of proximity analysis as described by Busch et al. (2005). Texts that demonstrate the presence of co-occurring GARP® derived recordkeeping requirements, as represented by the presence of the terms/keywords coded for, are deemed relevant practices for electronic RIM. The goal is to identify texts that address electronic RIM practices through the identification of a strong relationship between the detailed practices and the concept(s) derived from the GARP® principle. Relationships are considered to be strong when

they are closely aligned with one or more of the identified recordkeeping requirements for each principle (Busch, et al, 2005).

Writing Plan

The Writing Plan describes the approach taken to the organization of content derived during data analysis. The approach is thematic, and used to present information in the Review of the Literature and Conclusions sections of this document.

The overall structure of the study is organized around three key concepts: (a) an overview of the GARP® principles and the foundational sources used in their development; (b) a listing of the recordkeeping requirements derived from the GARP® principles; and (c) a review and analysis of various electronic RIM practices viewed through perspective of the identified recordkeeping requirements. The first key concept is used to design the data analysis process. The second and third key concepts define the themes that make up the content in the Review of the Literature.

The first key concept presents an overview of the GARP® principles and the foundational sources used in their development in an effort to provide context for the data analysis process. Results of each stage of the data analysis process are reviewed and organized into themes (Obenzinger, 2005) that mirror the structure of the GARP® principles.

The second key concept presents recordkeeping requirements derived through an analysis of the GARP® principles and the core foundational references used in their development. Recordkeeping requirements are identified through an analysis of each of the GARP® principles. Once identified, these requirements are organized into themes that mirror the structure of the GARP® principles.

The third key concept presents practices for the management of the electronic record and information identified through searches using keywords derived from the GARP® principles. Once identified, these practices are compared to and analyzed in conjunction with the identified recordkeeping requirements derived from GARP®. The goal is to identify electronic RIM practices that meet or achieve the requirements derived from GARP®. In determining if a practice can be deemed as addressing the GARP® derived requirement(s), the researcher determines if there is a strong relationship between the identified practice and the recordkeeping requirements. The identified practices are summarized and the content is presented in the Conclusions section of the paper.

When viewed together, this listing of practices for each of the GARP® principles represents a guide for electronic RIM. Presenting a guide that is based on methods and techniques of the last five years is intended to assist the audience in addressing the current and growing challenges of managing electronic records and information (Saffady, 2009; Stephens, 2009). The goal is to provide these professionals with content-rich support as they work together to become increasingly involved in the management of the information lifecycle at all stages (ARMA International, 2009e).

Annotated Bibliography

The references selected for use in this study are evaluated for relevance, credibility and significance. Texts that are determined to be significant to the development of the GARP® principles and in understanding the recordkeeping requirements extrapolated from the principles are presented in this section of the document (Obenzinger, 2005). This section also includes the texts that detail practices that, through the data analysis process outlined by Busch et al. (2005), meet the requirements derived from GARP® and meet the stricter definition of practice used for this study. This annotated bibliography lists 35 entries. Each entry includes the complete citation, the published abstract or summary of the reference, an assessment of its relevance to this study and a determination of its credibility. The credibility of a number of these references is, in part, supported through personal communication with ARMA International President-elect and GARP® committee member Galina Datskovsky, Ph.D., CRM and GARP® committee member Lenore Greenburg, CRM.

The following set of references pertains to the GARP® principles and the core standards and guidelines used in their development. References include the set of literature subjected to coding during the first stage of conceptual analysis.

ARMA International. (2009d). ***The generally accepted recordkeeping principles® (GARP®)*** **[full version]. Retrieved March 30, 2010, from http://www.arma.org/garp/garp.pdf**

Abstract. Records are the foundation of compliance and the key to success for organizations – big or small, public or private – in any industry. Litigation professionals, too, are becoming painfully aware of the need to manage e-mail at an organizational level in order to mitigate risk during the legal discovery process. Businesses are also coming to

realize greater efficiency and cost savings due to better information management. As a result, recordkeeping practices have become a process and skill needed by not only records professionals, but by every employee.

Due to the exponentially expanding volume of information available and the pressing need to manage information correctly, ARMA International is pleased to announce a set of Generally Accepted Recordkeeping Principles®.

Through these principles, ARMA International provides a framework for guidance in implementing information management programs to help business leaders, legislators, the judiciary, and other stakeholders understand and address the key components of records and information management as a discipline and as a best business practice. The principles were developed from related information management legislation, the combined experiences of the task force members, applicable ARMA International, ANSI, and ISO standards, the recommendations of ARMA International's more than 11,000 professional practitioners, and case law.

Each of the eight principles has an expanded description containing detailed information on how to ensure organizations are meeting the criteria for a sound information management program.

Comments. This article outlines the key complements (principles) necessary for effective, complete, and compliant RIM programs. Though not specific to electronic RIM, it is the foundational reference for this research. This article is considered credible because ARMA International, recognized as the leading professional organization that addresses records and information management issues, publishes it.

ARMA International. (2010a). ***ARMA International maturity for information governance*** **[GARP® Maturity Model]. Retrieved May 15, 2010 from http://www.arma.org/garp/Garp%20maturity%20Model.pdf**

Abstract. The Maturity Model for Information Governance begins to paint a more complete picture of what effective information governance looks like. It is based on the eight GARP® principles as well as a foundation of standards, best practices, and legal/regulatory requirements. The maturity model goes beyond a mere statement of the principles by beginning to define characteristics of various levels of recordkeeping programs. For each principle, the maturity model associates various characteristics that are typical for each of the five levels defined in the model.

Comments. This article defines the characteristics of the GARP® principles by describing how they are represented/realized at various levels of recordkeeping programs. Though not specific to electronic RIM, it is a corollary reference developed from the foundational reference for this research: the GARP® principles. This article is considered credible because ARMA International, recognized as the leading professional organization that addresses records and information management issues, publishes it and because of its relation to the GARP® principles.

ARMA International. (2010c) ***Course notes: Generally accepted recordkeeping principles®: Overview*** **[Online course handouts]. Retrieved May 25, 2010 from http://www.courses.learnsomething.com/scormcourses/o5642c9adab5b4668a3e5d59ba5bbdf18/p62ab316db617435e999f6e420a7bc86d/data/resources/GARP%20Course%20Notes%5fFinal%5f2010%2d4%2d30%2epdf?download=true**

Abstract. This online overview course focuses on the importance of each GARP® principle and how you can integrate each into your RIM program. The course will also provide you vital facts that you can take back to executive-level managers, who may be unfamiliar with the benefits of RIM, but need to be familiar with GARP ® and the benefits to your organization - as well as the perils of ignoring them. You will learn why the principles are a standard of excellence for records systems and why your organization should regard GARP ® compliance as a holistic organizational imperative – and a mandate for better information governance.

Comments. This online course and companion handout examines each of the GARP® principles in detail. This reference is considered credible because ARMA International, recognized as the leading professional organization that addresses records and information management issues, produces and publishes it.

DLM Forum. (2008a). ***MoReq2: Model requirements for the management of electronic records, v1.04*****. Retrieved May 15, 2010 from http://www.dlmforum.eu/index.php?option=com_jotloader&view=categories&cid=10_f56391a0c9ea9456bf24e80b514f5dda&Itemid=36&lang=en**

Abstract. The MoReq specification describes model requirements for the management of electronic records and focuses mainly on functional requirements for electronic records management systems (ERMS). MoReq contains a model of how filing plans, files and records relate to each other within the context of a classification scheme, and, very importantly, it can be applicable to both electronic (digital), physical (paper), and hybrid files.

Comments. This standard is included because it is considered to be one of the most influential of the GARP® foundational references (L. Greenberg, personal communication, May 12, 2010; G. Datskovsky, personal communication, May 13, 2010) It outlines essential elements of an ERMS to ensure that records are properly managed, can be accessed at all times, are retained for an appropriate period of time, and are properly disposed of. This standard is considered credible because it is one of the reference documents for the GARP® principles, is published by the DLM Forum which was formed by the EU specifically to address information management lifecycle issues throughout Europe (DLM Forum, 2009), is a recognized standard concerning the management of electronic records and information, is frequently referenced by other electronic RIM standards and guidelines, and is based on prior and recognized standards concerning the management of records and information.

DLM Forum. (2008b). ***MoReq2: Model requirements for the management of electronic records, v1.04 Appendix 9 – Metadata model*****. Retrieved May 15, 2010 from http://www.dlmforum.eu/index.php?option=com_jotloader&view=categories&cid=10_f56391a0c9ea9456bf24e80b514f5dda&Itemid=36&lang=en**

Abstract. This document is appendix 9, the metadata model, of MoReq2. It is published separately from the rest of MoReq2 because of its length and to facilitate use. It is published at http://dlm-network.org/moreq2 . This appendix describes the MoReq2 metadata model. It is significantly different from the model in MoReq. Accordingly there is no cross-reference between the two models.

Due to its focus on records, the metadata model does not include metadata for documents that are not considered records. Metadata for documents can easily be added to this model, preferably by using the records metadata as a basis and supplementing it with document-specific elements (in particular those related to version control and checkout/check in). The metadata model is described in terms of a minimum set of metadata "elements." These "elements" are those that the ERMS must be able to export, import, and process. An "element", referred to as "field" in the past, is the variable used to hold a metadata "value". Examples of metadata elements and values are shown below.

Comments. This standard is included because it is an addition/revision to a standard considered to be one of the most influential of the GARP® foundational references (L. Greenberg, personal communication, May 12, 2010; G. Datskovsky, personal communication, May 13, 2010). It defines the metadata requirements needed for the effective management of electronic records throughout the information lifecycle. This standard is considered credible because it is one of the reference documents for the

GARP® principles, is published by the DLM Forum which was formed by the EU specifically to address information management lifecycle issues throughout Europe (DLM Forum, 2009), is a recognized standard concerning the management of electronic records and information, and is frequently referenced by other electronic RIM standards and guidelines.

International Organization for Standardization. (2001a). ***Information and documentation – Records management part 1: General (ISO 15489-1)*****. Geneva: ISO.**

Abstract. Based on the Australian Standard AS 4390, *Records Management*, this ISO standard was developed to standardize international best practice in records management. It provides guidance on managing records of originating organizations, (public or private, for internal and external clients) to ensure that adequate records – in all formats and media – are created, captured, and managed. This standard also provides guidance on determining organizational responsibilities for records and records policies, procedures, systems, and processes supporting a quality process framework to comply with ISO 9001 and ISO 14001 designing and implementing a records system (but not the management of archival records within archival institutions). Procedures that help to ensure the management of records according to the principles and elements outlined in this part of ISO 15489 are provided in ISO/TR 15489-2 Information and Documentation — Records Management —Part 2: Guidelines.

Comments. This standard is included because it is considered to be one of the most influential of the GARP® foundational references (L. Greenberg, personal communication, May 12, 2010; G. Datskovsky, personal communication, May 13, 2010). It is considered credible because it is one of the reference documents for the GARP®

principles, is published by the International Organization for Standardization, a leading international standards organization, and is based on prior and recognized standards concerning the management of records and information.

International Organization for Standardization. (2001b). ***Information and documentation – Records management part 2: Guidelines (ISO/TR 15489-2)*****. Geneva: ISO.**

Abstract. The international records management standard, ISO 15489-1, specifies the elements of records management and defines the necessary results or outcomes to be achieved. This technical report, ISO/TR 15489-2, is supplementary to the standard, providing further explanation and one methodology for implementation of the standard. Both ISO 15489-1 and this technical report apply to records in any format or media, created or received by any public or private organization during the course of its activities. For records management, this technical report addresses: (1) policies and responsibilities, (2) strategies, design, and implementation (3) processes and controls, (4) monitoring and auditing, and (5) training.

Comments. This standard is included because it is considered to be one of the most influential of the GARP® foundational references (L. Greenberg, personal communication, May 12, 2010; G. Datskovsky, personal communication, May 13, 2010). It is considered credible because it is one of the reference documents for the GARP® principles, is published by the International Organization for Standardization, a leading international standards organization, and is based on prior and recognized standards concerning the management of records and information.

The Sedona Conference®. (2007, March*). Best practices commentary on the use of search & information retrieval methods in e-discovery.* Retrieved May 28, 2010 from http://www.thesedonaconference.org/content/miscFiles/publications_html

Abstract. The goal of this Best Practices Commentary is to provide the bench and bar with an educational guide to an area of e-discovery law that we believe will only become more important over time, given the need to accurately and efficiently search for relevant evidence contained within the exponentially increasing volumes of electronically stored information (ESI) that are stored and made subject to litigation, investigations, and regulatory activities. We also understand that the subject of what constitutes best practices in this area will necessarily be subject to change, given the accelerating pace of technological developments that the law is struggling to keep up with.

Comments. This commentary is included because it is considered to be an excellent summary of one of the major influences on the development of GARP® (G. Datskovsky, personal communication, May 13, 2010). This text addresses several challenges with the discovery of electronic records and information. Much of the commentary provides practical solutions and considerations for electronic discovery. This text is deemed credible because it is published by The Sedona Conference® recognized as a leading research and educational organization that focuses on complex litigation issues (The Sedona Conference®, 2005, p.106), some members of the GARP® committee are also members of The Sedona Conference®, and because related subject matter experts were consulted during the development of GARP® (G. Datskovsky, personal communication, May 13, 2010).

The Sedona Conference®. (2007, November). ***The Sedona guidelines: Best practice guidelines & commentary for managing information & records in the electronic age, Second edition*****. Retrieved May 8, 2010 from http://www.thesedonaconference.org/content/miscFiles/publications_html**

Abstract. A companion piece to The Sedona Principles on Electronic Document Production, this article suggests basic guidelines, commentary, and illustrations to help organizations develop sound and defensible processes to manage electronic information and records.

Comments. This commentary is included because it is considered to be an excellent summary of one of the major influences on the development of GARP® (G. Datskovsky, personal communication, May 13, 2010). This text addresses several challenges with the creation and management of electronic records and information, predominately from a legal perspective. Much of the commentary provides practical solutions and considerations for electronic RIM. This text is deemed credible because it is published by The Sedona Conference® recognized as a leading research and educational organization that focuses on complex litigation issues (The Sedona Conference®, 2005, p.106), some members of the GARP® committee are also members of The Sedona Conference®, and because related subject matter experts were consulted during the development of GARP® (G. Datskovsky, personal communication, May 13, 2010).

The Sedona Conference®. (2008, March). ***Commentary on ESI evidence & admissibility.***

Retrieved May 28, 2010 from

http://www.thesedonaconference.org/content/miscFiles/publications_html

Abstract. During the last decade, culminating with the adoption of significant amendments to the Federal Rules of Civil Procedure (FRCP) on December 1, 2006, the legal community has expended significant energy and focus on electronic data. A main focus has been on whether and under what circumstances a litigant must provide such data – known more formally as electronically stored information or "ESI" – to an adverse party. While there are still significant issues to resolve with the amended FRCP and electronic discovery, the legal community is also grappling with whether and how ESI, once produced, can actually be authenticated and used as evidence at trial or in motion practice. This commentary focuses specifically on that concern, and is divided into three parts: Part I is a brief survey of the applicability and application of existing evidentiary rules and case law addressing the same. Part II addresses new issues and pitfalls that are looming on the horizon. Part III provides practical guidance on the use of ESI in depositions and in court.

Comments. This commentary is included because it is considered to be an excellent summary of one of the major influences on the development of GARP® (G. Datskovsky, personal communication, May 13, 2010). This text addresses several challenges with the creation and management of electronic records and information, predominately from a legal perspective. Much of the commentary provides practical solutions and considerations for electronic RIM. This text is deemed credible because it is published by The Sedona Conference® recognized as a leading research and educational organization

that focuses on complex litigation issues (The Sedona Conference®, 2005, p.106), some members of the GARP® committee are also members of The Sedona Conference®, and because related subject matter experts were consulted during the development of GARP® (G. Datskovsky, personal communication, May 13, 2010).

The Sedona Conference®. (2009, May). ***Commentary achieving quality in the e-discovery process.*** **Retrieved May 28, 2010 from http://www.thesedonaconference.org/content/miscFiles/publications_html**

Abstract. Commentary recognizes that the exponentially increasing volume of electronically stored information (ESI) that is stored and made subject to litigation, investigations, and regulatory activities, necessitates fundamental changes in thinking and practice on the part of the legal profession. As outlined here, these include greater reliance on automated methods in gauging the quality of document productions, including the use of sampling and other forms of measurement, as well as greater attention paid to project management of the e-discovery process. This Commentary is intended to be read in conjunction with *The Sedona Conference Commentary on the Use of Search and Information Retrieval Methods in E-Discovery* (2007).

Comments. This commentary is included because it is considered to be an excellent summary of one of the major influences on the development of GARP® (G. Datskovsky, personal communication, May 13, 2010). This text addresses several challenges with the creation and management of electronic records and information, predominately from a legal perspective. Much of the commentary provides practical solutions and considerations for electronic RIM. This text is deemed credible because it is published by The Sedona Conference® recognized as a leading research and educational organization

that focuses on complex litigation issues (The Sedona Conference®, 2005, p.106), some members of the GARP® committee are also members of The Sedona Conference®, and because related subject matter experts were consulted during the development of GARP® (G. Datskovsky, personal communication, May 13, 2010).

U.S. Department of Defense. (2007). ***DoD5015.2-STD, Electronic records management software applications design criteria standard*****. Retrieved March 31, 2010 from http://jitc.fhu.disa.mil/recmgt/p50152stdapr07.pdf**

Abstract. This Standard is reissued under the authority of DoD Directive 5015.2, "Department of Defense Records Management Program," March 6, 2000, (Reference (a)) which provides implementing and procedural guidance on the management of records in the Department of Defense. It sets forth mandatory baseline functional requirements for Records Management Application (RMA) software used by the DoD Components in implementing their records management programs; defines required system interfaces and search criteria that RMAs shall support; and describes the minimum records management requirements that must be met based on current National Archives and Records Administration (NARA) regulations.

Comments. This standard is included because it is considered to be one of the most influential of the GARP® foundational references (L. Greenberg, personal communication, May 12, 2010; G. Datskovsky, personal communication, May 13, 2010). It details the requirements necessary to effectively manage records and information in all stages of the information lifecycle and includes several technical requirements. This standard is considered credible because it is one of the reference documents for the GARP® principles, because it is considered by many in the RIM profession to be the de

facto standard for the design and creation of electronic RIM applications and systems, and because it is frequently referenced and listed in the bibliographies of publications addressing electronic RIM.

The following set of references addresses practices for electronic records and information management. References comprise the set of literature subjected to coding during the second stage of conceptual analysis.

Adam, A. (2008). ***Implementing electronic document and record management systems*****. New York, NY: Auerbach Publications.**

Abstract. The global shift toward delivering services online requires organizations to evolve from using traditional paper files and storage to more modern electronic methods. Implementing Electronic Document and Record Management Systems explains how to efficiently store and access electronic documents and records in a manner that allows quick and efficient access to information so an organization may meet the needs of its clients. The book addresses a host of issues related to electronic document and records management systems (EDRMS). From starting the project to systems administration, it details every aspect in relation to implementation and management processes. It offers case studies that examine how various organizations across the globe have implemented EDRMS.

Comments. This reference is deemed relevant because it addresses several of the key issues related to the GARP® principles, is specific to electronic recordkeeping, reviews techniques and practices including technical details, and provides case studies related to electronic RIM. This reference is deemed credible because it is extensively cited and

incorporates and builds off of several recognized standards including: ISO 15489, DoD 5015.2, MoReq/MoReq2.

Adler, G., Howard, G. & Lona, M. (Eds.). (2007, October). ***Electronic discovery and retention guidance for corporate counsel 2007.*** **New York, NY: Practising Law Institute.**

Abstract. This course handbook is one of about 200 published each year by the Practising Law Institute and serves as a supplement and reference to the continuing legal education seminar of the same name. This edition addresses the status of e-discovery law, various aspects of the e-discovery process, and reviews retention requirements for electronically stored information (ESI).

Comments. This reference is deemed relevant because it reviews the impact of e-discovery issues on electronic records and information management practices, reviews various retention requirements and issues for ESI, and details requirements for ESI before, during and after the litigation process. This reference is deemed credible because the editors are regular speakers about the e-discovery process, have been published in various legal and professional journals, and work for/represent some of the largest and most respected law firms working on e-discovery issues (Adler et al. 2007). The reference and educational seminar with which it is associated are produced by Practising Law Institute, a non-profit legal education organization charted by the Regents of the University of the State of New York (Practising Law Institute, 2010).

Adler, G., Howard, G. & Lona, M. (Eds.). (2009, October). ***Electronic discovery guidance 2009: What corporate and outside counsel need to know.*** **New York, NY: Practising Law Institute.**

Abstract. This course handbook is one of about 200 published each year by the Practising Law Institute and serves as a supplement and reference to the continuing legal education seminar of the same name. This edition addresses the status of e-discovery law and various aspects of the e-discovery process including the collection, review and admissibility of electronically stored information (ESI).

Comments. This reference is deemed relevant because it reviews the impact of e-discovery issues on electronic records and information management practices and details requirements for electronic information issues before, during and after the litigation process. This reference is deemed credible because the editors are regular speakers about the e-discovery process, have been published in various legal and professional journals, and work for/represent some of the largest and most respected law firms working on e-discovery issues (Adler et al. 2009). The reference and educational seminar with which it is associated are produced by Practising Law Institute, a non-profit legal education organization charted by the Regents of the University of the State of New York (Practising Law Institute, 2010).

ARMA International. (2007a). ***The digital records conversion process: Program planning, requirements, procedures (ANSI/ARMA 16-2007)*****. Lenexa, KS: ARMA International.**

Abstract. This American National Standard provides requirements for ensuring that electronic records remain authentic and trustworthy as they are converted from one digital recordkeeping system to another. Though it does not address digital preservation,

there is a substantial link between conversion and digital preservation, as many preservation strategies involve some type of conversion process. Part I of the standard addresses the decisions relating to program planning and recordkeeping issues. Part II discusses the actual conversion process. Appended are tables, a template that draws together recordkeeping requirements, the risks/drivers impinging on the conversion process, the controls, the stages of the conversion process, and tools designed to aid records professionals and others assigned the conversion task. Using this American National Standard in conjunction with the international standard *ISO 14721:2003, Space data and information transfer systems – Open archival information system – Reference model* will provide additional background and contextual information.

Comments. This article addresses key concerns and establishes requirements for data migrations to ensure record integrity, usability, and accessibility. This article is considered credible because it is authorized by the American National Standards Institute (ANSI), and is published by ARMA International, recognized as the leading professional organization that addresses records and information management issues.

ARMA International. (2009e). *Records and information management for information technology professionals*. Lenexa, KS: ARMA International.

Abstract. A variety of business drivers, including electronic commerce, emerging technologies, and privacy and security requirements, are compelling records and information management (RIM) and information technology (IT) professionals to collaborate to create cohesive information management solutions.

Consequently, RIM professionals need to extend their IT knowledge, and IT professionals need a clear understanding of records retention and archiving

requirements and methodologies. This guideline, which focuses on key records processes that are relevant in managing information through the use of information technologies, will help both groups gain a better awareness of RIM and IT roles and responsibilities.

Comments. This article translates key records concepts, practices and requirements into language and terminology accessible to non-RIM professionals (specifically IT professionals). It is useful for the identification of terms, techniques and approaches associated with RIM and electronic recordkeeping. This reference is considered credible because it is published by ARMA International, recognized as the leading professional organization that addresses records and information management issues.

ARMA International. (2009f). ***Using DoD 5015.2-STD outside the federal government sector.*** **Lenexa, KS: ARMA International.**

Abstract. DoD 5015.2-STD *Design Criteria Standard for Electronic Records Management Software Applications* specifies hundreds of requirements that electronic records management (ERM) products must be certified against if they are to be acquired by Department of Defense (DoD) organizations. It has also become a vehicle for granting a de facto seal of approval that signals that an ERM product provides the tools necessary to manage electronic (as well as paper-based) information effectively.

Comments. This reference is deemed relevant because it reviews the applicability of a significant government standard for electronic RIM issues to the private sector. DoD5015.2 is considered to be a de facto standard by many and this text reviews implementation related information, reviews the detailed requirements of DoD5015.2 and

identifies gaps in the standard for further exploration. This reference is considered credible because it is based on DoD5015.2 and is published by ARMA International, the leading professional organization that addresses records and information management issues.

Brown, P. (Ed.). (2007, March). ***Information technology law institute: Systems security, record retention and the rise of information life cycle management.*** **New York, NY: Practising Law Institute.**

Abstract. This course handbook is one of about 200 published each year by the Practising Law Institute and serves as a supplement and reference to the continuing legal education seminar of the same name. This edition addresses the status of information security, related laws and various aspects of record retention and information life cycle management practices as they relate to information technology law.

Comments. This reference is deemed relevant because it reviews the legal importance of information security and record retention practices for electronic records to ensure compliance with various laws and regulations, as well as to ensure the admissibility, security and integrity of the electronic records. This reference is deemed credible because the editor is a regular speaker about the legal aspects of information security practices and compliance, serves on the board of directors for the International Technology Law Association, served as an adjunct professor of computer law at Dartmouth College, co-authored two books on law and technology subjects, and writes a monthly column for the *New York Law Journal* (Brown, 2007). The reference and educational seminar with which it is associated are produced by Practising Law Institute,

a non-profit legal education organization charted by the Regents of the University of State of New York (Practising Law Institute, 2010).

Burns, R. & Peterson, Z. (2010). Security constructs for regulatory-compliant storage. ***Communications of the ACM, 53(1),*** **126-130. Retrieved April 1, 2010, from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=buh&AN=47220623&loginpage=Login.asp&site=ehost-live&scope=site.**

Abstract. The article discusses methods for making electronic records more resistant to tampering or falsification, thus enhancing their evidentiary value in terms of regulatory compliance. An overview of three technological methods is presented: secure-digital audit trails, secure deletion, and authenticated encryption. Some of the technical details are discussed for each of these approaches, along with commentary on suitable circumstances for their use.

Comments. This reference is deemed relevant because it addresses several of the key issues related to the GARP® principles and reviews the related techniques and practices including technical details. The reference is considered credible because *Communications of the ACM* is a peer reviewed academic journal and the official publication of ACM, Inc. (Association of Computing Machinery), an educational and scientific society uniting the world's computing educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges (ACM, Inc., 2010)

Determann, L. & Hwang, J.D. (2009). Data security requirements evolve: From reasonableness to specifics. *Computer & Internet Lawyer, 26(9),* 6-17. Retrieved April 1, 2010, from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=buh&AN=43819063&loginpage=Login.asp&site=ehost-live&scope=site

Abstract. The article discusses various data privacy and security laws in government agencies and companies in the U.S. It cites the Health Insurance Portability and Accountability Act (HIPAA), which applies to health care companies and the Gramm-Leach-Bliley Financial Services Modernization Act for financial services providers. It highlights the requirements for industry groups to implement data security standards and sanctions for companies which will not comply.

Comments. This reference is deemed relevant because it addresses concepts and practices related to the GARP® principles of integrity, protection and compliance. The reference is considered credible because *Computer & Internet Lawyer* is a peer reviewed academic journal focusing on legal and IT issues.

Doyle, J., Viktor, H., & Paquet, E. (2009). Long-term digital preservation: Preserving authenticity and usability of 3-D data. *International journal on digital libraries, 10(1),* 33-47. Retrieved May 16, 2010 from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=cph&AN=38608860&loginpage=login.asp&site=ehost-live&scope=site

Abstract. Long-term digital preservation, the process of maintaining digital objects through time to ensure continued access, has become a crucial issue in recent years. Whilst the amount of digitised information is constantly increasing, so too is the pace of

progress in information technology, resulting in obsolescence of the software and hardware required to access and view digital information. Despite many organisations recognising this threat and the resulting need for preservation action, more work is required to effectively address the issue. We present in this article a framework for the long-term digital preservation of 3-D data. This framework is based on two pertinent preservation practices, emulation and metadata which ensure that the authenticity and usability, respectively, of a preserved digital object remain intact through time. An evaluation of our framework is presented which illustrates the viability of our approach in retaining accessibility, authenticity and usability for future end users.

Comments. This reference is deemed relevant because it addresses several of the key issues related to the GARP® principles and reviews the related techniques and practices. The reference is deemed credible because it is published in the *International Journal on Digital Libraries*, a peer reviewed academic journal.

Hayden, L. (2009, November). Designing common control frameworks: A model for evaluating information technology governance, risk and compliance control rationalization strategies. *Information security journal: A global perspective, 18(6)* 297-305. Retrieved May 16, 2010 from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=cph&AN=49232884&loginpage=login.asp&site=ehost-live&scope=site

Abstract. Information security professionals are faced with increasing compliance obligations associated with laws, regulations, and industry standards. Meeting multiple control framework requirements separately can be costly and inefficient due to similarities between various frameworks that produce redundancy duplication of effort in

the organization's compliance initiatives. To mitigate these inefficiencies many organizations are seeking to streamline and rationalize frameworks in ways that combine overlapping control objectives into a smaller set of controls that still meet the requirements of all frameworks included. This article discusses strategies for such rationalizations, including the benefits and limits of specific strategies.

Comments. This reference is deemed relevant because it addresses several of the key issues addressed in the GARP® principles and establishes a framework for the implementation of related practices. This reference is deemed credible because it is excerpted from the official journal of (ISC)^2; the International Information Systems Security Certification Consortium, Inc. (ISC)^2 is an educational organization that provides certification in a variety of information security disciplines ((ISC)^2, 2010).

Kahn, R. & Blair, B. (2005). ***Information nation warrior: Information management compliance boot camp*****. Silver Spring, MD: AIIM.**

Abstract. The call for greater corporate accountability and transparency continues unabated across the globe, as legal, compliance and privacy issues continue to develop and corporate fears are realized time and again. Companies without the foresight to manage their information properly are finding themselves beleaguered by tech-savvy prosecutors, regulators, and investigators who increasingly look to digital information to find a smoking gun. Aside from the legal and regulatory impact of information mismanagement, many organizations struggle to corral and manage their information assets for business purposes and suffer the consequences in the form of inefficient systems and wasted resources. *Information Nation Warrior: Information Management Compliance Boot Camp* takes you to the frontlines with a practical and comprehensive

approach that is required reading for anyone who plays a role in managing their organization's most valuable asset – its information. As the practical follow-on book to Randolph A. Kahn's and Barclay T. Blair's *Information Nation: The Seven Keys to Information Management Compliance, Warrior* provides the template for a comprehensive, hands-on approach for dealing with enterprise information and compliance issues.

Comments. This reference is deemed relevant because it addresses several of the key issues addressed in the GARP® principles, specifically addressing issues relating to the principles of accountability, transparency and compliance. The text presents a template and procedures for implementing a process addressing these issues. The reference is deemed credible because the authors are frequent speakers and presenters on these issues, including presentations for ARMA International, and have written several texts on various issues related to electronic RIM (Kahn, R. & Blair, B., 2009).

Kahn, R. & Blair, B. (2009). ***Information nation: Seven keys to information management compliance, second edition*****. Indianapolis, IN: Wiley Publishing Inc.**

Abstract. This fully updated edition demonstrates how businesses can succeed in creating a new culture of information management compliance (IMC) by incorporating an IMC philosophy into a corporate governance structure. Expert advice and insight reveals the proven methodology that adopts the principles, controls, and discipline upon which many corporate compliance programs are built and explains how to apply this methodology to develop and implement IMC programs that anticipate problems and take advantage of opportunities. Plus, you'll learn how to measure information management compliance through the use of auditing and monitoring, following the proper delegation

of program roles and components, and creating a culture of information management awareness.

Comments. This text is relevant because it addresses several of the key issues addressed in the GARP® principles, specifically addressing issues relating to the principles of accountability, transparency and compliance. The text presents a methodology for addressing these issues and an overview of the requirements for their implementation. The text is deemed credible because the authors are frequent speakers and presenters on these issues, including presentations for ARMA International, and have written several texts on various issues related to electronic RIM (Kahn, R. & Blair, B., 2009).

Kamel, I. (2009). A schema for protecting the integrity of databases. *Computers & Security, 28(7),* 698-709. Retrieved April 1, 2010, from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=cph&AN=44469643&loginpage=login.asp&site=ehost-live&scope=site

Abstract. Unauthorized changes to databases can result in significant losses for organizations as well as individuals. Watermarking can be used to protect the integrity of databases against unauthorized alterations. Prior work focused on watermarking database tables or relations. Malicious alteration cannot be detected in all cases. In this paper we argue that watermarking database indexes in addition to the database tables would improve the detection of unauthorized alterations. Usually, each database table in commercial applications has more than one index attached to it. Thus, watermarking the database table and all its indexes improve the likelihood of detecting malicious attacks. In general, watermarking different indexes like R-trees, B-trees, Hashes, require different watermarking techniques and exploit different redundancies in the underlying data

structure. This diversity in watermarking techniques contributes to the overall integrity of the databases.

Comments. This article is deemed relevant because it directly addresses issues associated with the GARP® *Principle of Integrity* for electronically managed information and proposes solutions and techniques for resolving these issues. The reference is considered credible because *Computers & Security* is a peer reviewed academic journal.

Moreau, L., Groth, P., Miles, S., Vazquez-Salceda, J., Ibbotson, J., Jiang, S., Munroe, S., Rana, O., Schreibner, A. Tan, V., & Varga, L. (2008). The provenance of electronic data. *Communications of the ACM, 51(4)*, 52-58. Retrieved April 1, 2010, from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=buh&AN=31663006&loginpage=Login.asp&site=ehost-live&scope=site

Abstract. The article focuses on electronic data's provenance. Applications' electronic data of users must be accompanied with its provenance, which describes the process documentation that resulted in its production. The authors propose an open approach wherein applications record their execution in an open data model that can be used to operate provenance queries based on users' needs. Moreover, it allows the documentation of complex applications that involve multiple technologies, including monolithic executables, and others.

Comments. This article is deemed relevant because it deals with data provenance, an issue related to several of the GARP® principles, and because it reviews methods and techniques that can be used in achieving data provenance. The reference is considered credible because *Communications of the ACM* is a peer reviewed academic journal and the official publication of ACM, Inc. (Association of Computing Machinery), an

educational and scientific society uniting the world's computing educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges (ACM, Inc., 2010).

Padayachee, K. & Eloff, J.H.P. (2009). Adapting usage control as a deterrent to address the inadequacies of access controls. *Computers & Security*, *28(7)*, 536-544. Retrieved April 1, 2010, from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=cph&AN=44469629&loginpage=login.asp&site=ehost-live&scope=site

Abstract. Access controls are difficult to implement and evidently deficient under certain conditions. Traditional controls offer no protection for unclassified information, such as a telephone list of employees that is unrestricted, yet available only to members of the company. On the opposing side of the continuum, organizations such as hospitals that manage highly sensitive information require stricter access control measures. Yet, traditional access control may well have inadvertent consequences in such a context. Often, in unpredictable circumstances, users that are denied access could have prevented a calamity had they been allowed access. It has been proposed that controls such as auditing and accountability policies be enforced to deter rather than prevent unauthorized usage. In dynamic environments preconfigured access control policies may change dramatically depending on the context. Moreover, the cost of implementing and maintaining complex preconfigured access control policies sometimes far outweighs the benefits. This paper considers an adaptation of usage control as a proactive means of deterrence control to protect information that cannot be adequately or reasonably protected by access control.

Comments. This article is deemed relevant because it deals with issues related to several of the GARP® principles and reviews and proposes procedures and techniques for addressing them. The reference is considered credible because *Computers & Security* is a peer reviewed academic journal.

Saffady, W. (2009). *Managing electronic records, 4th Edition.* Lenexa, KS: ARMA International.

Abstract. The fourth edition of this best-selling classic provides a comprehensive discussion of records management concepts and methods as they apply to electronic records. It is intended for anyone with responsibilities for creating, maintaining, managing, controlling, and using electronic records created by computer, audio, and video systems. The treatment is practical rather than theoretical. On completion of the book, the reader should understand: The special records management issues and problems associated with electronic records; Principles and procedures for inventory electronic records and for determining how long they need to be retained to satisfy legal and operational requirements; Factors that influence the stability and durability of electronic records; Methods of protecting vital records against damage and destruction; Guidelines for the daily management of electronic records as working information resources.

Comments. This reference identifies many of the key concerns with the creation and management of electronic records and information. It establishes several of the key technology independent requirements and discusses strategies for implementation and management structures. This reference is considered credible because the author is a recognized expert in RIM; the text is heavily referenced, is included as a reference in

multiple bibliographies, and is published by ARMA International, the leading professional organization that addresses records and information management issues.

Scholz, J. (2009). Securing critical IT infrastructure. ***Information security journal: A global Perspective, 18(1),*** **33-39. Retrieved May 16, 2010 from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=cph&AN=36353501&loginpage=login.asp&site=ehost-live&scope=site**

Abstract. By now most everyone has some form of a plan in place for the security of their infrastructure. Unfortunately, the plan may not be complete, omit critical processes, or is based on someone's idea of what is acceptable. Regardless of what is incorporated into the infrastructure, the plan hopefully includes a systemic and methodical process of beginning, maintaining, and changing throughout the lifecycle. No matter how you are structured, you must have management buy in or you have nothing! Although most "security professionals" have either just begun, are in an intermediate stage, or have years of experience with the common bodies of knowledge (CBK), most forget the basics or are unable to incorporate them due to client misunderstanding of them or the process of developing a secure infrastructure. Information Technology Infrastructure Library (ITIL) took the industry standards of business and built the processes to follow to build a structured environment. When you evaluate the requirements of ITIL and then evaluate what the National Institute of Standards and Technology (NIST) have developed over the years, in conjunction with the Rainbow Series, you have it all. NIST takes you a little further because they build the infrastructure from a secure foundation, whereas ITIL relates two paragraphs to the discipline. A secure environment starts with your foundation of security; every process thereafter falls into place as you develop your

baseline security requirements (BLSR). Asset Management, Configuration Management, Change Management, Incident Management, Capacity Management, and Financial Management become a by-product of your foundation.

Comments. This reference is considered relevant because it addresses issues of information security and applies standards and practices from nationally recognized standards organizations (ITIL and NIST) to develop a process for their implementation and maintenance. This reference is deemed credible because it builds from the work of recognized standards organizations (ITIL and NIST) and is excerpted from the official journal of $(ISC)^2$. The International Information Systems Security Certification Consortium, Inc. $(ISC)^2$ is an educational organization that provides certification in a variety of information security disciplines ($(ISC)^2$, 2010).

Song, S. & JaJa, J. (2009). Techniques to audit and certify the long-term integrity of digital archives. *International Journal on Digital Libraries, 10(2/3),* 123-131. Retrieved April 1, 2010, from http://dx.doi.org/10.1007/s00799-009-0056-2

Abstract. A fundamental requirement for a digital archive is to set up mechanisms that will ensure the authenticity of its holdings in the long term. In this article, we develop a new methodology to address the long-term integrity of digital archives using rigorous cryptographic techniques. Our approach involves the generation of a small-size integrity token for each object, some cryptographic summary information, and a framework that enables cost-effective regular and periodic auditing of the archive's holdings depending on the policy set by the archive. Our scheme is very general; architecture and platform independent, and can detect with high probability any alteration to an object, including malicious alterations introduced by the archive or by an external intruder. The scheme

can be shown to be mathematically correct as long as a small amount of cryptographic information, in the order of 100 KB/year, can be kept intact. Using this approach, a prototype system called ACE (Auditing Control Environment) has been built and tested in an operational large-scale archiving environment.

Comments. This article is deemed relevant because it deals with issues related to the GARP® principles of integrity, availability, and retention and reviews and proposes procedures and techniques for addressing them. The reference is deemed credible because it is published in the *International Journal on Digital Libraries*, a peer reviewed academic journal.

Stephens, D.O. & Wallace, R.C. (2003). ***Electronic records retention: New strategies for data life cycle management.*** **Lenexa, KS: ARMA International.**

Abstract. Building on their 1995 groundbreaking book on electronic records retention, David Stephens and Roderick Wallace have authored a comprehensive new book that defines a practical methodology for applying the principles of records retention to computer-based recordkeeping environments. The book includes chapters on:

the business case for electronic records retention, a cost-benefit analysis for retaining versus scheduling and purging electronic records, desktop environments, e-mail retention, Web environments, digital preservation / long-term data retention, legacy data, legislation and court cases, and case studies.

This book also addresses the implications of: the international records management standard, the first-ever global standard on records management, which endorsed the concept of records retention as a best practice for managing the life cycle of information (*ISO 15489 - 1 Information and Documentation — Records Management — Part 1:*

General), the U.S. Department of Defense standard prescribing requirements pertaining to records management software applications (DoD 5015.2-STD, "Design Criteria Standard for Electronic Records Management Software Applications"), the U.S. Internal Revenue Services-issued Revenue Procedure 98-25, which imposes certain long-term data retention requirements on corporate taxpayers.

Comments. This reference is deemed relevant because it addresses multiple aspects of electronic RIM and reviews and incorporates several of the standards deemed influential to the development of the GARP® principles. This reference is considered credible because Stephens is a recognized expert in RIM; both authors are Certified Records Managers (CRM), the text is heavily referenced, and is published by ARMA International, the leading professional organization that addresses records and information management issues.

United States Government Accountability Office (2009). *Federal information system controls audit manual (FISCAM)*. U.S. Govt. Accountability Office. Retrieved April 1, 2010, from http://www.gao.gov/new.items/d09232g.pdf.

Abstract. This manual lists specific control activities and techniques and related suggested audit procedures. These are described at a high level and assume some level of expertise for an auditor to perform these audit procedures effectively. Accordingly, the auditor, applying judgment, should develop more detailed audit steps and tailor control activities based on the specific software and control techniques employed by the entity, the audit objectives, and significant areas of audit interest. Further, the auditor is responsible for identifying any necessary changes to IS control-related criteria, including

changes to control activities and techniques, based on publications issued after December 2008.

Comments. This reference is deemed relevant because it addresses aspects of the GARP® principles of accountability and integrity, specifically examines these issues in relation to the information systems used to manage records and information, and reviews specific practices to insure the accountability and integrity of electronic information and the systems and access controls needed. This standard is considered credible because it is published by the GAO, "known as the investigative arm of Congress and the congressional watchdog. The GAO is an independent, nonpartisan agency that works for Congress. GAO investigates how the federal government spends taxpayer dollars. The head of GAO, the Comptroller General of the United States, is appointed to a 15-year term by the President from a slate of candidates Congress proposes" (United States Government Accountability Office, n.d, para 1).

Ward, B., Purwin, C., Sipior, J., & Volonino, L. (2009). Recognizing the impact of e-discovery amendments on electronic records management. *Information Systems Management, 26(4),* 350-356. Retrieved May 16, 2010 from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=cph&AN=44820810&loginpage=login.asp&site=ehost-live&scope=site

Abstract. Amended rules to the Federal Rules of Civil Procedure (FRCP), which became law in December 2006, are aimed at a single issue—the discovery of electronically stored information (ESI), referred to as electronic discovery (e-discovery). All forms of ESI may be subject to discovery, the investigative phase of a legal case when the parties determine what evidence is, or might be, available. This article addresses concerns of organizations

in responding to e-discovery requests and concludes with recommendations for the design and development of an electronic records management (ERM) policy that recognizes the duties imposed by the e-discovery amendments.

Comments. This reference is deemed relevant because it addresses the impact of the FRCP, one of the major factors impacting the RIM landscape today (AXS-One, Inc., 2007), and reviews practices for ensuring legal compliance, availability, retention and protection of ESI; issues directly related to several of the GARP® principles. The reference is deemed credible because two of the authors are affiliated with major universities, the third is a licensed and practicing attorney and the article is published in *Information Systems Management*, a peer reviewed academic journal.

Weitzner, D., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., & Sussman, G. (2008). Information accountability. *Communications of the ACM, 51(6),* 82-87. Retrieved April 1, 2010, from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=buh&AN=32801384&loginpage=Login.asp&site=ehost-live&scope=site

Abstract. The article discusses mechanisms for ensuring the responsible use of personal information. Traditional approaches have emphasized various legal and technical devices such as copyrights and encryption. The ubiquity of Internet use coupled with the world's growing connectedness, however, renders these approaches inadequate. In the authors' view the best approach involves legal and social rules that emphasize transparency and accountability. How data are being used should be readily discernable, and individuals should be held accountable in the event of misuse.

Comments. This reference is deemed relevant because it addresses aspects of the GARP® *Principle of Accountability* and reviews a variety of practices to insure the accountability of electronic information and the systems and access controls needed. The reference is considered credible because *Communications of the ACM* is a peer reviewed academic journal and the official publication of ACM, Inc. (Association of Computing Machinery), an educational and scientific society uniting the world's computing educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges (ACM, Inc., 2010).

Review of the Literature

Targeted keyword searches of online indices, library collections, and professional organization resources reveal that there is a significant amount of information available on the topics related to electronic RIM. Though the Generally Accepted Recordkeeping Principles® (GARP®) presented by ARMA International provide a framework for reviewing these vast resources, a variety of approaches, techniques and practices abound. As a way to present the information garnered during content analysis of selected references, the review of literature is structured into three major sections:

- An overview of the GARP® principles including its purpose, development, a summary of each principle, and the foundational references used in its development.
- A detailing of the recordkeeping requirements derived from each of the GARP® Principles.
- An identification of practices for the management of electronic records and information related to the GARP® derived requirements, presented as conclusions.

Where possible, these sections are ordered to mirror the structure of GARP® for consistency and so that the concepts, requirements and practices presented are easily associated with the appropriate GARP® principle.

Overview of the Generally Accepted Recordkeeping Principles® (GARP®)

Records and recordkeeping are essential to the performance of organized activities (ARMA International, 2009d). Through the creation and proper maintenance of records and information, organizations are able to understand what has been accomplished and plan for their future (ARMA International, 2009d). As a result, records play an essential role in the success or failure of an organization. More and more organizations, and the professionals that advise and manage them, have come to the realization that every member of the organization is in need of recordkeeping processes and skills (ARMA International, 2009a).

The purpose of GARP®. In an effort to aid these organizations and professionals, ARMA International drafted the Generally Accepted Recordkeeping Principles® (GARP®) in the spring of 2009 (ARMA International, 2009a). The intent of GARP® is to provide business leaders, legislators, the judiciary and others with a framework necessary to implement information management programs (ARMA International, 2009a). Through the dissemination of the GARP® principles, the goals are to establish uniform RIM practices, increase the general awareness and soundness of RIM practices, and to offer guidance to both RIM and non-RIM practitioners in their pursuit of RIM initiatives (ARMA International, 2010c).

The development of GARP®. GARP® was developed from RIM legislation and regulation, the combined experiences of the GARP® development committee, the existing and extensive body of national and international standards and guidelines, current litigation trends and case law, and the recommendations and input of ARMA International's 11,000+ professional practitioners (ARMA International, 2009a). The development of GARP® "represents the application of the standards development and vetting process to the field of records and information management (RIM)" (ARMA International, 2010c, p. 7).

Summary of the GARP® Principles. Records and information management practices are not new (Stephens, 2009) and the principles of recordkeeping have been well developed by those fully involved in the RIM field (ARMA International, 2009d). With the rapid expansion of available information, especially electronic, organizations have come to the realization that an understanding of RIM principles is essential for individuals whether they are directly involved in the RIM field or not (ARMA International, 2009a). An extensive set of RIM standards, best practices, and formal guidelines was already in existence before GARP® (ARMA International 2010c). GARP® condenses this extensive body of work into eight fundamental principles (ARMA International, 2009d):

- *Principle of Accountability*
- *Principle of Integrity*
- *Principle of Protection*
- *Principle of Compliance*
- *Principle of Availability*
- *Principle of Retention*
- *Principle of Disposition*
- *Principle of Transparency*

These principles "set a standard of conduct and practice deemed by practitioners in the RIM field to represent sound policy and practice" for the management of records and information (ARMA International, 2010c, p. 7-8). The eight GARP® principles establish the characteristics of an effective recordkeeping program independent of an organization's size, industry, complexity or other unique factors (ARMA International, 2009a). Accordingly, the principles are designed to be comprehensive in scope, but general in nature (ARMA International, 2009d).

When describing the *Principle of Accountability*, ARMA notes, "An organization shall assign a senior executive who will oversee a recordkeeping program and delegate responsibility to appropriate individuals, adopt policies and procedures to guide personnel, and ensure auditability" (2009d, p. 3). The *Principle of Accountability* focuses mainly on the manual processes, procedures, governance structures and documentation necessary to clearly indicate the roles played by individuals in the RIM process at all levels of the organization (ARMA International, 2010c). Additionally, audits are presented as a key tool used to assess that appropriate levels of RIM-related accountability are achieved throughout the organization (ARMA International, 2010c). As such, all aspects of the organizational RIM process must be developed to include audits in order to demonstrate to stakeholders that both the levels of accountability and the outcomes are measured and evaluated. Additionally, the audit process must include processes for addressing any accountability delinquencies identified (ARMA International, 2010c).

The GARP® *Principle of Integrity* states, "A recordkeeping program shall be constructed so the records and information generated or managed by or for the organization have a reasonable and suitable guarantee of authenticity and reliability" (ARMA International, 2009d, p. 4). Authenticity and reliability are two of the four essential characteristics of a record as outlined in ISO 15489-1 and are fundamental in differentiating records from general information sources (International Organization for Standardization, 2001a). In order to achieve record integrity, GARP® establishes the importance of capture mechanisms, appropriate rules and structure, change management processes, and the necessary security and controls needed at all stages of the organizational RIM process (ARMA International, 2010c).

In establishing the GARP® *Principle of Protection***,** ARMA states, "A recordkeeping program shall be constructed to ensure a reasonable level of protection to records and information that are private, privileged, secret or essential to business continuity" (2009d, p. 5). The *Principle of Protection* addresses not only the physical and electronic protections typically associated with information security practices, but also addresses the need for business continuity and recovery (BC&R) planning. According to ARMA, such comprehensive efforts are necessary to ensure the full protection of records and information and the various physical and electronic systems used in RIM (ARMA International, 2010c). To balance the competing issues of cost and protection, ARMA puts forward the concept of a "Spectrum of Protection" to assist organizations with establishing various needs and justifications to protect, or not protect, organizational records and information (ARMA International, 2010c, p. 39-41).

Compliance with laws and regulations plays a major role in the development of RIM programs (Kahn & Blair, 2009). Equally important is the establishment of, and compliance with, the business requirements that drive the need for and creation of records and information (Kahn & Blair, 2009). To emphasize this trilateral relationship, GARP® includes all three in establishing the need for record compliance. The *Principle of Compliance* states that, "the recordkeeping program shall be constructed to comply with applicable laws and other binding authorities, as well as the organization's policies" (ARMA International, 2009d, p. 6). As with the *Principle of Accountability*, ARMA emphasizes the role of audits in demonstrating organizational compliance with established requirements (ARMA International, 2010c).

While the correct management, compliance, and accountability structures are all important aspects of RIM programs, in their most essential form records are tools that support decision-making, delivery of goods and services, and essentially all organizational functions

(ARMA International, 2010c). For records to be effective in this role, they must be available when needed (ARMA International, 2010c). As such, the GARP® *Principle of Availability* establishes that "an organization shall maintain records in a manner that ensures timely, efficient, and accurate retrieval of needed information" (ARMA International, 2009d, p. 7). ARMA puts forth a solution that includes a combination of "knowledge, design, process and documentation, and compliance and accountability" (ARMA International, 2010c, p. 58) to address this need.

The value that records provide to organizations typically diminishes overtime; this is a concept known as the record lifecycle (U.S. Department of Defense, 2007). This diminishing value, combined with the costs associated with record maintenance and management, makes it logical for organizations to delete or destroy valueless records and reduce the inefficiencies and risks that result from unending retention (ARMA International, 2010c). However, an ad hoc approach to record destruction could impair organizational processes and run afoul of laws and regulations (ARMA International, 2010c). To address this potential conflict, the GARP® *Principle of Retention* states that "an organization shall maintain its records and information for an appropriate time, taking into account legal, regulatory, fiscal, operational, and historical requirements" (ARMA International, 2009d, p. 8). Once retention criteria have been established, auditing for compliance is essential to ensure that records are retained as outlined and that disposition occurs in an appropriate fashion (ARMA International, 2010c).

When the time comes to discard records and information, it is not as simple as hitting a delete key or putting the records to the curb with the rubbish; nor is record disposition limited to their ultimate destruction (ARMA International, 2010c). The how and the why of record disposition is impacted by many factors: laws, regulations, organizational changes, divestures, etc. In addressing the many facets of record disposition, the GARP® *Principle of Disposition*

puts forth that “an organization shall provide secure and appropriate disposition for records that are no longer required to be maintained by applicable laws and the organization’s policies” (ARMA International, 2009d, p. 9) and examines destructive and non-destructive disposition. A key component of the disposition process is the inclusion of adequate security to prevent the inadvertent disclosure of sensitive information (ARMA International, 2010c). To ensure that all aspects of the disposition process are in compliance, and to guard against gaps that could result in significant problems for the organization, ARMA again includes audits as a necessary check on the overall process (ARMA International, 2010c).

In describing the *Principle of Transparency*, ARMA states “the process and activities of an organization’s recordkeeping program shall be documented in an understandable manner and be available to all personnel and appropriate interested parties” (ARMA International, 2009d, p. 10). If legitimately interested parties cannot ascertain how the organizational RIM program and structure functions in achieving RIM goals and outcomes, the program is ultimately a failure. This is because the organization, and its stakeholders, is subject to the risks, inefficiencies, and lack of confidence in organizational decisions and actions that RIM programs attempt to address (ARMA International, 2010c). The GARP® *Principle of Transparency* establishes the final essential element that provides the necessary framework to knit the components together into a cohesive recordkeeping program.

GARP® Key Foundational References

GARP® was developed with "all of the major ANSI/ISO/ARMA standards playing a foundational role" (ARMA International, 2009a, para. 3) and the principles of recordkeeping have been well developed by those fully involved in the RIM field (ARMA International, 2009d). As a result, a significant number of standards, guidelines, best practices, and other sources are available for review to understand the development and applications of GARP®.

According to ARMA International President-elect and GARP® committee member Galina Datskovsky Ph.D., CRM (personal communication, May 13, 2010) and GARP® committee member Lenore Greenburg, CRM (personal communication, May 12, 2010), of the multitude of sources referenced during the development of GARP®, four were particularly influential: (a) ISO 15489, (b) DoD 5015.2, (c) MoReq2, and (d) litigation trends and precedents.

ISO 15489 was published in 2001 by the International Organization for Standardization. *Information and documentation – records management part 1 & part 2*, ISO 15489 collectively, represent the first international standard for records management and is the culmination of a global best practices movement 15 years in the making (Stephens, 2001). The 11 sections and separate technical report that make up the standard establish several normative references for the RIM field and address the various components, general baseline requirements and reasonably anticipated benefits of a comprehensive records management program (Stephens, 2001). Heavy emphasis is placed on the development of policies, procedures and practices necessary to ensure that records are adequately created, captured and managed (Stephens, 2001). Building from prior standards including ISO 9000, AS 4390, the UN Model Law on Electronic Commerce, and the 1997 version of DoD 5015.2 (Stephens, 2001), ISO 15489 has become the key standard for RIM

and has played a significant role in the development of additional standards and practices including GARP® (ARMA International, 2009a).

DoD5015.2-STD is the electronic records management software applications design criteria standard, published by the U.S. Department of Defense in 1997 and revised in 2002. It has become a de facto standard for government agencies, private corporations, and has played a role in the development of RIM standards in other countries (Gable, 2002). The standard defines mandatory functionality for records management application software and details several mandatory requirements for software to be DoD 5015.2 certified (Gable, 2002).

Building from IS0 15489, DoD 5015.2 and several other country specific standards (Gable, 2002; Fresko, 2008), the *Model requirements for the management of electronic records, update and extension,* published in 2008 by the DLM Forum, is a significant standard in its own right. The 2008 update, commonly referred to as *MoReq2*, is intended as a specification for records management systems that address the management of electronic and physical records and includes several enhancements and changes to the original standard (Fresko, 2008). MoReq2 establishes general specifications for the management of electronic records including: retention, classification scheme integration, vital records, email, naming and numbering protocols, long-term preservation, and application ease of use (Fresko, 2008).

GARP® was not influenced by a specific precedent or case, but rather by *litigation trends and precedents* observed over the last several years (G. Datskovsky, personal communication, May 13, 2010). While there have been several cases that have raised the importance of electronic RIM, leading the way to the recent trends were the 2006 amendments to the Federal Rules of Civil Procedure (FRCP) (The Sedona Conference®, 2007, November) that introduced the concept of electronically stored information (ESI) and established requirements for the search

and production of electronic records and information in the federal courts (AXS-One, Inc., 2007). According to The Sedona Conference® (2008) the result has been court decisions and developing case law focusing on and raising issues concerning: "(A) determining the owner/creator of ESI; (B) understanding the limits of technology in authentication; (C) analyzing threats to the integrity of ESI; (D) dealing with the sheer volume of ESI; and (E) identifying the custodian and qualifying the custodian for testimony." GARP® was drafted, in part, to address these and other issues (G. Datskovsky, personal communication, May 13, 2010).

Recordkeeping Requirements Derived from the GARP® Principles

GARP® was developed with "all of the major ANSI/ISO/ARMA standards playing a foundational role" (ARMA International, 2009a, para. 3) and is intended to set forth the characteristics of an effective recordkeeping program (ARMA International, 2009d). To accomplish this goal, each of the eight principles outline issues of general applicability and general considerations that, when combined with the unique needs and circumstances of an organization, can be applied to the development of a customized recordkeeping solution (ARMA International, 2010c). To do this effectively, these principles must be translated into requirements that identify the constraints, demands, necessities, needs, or parameters that must be met or satisfied for the creation and maintenance of records by an organization.

Requirements related to the GARP® *Principle of Accountability*. The GARP® *Principle of Accountability* defines accountability by examining issues of authority, responsibility, and resulting outcomes (ARMA International, 2010c). The main premise of this principle is that "if no one is responsible for ensuring that a thing gets done, and there are no consequences for it not getting done, it doesn't get done" (ARMA International, 2010c, p. 11). For an organization to achieve true accountability in RIM practices, either physical or electronic,

there are several requirements that must be met. Key among the requirements for accountability is authority. For the recordkeeping program to meet its goals, the individual(s) with assigned responsibility must have the authority to: (a) force change when needed, (b) assign and delegate responsibilities including making assignees responsible for the outcomes, and (c) obtain and distribute needed resources (ARMA International, 2010c).

Achieving accountability does not begin and end with authority. Parties must be able to demonstrate that the processes for which they are responsible are well constructed, well documented, and actually achieve the outcomes and/or improvements claimed (ARMA International, 2010c). To do this the documentation must be consistent, have built in processes for review and approval when aspects of the program are introduced or changed, be compatible with existing and anticipated business processes, and be subject to audit and remediation (ARMA International, 2010c). It is this last requirement, audit and remediation, that allows the organization to demonstrate that the authority it has granted is well placed, that individuals are accountable for the outcomes of the RIM program, and that when issues are identified the necessary changes are made (ARMA International, 2010c). Audit and remediation programs allow the organization to: (a) reinforce compliance by holding individuals accountable for results and through the reporting of those results to senior staff, (b) identify program and performance weaknesses or gaps, (c) develop plans for addressing the identified delinquencies, and (d) demonstrate to stakeholders that the organization has developed and is following processes that achieve the desired results and have reasonable process for the identification and addressing of program performance issues (ARMA International, 2010c).

Requirements related to the GARP® *Principle of Integrity*. Unless suitable controls are in place, recordkeeping systems, be they physical or electronic, will become unreliable and imprecise (ARMA International, 2010c). To address this issue, the GARP® *Principle of Integrity* establishes requirements for all stages of the record lifecycle and the development and management of the recordkeeping system. For a record to demonstrate that it has authenticity and reliability, and therefore possess integrity per the GARP® definition, there must be mechanisms and controls in place to ensure that information is accurately captured at inception, is protected against inadvertent or deliberate alteration during usage and maintenance, is secured against unauthorized access, and that proper and appropriate disposition occurs at the end of its required retention (ARMA International, 2010c).

Recordkeeping systems must achieve these goals as well. This can be done through the usage of access controls, the application of information security protocols, the enforcement of rules through the use of workflows and audit trails, and the facilitation of quick and accurate search (ARMA International, 2010c).

For electronic recordkeeping systems the proper creation and capture of metadata and other necessary data attributes is required (ARMA International, 2010c). The proper maintenance and upgrading of application software and systems is also essential (ARMA International, 2010c). Electronic recordkeeping systems are particularly prone to record integrity issues during data migrations and transformations and adequate design and planning are essential to protect against data loss or alteration (ARMA International, 2010c). During normal operations, system upgrades, or media migrations, care must be taken to ensure that the process does not mar the integrity of the initial data set and structure (ARMA International, 2010c). In addition to the base requirements to ensure record integrity, efforts must be taken to capture

necessary data elements that will support the continued use and preservation of the record (ARMA International, 2010c). Failure to meet these, and all the requirements that establish record integrity, will result in wasted expenditures and may subject the organization to operational, legal and/or regulatory difficulties.

Requirements related to the GARP® *Principle of Protection*. To provide the goods and services that people expect in modern society, organizations collect significant amounts of information (ARMA International, 2010c). The information collected and maintained by organizations contains various economic, historical and personal value and includes basic contact information, detailed purchase histories, medical information, trade and government secrets, and everything in between (ARMA International, 2010c). Organizations that create and host this sensitive information have an obligation to protect it from loss, alteration, or unauthorized access; failure to do so can be costly not only to the organization itself, but to all stakeholders involved (ARMA International, 2010c). The GARP® *Principle of Protection* addresses this obligation by establishing requirements for the proper protection of both physical and electronic records and information.

To meet their protection obligations, organizations must have knowledge of what information is collected, why it is collected, and what happens to that information when it is no longer needed (ARMA International, 2010c). Once this universe of information is ascertained, an understanding of the laws and regulations that impact what information is and can be collected, how and where it is maintained, how long it can or must be maintained, and the appropriate or mandated forms of disposition are needed (ARMA International, 2010c). Once these core elements of the RIM process are understood, the requirements associated with the GARP® *Principle of Protection* provides the guidance necessary. This guidance includes the

physical and electronic protections needed during normal operations and also addresses business continuity and recovery (BC&R) planning (ARMA International, 2010c).

To ensure that records and information are adequately protected at all times, several factors must be built into the RIM process. In protecting the records and information directly, information security protocols such as limited data access, strong passwords, encryption, data backup and replication are all required (ARMA International, 2010c). Additionally, physical protection measures such as limiting access to data storage centers or other IT infrastructure and the placement of the data storage hardware including the location of the facility must all be considered (ARMA International, 2010c). Once the records and information are ready for disposition, disposing data in a manner that is consistent with its level of sensitivity is essential (ARMA International, 2010c). Simpler and less technology dependent requirements include only collecting information that is needed to perform organizational functions and then keeping the collected information only as long as is necessary or required (ARMA International, 2010c). Finally, in addition to the requirements necessary for routine day-to-day operations, organizations must design, implement and test BC&R plans and protocols to ensure that sensitive records and information can be accessed and properly protected under adverse conditions (ARMA International, 2010c).

Requirements related to the GARP® *Principle of Compliance*. Regardless of purpose or focus, every organization is subject to a mix of internal and external factors that impact and direct how records and information are managed (ARMA International, 2010c). These factors include (ARMA International, 2010c):

- Statutes
- Regulations

- Internal authorities, policies and procedures
- Industry specific best practices, codes and customary procedures

For organizations to be successful, and to protect the interests of all stakeholders, compliance with these varied and disparate factors is required (ARMA International, 2010c). The GARP® *Principle of Compliance* addresses these factors by establishing broad requirements that will allow organizations to achieve this needed compliance.

Key among the requirements established by the GARP® *Principle of Compliance* is for organizations to gain a fundamental understanding of the various internal and external compliance requirements they are subject to as well as an understanding of the repercussions of non-compliance (ARMA International, 2010c). By understanding these factors organizations can then determine which compliance factors have the greatest impact on recordkeeping, if any of the requirements overlap, and if internal policies and procedures are in conflict (ARMA International, 2010c). Organizations can then prioritize the efforts necessary to address compliance needs and establish the mechanisms to address them (ARMA International, 2010c).

Not only must the recordkeeping system be compliant, but the processes and technology that support it must be compliant as well (ARMA International, 2010c). Simply stating that a recordkeeping program is compliant is not sufficient. Organizations must be able to both demonstrate and document their compliance to all legitimately interested parties (ARMA International, 2010c). Additionally, as with the GARP® *Principle of Accountability*, audit and remediation programs are necessary to validate that process and procedural outcomes are in fact in compliance and to identify and implement any needed changes to ensure that compliance in the future (ARMA International, 2010c).

Requirements related to the GARP® *Principle of Availability*. ARMA argues that, in their purest form, records are tools (ARMA International, 2010c). As such, for records to be effective in this role organizations must be able to retrieve the records they have created, for the purpose for which they have been created, and be able to do so in a timely fashion (ARMA International, 2010c). While this may seem an obvious point, too often this is not the reality (ARMA International, 2010c). Poor recordkeeping system design, lack of organization, and the sheer volume of information and records maintained conspire to create poor availability (ARMA International, 2010c). To prevent valuable information from becoming lost, the GARP® *Principle of Availability* establishes base requirements to ensure the availability of records throughout their lifecycle.

First, organizations must be knowledgeable of the records and information they create and test these expectations against reality (ARMA International, 2010c). Too often records that are expected to be available do not exist, either in whole or in part, because no effort was made to validate that they were being created, that the system(s) that maintain them are not destroying or corrupting them, that the workflow that results in record creation is standardized and results in expected outcomes, or that the workflow to capture the necessary records is unused or bypassed (ARMA International, 2010c). Additionally, often when the records are created they are rendered unavailable because the information necessary to retrieve them is unavailable, not created consistently or at all, becomes lost or altered, or because the resulting outcome of the workflow process is simply unknown (ARMA International, 2010c).

To prevent this type of loss, and to ensure that records are available when needed, robust and detailed recordkeeping system design and documentation is required (ARMA International, 2010c). Recordkeeping systems should be reliable and avoid the loss or corruption during

routine operation (ARMA International, 2010c). The workflows at all stages of the RIM lifecycle should be standardized, understood by all, and be subject to validation (ARMA International, 2010c). Additionally, rather than relying on tacit organizational knowledge, systems, workflows and expected outputs should be meticulously documented so that this knowledge is not lost during organizational restructurings, personnel changes, or through the passage of time (ARMA International, 2010c).

Standardized processes and workflows can only dictate where the records should go; technology, when properly implemented, can play a significant role in ensuring record availability by automating processes and alerting users to unexpected results (ARMA International, 2010c). Proper implementation of technology requires that: (a) the system is appropriate for the task undertaken; (b) effective controls and procedures are in place to ensure the proper access to and availability of records and information created and maintained; (c) systems are properly configured and, where necessary, integrated; and (d) users understand how to use the system, how it impacts record and information creation and maintenance, and what to do if errors or omissions are discovered (ARMA International, 2010c). As before, audits and remediation can and should play a significant role in validating these process and procedures and in detailing the actions to be taken when discrepancies are discovered (ARMA International, 2010c).

Requirements related to the GARP® *Principle of Retention*. Though records are valuable tools, few records maintain a consistent level of value after creation (ARMA International, 2010c). In essence, records have lives: they are born, have a working life, retire due to inactivity, and eventually die (ARMA International, 2010c). This concept, known as the information lifecycle (U.S. Department of Defense, 2007), should be predictable (ARMA

International, 2010c). Regardless of form, records are expensive to maintain indefinitely and most organizations desire and benefit from the proper deletion of expired records and information (ARMA International, 2010c). Before records can be deleted however, organizations must understand the retention requirements to which the records and information they create and maintain are subject (ARMA International, 2010c). The GARP® *Principle of Retention* provides a framework to assist organizations in determining their retention requirements as well as the basic requirements to ensure that stakeholders are not inadvertently denied the information and records they need or to which they are entitled.

To determine appropriate retention, several factors must be evaluated (ARMA International, 2009d):

- Legal and regulatory requirements
- Fiscal requirements
- Operational requirements
- Historical preservation requirements

Determination of retention periods is not always a straightforward process (ARMA International, 2010c). When legal and regulatory requirements exist, they typically do not directly align with the records and information created and maintained by the organization (ARMA International, 2010c); as a result "enlightened guessing" may be required at times (ARMA International, 2010c, p. 66).

Regardless of the methods used, once the various requirements have been identified the organization must document and implement the retention decisions (ARMA International, 2010c). While there are various documents that can and should be created as part of this process, the key requirement is consistency (ARMA International, 2010c). Both physical and electronic

recordkeeping systems must be designed with workflows and processes that support the identified retention period and, per the GARP® principles of Integrity, Protection, and Availability, ensure that the records and information are not lost, altered or rendered inaccessible until the identified retention requirements have been met (ARMA International, 2010c). Electronic information systems can be particularly problematic when it comes to retention requirements because they typically have not been designed with recordkeeping requirements in mind (ARMA International, 2010c) and often cannot delete individual data sets resulting in what is tantamount to permanent retention, or are transactional in operational focus and are not designed to maintain large volumes of data for extended periods of time (ARMA International, 2010c; Saffady, 2009). Existing systems must be evaluated for retention compliance and a plan must be developed to bring these systems into compliance through upgrades or replacement with new systems (Stephens, 2009).

As before, audits and remediation play a significant role in ensuring organizations are meeting their retention obligations (ARMA International, 2010c). When conducting audits for retention compliance multiple factors beyond the proper retention of records must be evaluated (ARMA International, 2010c). Additional considerations that must be assessed include: (a) changes in retention requirements; (b) modification or elimination of workflows or other processes that unintentionally impact retention; (c) and the overall complexity of the organization retention framework that may lead to poor or non-compliance (ARMA International, 2010c). As with all audits, findings must be adequately documented to assist with the development and implementation of remediation efforts (ARMA International, 2010c).

Requirements related to the GARP® *Principle of Disposition*. Once an organization has satisfactorily met its record retention requirement, it is time for disposition (ARMA International, 2010c). Before record disposition can occur, several factors must be evaluated to ensure that records and information are deleted, destroyed, or transferred in an appropriate manner (ARMA International, 2010c). The GARP® *Principle of Disposition* establishes the base requirements to ensure that this obligation is met.

As with the GARP® *Principle of Protection*, the security of records and information during the disposition process is an essential requirement (ARMA International, 2010c). The disposition method selected must be appropriate for the sensitivity of the information the records contain (ARMA International, 2010c). Additionally, the medium in which the record is maintained will affect the appropriateness and type of disposition method (ARMA International, 2010c). While shredding, burning, and pulping are typical destruction methods, they may not be appropriate based on environmental factors, storage media, regulation, historical preservation needs, or other factors (ARMA International, 2010c).

Electronic disposition creates additional complications. Unless the entire system is being retired or no longer needed, destruction or degaussing of the storage media is not a viable approach (ARMA International, 2010c). With the destruction of the storage media or system no longer an option, care must be taken to ensure that the deletion or overwriting of electronic records on active systems actually occurs (ARMA International, 2010c). Too often systems merely delete index entries or the metadata used to facilitate retrieval and the content continues to reside on the system for some time (ARMA International, 2010c; Kahn & Blair, 2005; Saffady, 2009). If the disposition of electronic records involves that transfer to an outside party or is intended to facilitate historical preseveration, several additional factors must be resolved

(ARMA International, 2010c). The format used to store the records as well as the software used to access them must be carefully selected or the records may be rendered inaccessible through technology obsolescence (ARMA International, 2010c).

Finally, proper disposition procedures require that potential gaps in the process are identified and addressed (ARMA International, 2010c). Are computers, copiers, servers, or other electronic storage devices properly wiped before resale or return to the vendor at end of life (ARMA International, 2010c)? Are records deleted or destroyed in a way that reasonably prevents their reconstruction and the information they contain (ARMA International, 2010c)? Are records and information destroyed in a timely and consistent manner across the organization, or is the approach ad hoc (ARMA International, 2010c)? Can the records be destroyed, or are they subject to a legal preservation order (ARMA International, 2010c)? These concerns and the issues related to them are again addressed through audits and remediation (ARMA International, 2010c). The goal of these audits is simple: a determination if the disposition of records occurs in an appropriate manner and in accordance with all identified requirements (ARMA International, 2010c).

Requirements related to the GARP® *Principle of Transparency*. For an organization to achieve transparency, not only must the recordkeeping activities and processes be fully documented, but they must also be made available to all legitimately interested parties (ARMA International, 2010c). Transparency offers organizations three primary benefits (ARMA International, 2010c):

- Operational efficiency – when personnel understand how processes work, they can better manage and optimize their performance.

- Compliance – an organization's records are subject to multiple legal, regulatory, and operational requirements; transparency of recordkeeping systems and processes allow organizations to demonstrate compliance with these requirements.
- Confidence – transparency of organizational recordkeeping processes demonstrates to interested parties that organizational activities and processes are being performed in a legitimate and appropriate fashion, thereby building confidence.

The GARP® *Principle of Transparency* addresses the need for organizational transparency in recordkeeping systems by establishing two broad range requirements: transparency of system design and transparency of system documentation (ARMA International, 2010c).

In order for organizations to achieve transparency in recordkeeping design, the following are required (ARMA International, 2010c):

- A system design with clear workflows
- Well-defined inputs and outputs
- Appropriate structure

Too often, electronic recordkeeping systems include "black-box" processes that are proprietary and not well understood (ARMA International, 2010c). As such black-box processes lack the transparency necessary for an organization to fully defend its actions and outcomes; it is in the organization's and stakeholders' best interests to eliminate them outright whenever possible (ARMA International, 2010c).

Transparency in recordkeeping systems is required so that organizations can demonstrate that their processes, procedures, workflows, and structures are reasonable, accurate, and enforceable (ARMA International, 2010c). In order to achieve documentation transparency and

the benefits that come with it, several key documents are required (ARMA International, 2010c, p 83):

- Strategic documents such as records management policies that clearly set forth the high-level goals and outcomes of the records management program
- Defined records creation processes
- Definitions of the data to be captured on the records in the system
- Well-understood workflows as records move through the system and organization
- Well-defined records lifecycles
- Defined processes for initiating and implementing exceptions such as legal holds
- Defined and consistently executed disposition processes

It is essential that these documents be captured in policies, procedures, operational instructions, diagrams, flow charts, and any other documents necessary to demonstrate recordkeeping processes and transparency (ARMA International, 2010c). Additionally, electronic recordkeeping systems require system-specific documentation demonstrating how records are retained, managed, and purged (ARMA International, 2010c). Such documentation must include the various systems and software used throughout the recordkeeping process and lifecycle (Kahn & Blair, 2005; Saffady, 2009).

Conclusions

This literature review is designed to assist RIM and IT professionals tasked with the responsibility of managing electronic records and information. The study presents information assembled from various sources including academic journals, ARMA International, recognized thought leaders in RIM, and various professional organizations from the RIM, IT and legal fields. This collected information is analyzed using the conceptual analysis process as described by Busch et al. (2005) to ensure that the selected literature is relevant to the electronic records and information management requirements derived from the GARP® principles, and is presented in a manner designed for the needs of the intended audience of this study.

The intent of GARP® is to provide various constituencies with the framework necessary to implement information management programs (ARMA International, 2009a). Once an organization decides to address their recordkeeping responsibilities, adherence to the GARP® principles allows for the establishment of uniform and sound RIM practices (ARMA International, 2010c). The Conclusions present specific practices and program elements that meet the recordkeeping requirements derived from GARP®. The sections that follow summarize major themes that the selected literature indicates are practices that should be considered to effectively address the recordkeeping requirements. Though there are overlaps in the identified requirements and associated practices, the sections are arranged to mirror the structure of GARP® for consistency and so that the identified practices are easily associated with the most relevant principle.

Practices related to the requirements of the GARP® *Principle of Accountability*.

The GARP® *Principle of Accountability* focuses mainly on the manual processes and structures necessary to achieve RIM accountability within an organization (ARMA International, 2009d). However, with the significant and continued growth of electronic information (Stephens, 2009), technology can and should have a role to play. If users are to be held accountable for the records and information they create, access and use, these processes must be made transparent for the user and relevant stakeholders (Weitzner, Abelson, Berners-Lee, Feigenbaum, Hendler & Sussman, 2008).

Practice #1: Employ technical architectures to improve accountability. For information user processes to be transparent, in addition to the authority required by the manual structures outlined by GARP® (ARMA International, 2010c), the user must be able to ascertain if the information they are creating, using and disseminating is occurring appropriately (Weitzner et. al, 2008). Weitzner et al. argue that if users are to be held accountable for the actions they take in regard to records and information, those actions must be based on informed decisions (2008). GARP® addresses this need by establishing a requirement of detailed and consistent procedures (ARMA International, 2010c); Weitzner et al. build off this manual process and suggest the implementation of three technical architectures that will improve transparency for the user and thereby accountability (Weitzner et al., 2008):

- Policy-aware transaction logs
- Policy-language framework
- Policy-reasoning tools

These technical architectures combine to create a structure that permits and documents informed user interactions with electronic records and information and the systems that manage them.

The goal of *policy-aware transaction logs* is straightforward: information events related to creation, access and use relevant to assessing accountability are recorded at each system endpoint (Weitzner et al., 2008). To properly assess these logged transactions, a common *policy-language framework* is required (Weitzner et al., 2008). Rather than relying on an organization-specific framework, Weitzner et al., suggest drawing on semantic web techniques to develop shared policy vocabularies that can be used to assess information accountability both internally and across organizations (Weitzner et al., 2008). Finally, if users are going to be held accountable for the information created, accessed and used, and if such information actions are going to be logged and assessed, a system must be in place to assist users with information-action related questions (Weitzner et al., 2008. p. 86) such as:

- Has data set X been created/accessed/used by an authorized user?
- Is it allowed for data set Y to be used for a given purpose?
- Is Z a reasonable inference in light of the data provenance and applicable rules?

This *policy-reasoning tool* architecture can be achieved through the placement of "accountability appliances" that serve as proxies to data sources (Weitzner et al., 2008). The appliances would control access to data sources based on defined rules and requirements, and protect data provenance and integrity by logging user activities (Weitzner et al., 2008). Additionally, these accountability appliances could be configured to present accountability-related information in human-readable ways to assist users by informing them of rules, policies, and procedures that govern the data resources accessed and allowing them to make informed decisions (Weitzner et al., 2008).

Practice #2: Log user information actions to perform audits. In addition to automating the enforcement of the documentation required by the GARP® *Principle of Accountability*, the technical accountability structure proposed by Weitzner et al. (2008) also provides organizations with a framework for achieving the other key requirement of the principle: audit and remediation (ARMA International, 2010c). By logging user information actions, organizations have the data necessary to perform audits that assess how users have created, accessed and used electronic information and records and if these actions occurred properly. Additionally, the log data and assessments can be used to identify weakness and gaps in the RIM program and related systems (ARMA International, 2010c). To achieve accountability as defined by GARP®, results of such audits and the plans for addressing identified gaps must be shared with senior management (ARMA International, 2010c).

Practice #3: Update and maintain accountability structures. To close the circle on this process, the technical accountability structure must be updated. Particular emphasis must be placed on ensuring the accountability appliances are updated and maintained or the logged data will lack the necessary relevance necessary to assess accountability and the overall technical framework will breakdown (Weitzner et al., 2008). One way to achieve this needed updating is to allow the accountability appliances to communicate through web-based protocols and communicate continuously as the accountability framework evolves (Weitzner et al., 2008).

Practice #4: Implement usage controls. Traditionally, access controls have been used to restrict users from accessing files, directories, devices, and other system objects based on the identity of the users, the groups to which they belong, their role within the organization, or some type of centralized governance structure that decides what users can access (Padayachee & Eloff, 2009). These access controls are difficult to implement and often deficient as they sometimes

eliminate needed access and ultimately do not hold users accountable for the content they do access (Padayachee & Eloff, 2009). As a result, access control policies can at times far outweigh any benefits (Padayachee & Eloff, 2009). Rather than eliminate access, Etalle and Winsborough (2007) suggest that accountability measures be enforced. Padayachee and Eloff (2009) view usage controls as a solution to address the limitations of access control.

Usage control addresses the concepts of *obligations* and *conditions* that are missing from traditional access control (Padayachee & Eloff, 2009). *Obligations* require the user to take an action, such as clicking an ACCEPT button on a usage notice or license agreement, to gain access (Padayachee & Eloff, 2009). Periodically, the same or similar action is required of the user to maintain the access once granted (Padayachee & Eloff, 2009). *Conditions* refer to system-oriented factors such as time-of-day or access location, and limit or deny user access based upon predetermined rules; e.g. content access is limited after business hours or is made inaccessible if the user is logging in remotely (Padayachee & Eloff, 2009). As users must actively acknowledge their obligations, they can no longer claim they are unaware that their actions are not allowed and can therefore be held accountable should they use or access content in a manner different from the purpose for which access was granted (Padayachee & Eloff, 2009). Padayachee and Eloff (2009) propose the following example structure to achieve accountability through usage control:

- Pre-obligation: The user must click on a button in a window indicating that s/he agrees to a usage statement.
- Ongoing obligation: A window with a warning message concerning appropriate usage stays open on the screen at all times.
- Pre-condition: The information may be accessed during business hours only.

- Ongoing condition: The information may be accessed during business hours only (same as the pre-condition, as it is time dependent). While the pre-condition may have been valid at the initial time of access, it may become invalid during the access period.
- Post-obligation: The user must send an email explaining the usage and need for access to the administrator if the access period extends beyond the pre-condition of access during business hours only (p.539).

The post-obligation allows the user to continue to perform necessary duties without interruption or undue restriction as long as they follow the post-obligation requirement (Padayachee & Eloff, 2009). Should the user fail to meet the post-obligation requirement, they are held accountable based on the rules established by the organization (Padayachee & Eloff, 2009).

Practices related to the requirements of the GARP® *Principle of Integrity*.

Establishing record integrity starts at the very beginning of the record and information lifecycle during the creation phase (ARMA International, 2010c; U.S. Department of Defense, 2007). For electronic records and information, establishing integrity requires the proper creation, capture and maintenance of metadata (ARMA International, 2010c; Stephens & Wallace, 2003). The metadata created and captured must support and validate the record characteristics of authenticity and reliability of the record (International Organization for Standardization, 2001b; Stephens & Wallace, 2003), and thereby the record integrity as defined by the GARP® principle (ARMA International, 2010c).

Practice #5: Capture metadata to validate record characteristics. In electronic RIM, establishing authenticity and reliability is achieved by defining record structure and context as well as content (Stephens & Wallace, 2003). According to Stephens and Wallace (2003, p. 76) the metadata that must be captured are defined as follows:

- *Content* metadata includes the words, numbers, sounds and images made by the record's creator.
- *Structure* metadata refers to the appearance and arrangement of the record's content. It includes the meaning of a record as conveyed by the appearance of its characteristics (i.e. typeface), the location of specific data fields… and the pointers used to link physical or logical groups of data.
- *Context* metadata includes the background information describing the origin of the record, which organizational unit created the record, who used it, the purpose for which it was used, and how it relates to other records.

Once metadata has been identified, created and captured, it must be properly maintained to ensure the integrity of the records and information during the remaining stages of the RIM lifecycle (ARMA International, 2010c).

Practice #6: Use database watermarking to ensure record integrity. While information is being actively used and stored, unauthorized changes can result in substantial losses for organizations and their stakeholders (Kamel, 2009). Databases typically contain critical information that requires protection from such alteration to protect the integrity of the records and information they contain (Kamel, 2009). If the integrity of the data maintained within the database is questioned, all related records, the recordkeeping program and the organization itself might be called into question and subject to operational, legal or regulatory complications (ARMA International, 2009d; ARMA International, 2010c; Kamel, 2009). To address the need for database protection and data integrity, Kamel posits the use of database watermarking (2009).

Database watermarking is a technique that hides a "secret message" in some of the attributes of a database relation and data elements (Kamel, 2009). Authorized changes to database elements properly update the hidden watermark as they occur within framework of the overall database structure (Kamel, 2009). Unauthorized changes manipulate individual elements outside of the database structure and do not presevere the data element(s) and relationships necessary to preserve the watermark (Kamel, 2009). Through regular monitoring and auditing of database watermarks, altered information and records are identified before the error is perpetuated thereby calling the integrity of the entire system into question (Kamel, 2009). Database watermarking is only a tool that can identify database information integrity issues (Kamel, 2009). Additional tools and processes must be in place to address integrity issues as they are identified and to preserve the integrity of records and information for the long-term (ARMA International, 2010c).

Practice #7: Implement integrity checks. Long-term preservation of electronic records and information is one of the most challenging problems faced by organizations (Song & JaJa, 2009). Electronic information is fragile due to the risks presented by hardware and software failures, advancements in technology that render present hardware and software obsolete, and the ongoing and growing threat of computer and network data breeches (Song & JaJa, 2009). Additionally, information and records residing on storage systems or being transmitted can become corrupted due to any one of a number of media, hardware or software failures (Song & JaJa, 2009). Once corrupted or rendered inaccessible or unreliable, the integrity of these records and information, and that of the records and information dependent on them, is lost (ARMA International, 2010c). A variety of techniques and practices must be considered to preserve the integrity of records and information for the long-term.

The most basic technique for preserving the integrity of electronic records and information is the implementation of integrity checks (Song & JaJa, 2009). This technique implements the use of data replication and achieves integrity verification through the comparing of replicated data sets against one another (Song & JaJa, 2009). As the constant storage and comparison of complete data sets is costly and error prone, Song and JaJa (2009) propose the use of cryptographic hashing, also called checksum, combined with replication as an integrity verification technique. Rather than doing a full bit-by-bit comparison, the checksum is used to verify the integrity of a data set (Song & JaJa, 2009). A checksum of the bit-stream is computed at record creation and is stored either with the data or separately (Song & JaJa, 2009). Over time, the checksum of the data set is periodically recalculated and compared against the original (Song & JaJa, 2009). If the hash values are correct, integrity is verified; if the checksum differs, the dataset is restored from the master-copy (Song & JaJa, 2009). As with database watermarking, these techniques are only a tool to verify the integrity of a record once it has been created. Organizations must implement and document adequate controls and processes to protect record integrity at various stages of the RIM lifecycle (ARMA International, 2010c).

Practice #8: Create detailed plans and manage metadata for record data migrations. Technology advancements and obsolescence often require that electronic records and information be migrated to new media and systems in order to preserve their integrity (ARMA International, 2007a). Ironically, as Kennedy and Kennedy (as cited in Brown, 2007) observe, the conversion process itself presents one of the most significant technical, operational, and legal risks to record integrity (p. 66-67). Unless proper analysis, planning, testing, and validation occur as part of the conversion process (ARMA International, 2007a), data integrity may be questionable due to data loss or corruption (Kennedy & Kennedy as cited in Brown, 2007).

Additionally, improper or poorly managed data conversions could alter regulatory required audit trails and/or be deemed spoliation should the data be subject to preservation in litigation (Kennedy & Kennedy as cited in Brown, 2007).

If the electronic conversion process is to preserve the integrity of the converted records and information, significant technical and non-technical planning must occur (ARMA International, 2007a). Before conversion occurs, organizations must document the business drivers requiring conversion, the current system status, identify known risks, establish a back-out plan should the conversion process fail, and appoint an officer responsible for the project (ARMA International, 2007a). Once these non-technical issues have been addressed, technical planning includes identification of the technical business requirements including functional needs and capabilities of the present system, present and end-state data structures, network connections, and technical recordkeeping requirements; most importantly metadata (ARMA International, 2007a). The capture and maintenance of metadata throughout the conversion process is necessary not only to ensure conversion occurs correctly and is defensible, but also to maintain the integrity of the records before, during, and after the conversion process (ARMA International, 2007a and 2010c).

Metadata management during the conversion process is necessary to allow organizations to demonstrate that converted records and information continue to be authentic and reliable and therefore possess the integrity of the original data (ARMA International, 2007a). Metadata management includes the identification of metadata required for recordkeeping and integrity in the present system(s) and the expected mapping of that metadata after conversion (ARMA International, 2007a). To protect the integrity of the metadata, and therefore the converted records and information, use of metadata repositories to gather, retain, and disseminate metadata

may be required (ARMA International, 2007a). Additionally, the use of extensible markup language (XML) is recommended to ease complications from interoperability between systems (ARMA International, 2007a). Though data conversions can be risky (Kennedy & Kennedy as cited in Brown, 2007), properly managed and controlled they are an integral part in ensuring the integrity of electronic record and information over the long-term (ARMA International, 2007a).

Practices related to the requirements of the GARP® *Principle of Protection*.

To meet the requirements of the GARP® *Principle of Protection* organizations must secure the records and information for which they are responsible during routine operations, and plan for record access and protection during adverse conditions. The fields of information security and business continuity and recovery (BC&R) are mature disciplines and should be viewed as partners in the efforts to bring RIM programs in line with the requirements of this principle (ARMA International, 2003 & 2010c; Determann & Hwang, 2009; Saffady, 2009; Scholz, 2009).

Practice #9: Implement an information security control framework. Information security is frequently described as focusing on three preservation goals, also known as the C-I-A Triad: Confidentiality, Integrity, and Availability (Baye as cited in Brown, 2007). It is important to note that information security is not a single tool or system that can be implemented to protect an organization (Baye as cited in Brown, 2007). Due to the complexity and diversity of most organizations and the information systems on which they rely, information security is instead a comprehensive strategy that addresses people, processes, policies, procedures, operations, locations, technologies and enforcement (Baye as cited in Brown, 2007). A fully developed information security strategy starts with a detailed control framework that is captured in organizational policies and procedures and addresses program governance and people (Baye as

cited in Brown, 2007). Technology implementation includes detailed strategies and policies as well as managed deployments of technology to support organizational functions and specific information security applications (Baye as cited in Brown, 2007). Once the program framework is established and in place, ongoing monitoring of the people, process and technology is required (Baye as cited in Brown, 2007).

While understanding the basic structure of information security strategies is important, recent developments in security related laws and regulations cannot be ignored. The Health Insurance Portability and Accountability Act (HIPPA), Gramm-Leach-Bliley (GLBA), Sarbanes-Oxley Act (SOX), and Federal Information Security Management Act (FISMA) all contain information security standards and requirements with which many organizations must comply, and they have been with us for some time (Baye as cited in Brown, 2007; Determann & Hwang, 2009). But as Determann and Hwang (2009) observe, beginning with the passage of California Civ. Code § 1798.82 in 2003 there has been a significant shift in the information security requirements to which organizations must adhere. In addition to California, New York, Nevada, Massachusetts, Maine and others have proposed, passed, or modified laws addressing organizational requirements for information security (Determann & Hwang, 2009). These various laws and statutes dictate new administrative, physical, and technical safeguards including tighter encryption standards, physical and electronic record access controls, limits on the types and kind of data that can be collected, and stricter reporting requirements to demonstrate compliance, and when data breeches occur (Determann & Hwang, 2009). For organizations to be consistent with the GARP® *Principle of Protection*, and other GARP® principles, the practices required by these new legislative efforts must be incorporated into the information security framework.

Practice #10: Establish vital record and BC&R programs. A comprehensive information security framework does not stop at addressing the day-to-day security needs of an organization (Paylago; Baye both as cited in Brown, 2007). Business continuity and recovery (BC&R) considerations and experts must be included in information security planning (Paylago as cited in Brown, 2007). Accordingly, the GARP® *Principle of Protection* includes BC&R planning as a requirement for RIM programs (ARMA International, 2010c).

The relationship between BC&R and RIM has been well established (Saffady, 2009). Various requirements and standards including ISO 15489-1 and DoD 5015.2, establish vital records programs, an essential component of BC&R planning, as a requirement to prevent the loss of essential information in the event of emergencies, catastrophic system failures, and other adverse operating conditions (ARMA International, 2009f; Saffady, 2009). Vital records, or those *essential* to the ongoing operations of an organization, require significant efforts and protections in the form of duplication, mirroring, imaging, back-up media strategies, off-line storage, and other techniques and practices (ARMA International, 2003). The challenge for most organizations is that vital record protection efforts, as well as BC&R planning generally, can be costly (Paylago; Baye both as cited in Brown, 2007; Saffady, 2009). These practices make no direct contribution to organizational revenues, product development, the delivery of goods and services and provide little benefit to the organization; that is until disaster occurs (Saffady, 2009).

Protecting the records and information is not enough. Organizations must protect the systems and applications used to create, access and process the information in their possession (ARMA International, 2003). Failure to do so could corrupt the information, render it inaccessible, or expose the organization to legal, operational or regulatory consequences. Such

outcomes ultimately fail to protect the needs of the organization or its stakeholders (ARMA International 2003 & 2010c; Paylago as cited in Brown, 2007). To assist organizations with the need to protect IT infrastructure, Scholz (2009) identifies seven steps based on the National Institute of Standards and Technology Special Publication [NIST SP 800-34] addressing IT BC&R concerns:

- Develop a contingency planning policy statement.
- Conduct a business impact analysis (BIA).
- Identify preventive controls.
- Develop recovery strategies.
- Develop an IT contingency plan.
- Plan testing, training, and exercises.
- Plan maintenance.

Following these basic steps, combined with the incorporation of general information security practices, will bring the organization into compliance with many of the security, BC&R, and other information protection requirements (ARMA International, 2010c; Determann & Hwang, 2009; Paylago as cited in Brown, 2007; Scholz, 2009). While adherence to these various requirements offers many potential advantages to organizations (Scholz, 2009), they represent only some of the compliance requirements to which organizations are subject (ARMA International, 2010c).

Practices related to the requirements of the GARP® *Principle of Compliance*.

When it comes to managing records and information, organizations are subject to a myriad of laws, regulations, best practices, and internal procedures (ARMA International, 2010c). Identification of these various requirements is the first step in achieving compliance (ARMA International, 2010c). With over 4,000 federal, state and local regulations impacting how records are created, stored, protected, accessed and destroyed, the task of identification can be daunting (Adam, 2008; Burns & Peterson, 2010). Compliance with the various laws, regulations and requirements that affect electronic records and recordkeeping systems is important and qualified personnel should conduct an evaluation and determine the applicability of these requirements to the organization (Adam, 2008).

Practice #11: Use control mapping to develop a compliance framework. For many organizations, once the initial challenge of identifying the compliance requirements is complete, the next challenge is to identify an efficient manner in which to streamline their compliance requirements into a single and well-organized strategy (Hayden, 2009). Hayden refers to this strategy as a control framework that includes the policies, processes and technologies put in place to govern organizational activities in an effort to achieve compliance (2009). Hayden suggests that organizations undertake control mapping to identify overlaps in the controls developed or needed so that they can be rolled into a single control framework for compliance (2009).

Hayden identifies two mapping strategies to achieve this goal: normative control mapping and transitive control mapping (Hayden, 2009). The intent of normative control mapping is to develop a new, single control framework that addresses the various needs of the organization by identifying and eliminating the redundant controls and control frameworks

(Hayden, 2009). The goal of transitive control mapping is essentially the same, but the approach and drivers are different (Hayden, 2009). In transitive control mapping an existing control framework is identified as the priority or default framework and controls from other control frameworks are mapped to it (Hayden, 2009). Regardless of the approach, once the various controls are identified, commonalities and overlaps are identified and eliminated to develop a single, cohesive and comprehensive framework for compliance (Hayden, 2009).

Practice #12: Conduct information system compliance audits. Identification of the compliance requirements and the development of a framework to manage them is not enough; organizations must be able to demonstrate compliance (ARMA International, 2010c). As explained by several of the GARP® principles, audit and remediation programs are how organizations demonstrate their compliance (ARMA International, 2010c). In 2009, the United States Government Accountability Office (GAO) published a comprehensive methodology for conducting such audits: the *Federal Information System Controls Audit Manual* or FISCAM. Though designed to assist federal agencies with their compliance and audit needs (United States Government Accountability Office, 2009), the overall approach offers organizations guidance in conducting various types of information system audits.

As part of the overall audit structure, the FISCAM identifies three key stages of information system audits: planning, testing, and reporting (United States Government Accountability Office, 2009). Each stage of the FISCAM strategy begins by detailing the documentation that must be prepared, and the basic steps that must be completed to ensure the audit is reasonable, consistent, and achieves actionable outcomes (United States Government Accountability Office, 2009). By targeting electronic information systems, the FISCAM

provides a strategy for evaluating the compliance of the vast majority of records and information managed by government agencies (United States Government Accountability Office, 2009).

Practice #13: Use digital audit trails, secure deletion and authenticated encryption. Electronic records and the recordkeeping systems used to create, hold and manage them typically represent the most significant volume of records and information in most organizations (Stephens, 2009). In order for these systems to be in compliance with various requirements, and to be subject to audits to demonstrate this compliance, Burns and Peterson (2010) have identified three technology practices and techniques that should be implemented: digital audit trails, secure deletion, and authenticated encryption.

Like a paper audit, a digital audit is a formal assessment of organizational compliance (Burns & Peterson, 2010). The digital audit verifies that electronic records and information have been retained, are unaltered, and are accessible within the file system or application used to manage them (Burns & Peterson, 2010).

Secure deletion is a form of non-destructive deletion used when the electronic RIM system remains actively used (Burns & Peterson, 2010). In most electronic recordkeeping systems a file or data set is "deleted" by removing the index entry referencing the file; the file remains accessible through various computer forensic techniques (ARMA International, 2010c). In addition to deleting the index entry, secure deletion is achieved by repeatedly overwriting data selected for deletion so that the data cannot be recovered (Burns & Peterson, 2010).

When compliance requirements dictate that data must be kept secure from accidental or unauthorized disclosure, or require that the integrity and authenticity of data can be verified, encryption is frequently implemented (Burns & Peterson, 2010). Unfortunately, standard encryption methods are often insufficient as they are subject to malicious or accidental alteration

unless properly configured and implemented (Burns & Peterson, 2010). Unlike standard encryption that encrypts the entire data set as a single unit, authenticated encryption binds authentication information to each block of a file allowing the integrity of the data to be verified block by block (Burns & Peterson, 2010).

Though not necessarily required of all systems, when properly implemented these techniques provide organizations with an ability to demonstrate that their data management practices meet the requirements in a verifiable manner (Burns & Peterson, 2010). By combining comprehensive control frameworks and regular audits and remediation efforts, organizations demonstrate a commitment to compliance that supports various aspects of the GARP® principles.

Practices related to the requirements of the GARP® *Principle of Availability*.

Regardless if they are paper or electronic, records and information are only useful to organizations and their stakeholders if they are available when they are needed (ARMA International, 2010c). Unlike their paper counterparts, electronic records and information cannot simply be pulled from a filing cabinet or shelf and be read; electronic records and information have the defining characteristic of being exclusively machine-readable (Saffady, 2009). For the majority of organizations, electronic records are essential for day-to-day operations, decision-making, and long-term planning (Saffady, 2009). As a result, ensuring that the electronic recordkeeping system preserves record accessibility and availability is crucial.

Practice #14: Adopt relevant DoD5015.2 design specifications. Reflecting this importance, in drafting the *Electronic records management software applications design criteria standard*, typically referred to as DoD5015.2, the U.S. Department of Defense included several design specifications related to record and information availability (2007). DoD5015.2 establishes various and specific criteria for electronic filing structures, search and retrieval,

metadata and other data elements in an effort to ensure that information systems make and keep the electronic record and information accessible and available when needed (ARMA International, 2009f). Since its initial drafting in 1997, DoD5015.2 has been very influential on the design of information systems and is viewed by many to be a de facto standard (Gable, 2002).

Practice #15: Use well constructed file plans. Adhering to the design specifications in DoD5015.2, and combining them with requirements from MoReq2, Saffady (2009) has also identified several key considerations for ensuring the availability of electronic records when acquiring and implementing records management application software. For a records management application to be effective, regardless of the types of content or information it is managing, it must arrange records into a hierarchical folder/subfolder structure that is understandable by users and should be based on a user-defined file plan (Saffady, 2009). In fact, Saffady (2009) asserts that a carefully designed file plan for electronic records is a prerequisite for a successful records management application software implementation.

To ensure that file plans are well constructed, Saffady (2009) identifies a three-phase process prior to implementation (p. 202):

- Investigative phase – In the investigative phase, record types to be managed by the records management application software are identified and are compared with existing filing methods in an effort to develop a draft file plan. Where possible, file plans from government agencies and other organizations are referenced for comparison.
- Prototype phase – The draft file plan is developed, and the folder structures that the records management application software will use to index the records are detailed. This draft file plan is circulated among key stakeholders and potential users to ensure

that the proposed file structures support organizational needs and are logical and understandable; several drafts may be required.

- Test phase – The file plan resulting from the prototype phase is implemented within the records management application software and tested on various collections of electronic data. The results are analyzed with key stakeholders and users and revisions are made as needed.

As the records transferred to the records management application software are typically considered the official records of the organization, unless the file structure is well planned and executed these records could be rendered unavailable, subjecting the organization to various operational, legal, and regulatory issues (Saffady, 2009; ARMA International, 2010c).

Practice #16: Plan for technology obsolescence. Not only do advancements in technology threaten the integrity of records, they threaten their availability as well (ARMA International, 2010c). When developing a long-term strategy to preserve the availability of electronic records, Doyle, Viktor and Paquet (2009) have identified key considerations that must be addressed in the plan:

- The user should be able to access the preserved digital document.
- The content should be executable, i.e. the host machine should be able to render the document in its original environment.
- The end user should be able to interpret and understand the content of the digital document.
- All of the above should be possible without the end user experiencing any errors or complexity.

- The preserved digital object should be authentic in the sense that its content is the same as was preserved and both its content and functionality remain the same through time (i.e. the data object does not become corrupted, or lose data through a process such as migration). The content of the data refers to the data it represents (e.g. a set of geometric points and topologies representing a 3-D anthropometric body scan). Preserving functionality also requires that the rendering application be preserved so that future users can interact with the preserved data object. Preserving the rendering application is necessary as many software applications do not ensure backward compatibility, and hence there is no guarantee that future, more sophisticated versions of the software will be able to render the preserved digital document.
- Metadata should accompany the digital document instructing the future end user on how to execute the document, as well as explaining the document content, its intended behavior and a description of the software required to run it.
- The digital preservation framework should be durable. It should run on any computing platform any number of years in the future (p. 34-35).

Long-term availability of records may be achieved by printing to paper or other non-electronic form (e.g. microfiche), encapsulation, migration, or any one of a number of preservation strategies. By identifying how these considerations can or should be addressed up front and as part of the overall recordkeeping strategy, organizations will have the information necessary to decide upon the appropriate steps and methods to undertake to preserve record availability (Doyle, Viktor & Paquet, 2009).

Practices related to the requirements of the GARP® *Principle of Retention*.

Few records maintain their value over time (ARMA International, 2010c). Unless otherwise needed, maintaining a record beyond its useful life is expensive (ARMA International, 2010c). Under normal circumstances, the destruction of business documents is not unlawful even if it is discovered at a later date that the records would have been relevant to a litigation or other inquiry (Lewis Owens as cited in Brown, 2007). The key is that such destruction must be done pursuant to a valid document retention policy that authorizes the destruction of organizational records as part of the normal course of business (Lewis Owens as cited in Brown, 2007).

Practice #17: Develop a retention schedule that includes electronic records. In addition to the policy, a retention schedule is required (ARMA International, 2005b). A retention schedule is, "a comprehensive list of records series, indicating for each the length of time it is to be maintained and its disposition" (ARMA International, 2007b, p. 22). Organizations have the option of issuing general retention guidelines for commonly held records, may prepare a customized program-specific schedule for electronic records that are unique to a particular department or unit, or a combination of both (Saffady, 2009).

According to Stephens and Wallace (2003), developing a retention schedule for electronic records offers three key benefits: (a) better overall management of stored data, (b) controlled growth of electronic records, and (c) reduced data storage costs (p. 10-11). Saffady (2009) identifies several additional benefits arising from the use of retention schedules:

- Ensures the availability and utility of records for an appropriate period of time so they may be referenced or reprocessed.
- Ensures compliance with recordkeeping requirements mandated by statute or regulation.

- Prevents the unauthorized or arbitrary destruction of records.
- Identifies records that do have long-term organizational or other secondary value.
- Prevents the needless accumulation of obsolete records and information, in so doing, eliminating the possibility that such content will be used in error (p.114).

Retention periods and corresponding schedules will need to be determined for every document managed within the information systems used by the organization (Adam, 2008). Ideally the retention, and ultimately deletion where appropriate, should occur automatically (Adam, 2008). Herein lays the challenge. More often than not, electronic information systems are not designed with record retention considerations in mind (ARMA International, 2010c). They either cannot delete discrete data sets or were not designed to hold large volumes of data for the long-term (ARMA International, 2010c). Both Adam (2008) and Saffady (2009) see the solution in the proper leveraging of records management application software and systems to accomplish this needed goal.

Practice #18: Leverage records management application software. One characteristic that separates records management application software from other electronic information systems is its ability to execute record retention rules on the records and information it manages instead of simply storing the content (Saffady, 2009). Adam (2008) also culls out retention as a distinctive feature of true electronic record management systems, or ERMS, and identifies several additional basic components:

- A repository – All ERMS will need a repository to store the records added to the system. Physically, the repository is located on one or more networked database servers even though the users will typically see a single, central repository. Based on access, users should have the ability to browse the repository for records.

- Hierarchical folder structures – The ERMS folder structure systematically categorizes where the records will exist within the system. The ERMS will need to support a hierarchical folder structure so that it can capture the file plan in an electronic form.
- Classification, indexing, and metadata – All records in the ERMS need to be categorized and indexed within the folder structure and use metadata to assist retrieval.
- Capture and declaration of records – The ERMS needs a method to automatically capture and declare records. Automation is essential to ensure that as documents become finalized they are declared as the official records of the organization in a timely fashion. Auto-declaration will keep user error from creeping into or even corrupting the process.
- Security – The ERMS must employ strict security protocols to not only protect the records, but to assist the organization in meeting its compliance needs.
- Management of physical records – The ERMS should centralize the management of all records, not just the electronic content. Centralization of records information allows users to locate records regardless of media and improves the overall accessibility of needed information.
- Search and retrieval – The ERMS should offer users multiple ways to locate needed records, be they physical or electronic.
- Auditing and reporting – The ERMS should allow authorized users and administrators to check and produce audit trails based on accessed and changes, dates created, dates modified and other criteria. Reporting capabilities will need to be flexible to support the evolving needs of the organization.

- Compliance with standards – For an ERMS to be compliant and legally accountable, the system must be designed to the standards, regulations and laws relevant to or required by the organization.
- Scanning and imaging – One of the main business drivers leading to the implementation of an ERMS is the need to provide users with instant access to centrally held records and information. Scanning and imaging functionality allow paper-based records to be easily incorporated into the ERMS management and access structure.
- Collaboration – Collaborative functionality allows users to communicate, work and share valuable organizational information regardless of physical location. As the primary task of the ERMS is to manage records and facilitate access to information, including functionality to encourage information sharing is consistent with this task.
- Workflow – Workflow processes, also referred to as business process management or BPM, automatically routes records and work in progress to necessary parties facilitating information access and organizational efficiencies (p. 17-20).

Though the line separating records management applications from other information management systems is not as defined as it once was, primarily resulting from evolving standards and legislation and advancements in technology (Adam, 2008), these basic components combined with retention are needed for effective electronic RIM (ARMA International, 2010c; Saffady, 2009; Stephens & Wallace, 2003).

Practices related to the requirements of the GARP® *Principle of Disposition*.

Retention periods identify the length of time an organization will maintain the records it creates and receives (ARMA International, 2009e). Once the retention requirement has been fulfilled, disposition represents the final administrative task the organization undertakes with regard to its records (ARMA International, 2009e). Though disposition does include deletion/destruction, this is not the only option, and the records may be transferred to another entity or preserved permanently (ARMA International, 2009e).

Practice #19: Combine IT and RIM support efforts. Properly carried out, record disposition occurs as part of the normal organizational business processes (ARMA International, 2009e). To do this effectively, RIM and IT professionals will need to work together. In most organizations, these professionals already support electronic recordkeeping systems and storage, and ARMA International (2009e) identifies several RIM and IT actions and support efforts that should be combined for effective dispositions:

- Storage of record and the associated metadata throughout the lifecycle
- Capture of audit trails for all changes, additions and deletions
- Media and storage location independent capture of records during active and inactive stages of use
- Application of retention and disposition rules to information held in various electronic repositories
- Identification and tracking of record formats and location(s)
- Accommodation of verification mechanisms for records to be dispositioned
- Maintain disposition in the records management system

- Accommodation of various types of electronic record dispositions including deletion, media destruction, transfer to archival storage devices including permanent storage
- Development of migration strategies in support of long-term or permanent retention

With the basic support structures aligned, record dispositions can occur efficiently. However, for record disposition to occur correctly and in a compliant manner, dispositions must occur based on the retention schedule and all actions and decisions should be documented, reviewed and authorized (ARMA International, 2009e).

Practice #20: Implement a litigation hold process. While the destruction of records is allowable under normal circumstances (Lewis Owens as cited in Brown, 2007), there have been attention-grabbing headlines dealing with the deletion of documents and electronic discovery issues (Gibson as cited in Adler, Howard & Lona, 2007). What these headlines typically fail to mention is the process for avoiding such sanctions: implementing litigation holds (Gibson as cited in Adler et al., 2007).

The 2009 amendments to the Federal Rules of Civil Procedure made it clear that organizations have a duty to preserve and produce electronically stored information (ESI) relevant to litigation as soon as such litigation is reasonably expected (Ward, Purwin, Sipior & Volonino, 2009). To meet this requirement, organizations must suspend the routine destruction of all relevant information, a process referred to as a *litigation hold* (Ward et al., 2009).

For the litigation hold to be successful, and to protect the organization from sanctions, the process should be systematic and include standardized procedures (Gibson as cited in Adler, Howard & Lona, 2009). Gibson (as cited in Adler et al., 2009) has identified the minimum procedures, based on best practices, which must be included in the legal hold process:

- Identification of relevant ESI and its likely locations

- Identification of record and information custodians who should be notified
- Notification to IT of what ESI should be preserved
- Notification to individual custodians
- Enforcement, including acknowledgement by IT and custodians of their compliance
- Verification of ESI preservation and suspension of automatic deletion where appropriate
- Routine updates and reminders of the legal hold
- Tracking of the legal holds, the ESI subject to legal holds, and custodians subject to legal holds
- Processes for removing legal holds (p. 121).

While the individual procedures may vary, overall the organization should follow the same approach to ensure that preservation obligations are met consistently (Gibson as cited in Adler et al., 2009).

Practice #21: Implement a discovery compliant records management policy. Having a litigation legal hold process by itself is not enough. Ward et al. (2009) cite the development of a well-conceived electronic records management policy, which takes into consideration the possibility of electronic discovery, as essential for record deletion to be considered routine. Typically, only routine, normal course of business disposition processes are deemed compliant with the requirements under the amended Federal Rules of Civil Procedure (Ward et al., 2009).

Fundamental to the development of this policy is an understanding of the discovery process and how it impacts the organization, its systems, storage devices, and operations (Ward et al., 2009). Each organization will need to set its own priorities and develop a plan that address identified objectives and capabilities (Ward et al., 2009). Specificity is essential, and

documentation of retention, storage devices, destruction methods, and disposal is required for each type of ESI (Ward et al., 2009).

Once the policy has been developed and implemented, it must be communicated to employees (Ward et al., 2009). To ensure understanding and compliance with the policy, training, policy reminders, and monitoring should be built into business processes (Ward et al., 2009). For the policy to be defensible the organization will need to demonstrate these actions through audits and the regular examination and updating of the policy as technology and organizational needs change (Ward et al., 2009).

With the procedures and monitoring in place, record and information disposition can occur as normal (Lewis Owens as cited in Brown, 2007; Ward et al., 2009). When litigation is anticipated, the structure exists to effectively demonstrate the good faith efforts of the organization should an inadvertent deletion of ESI occur (Ward et al., 2009). While these efforts will not eliminate the risks of litigation, the consequences of not taking the time and effort to address these issues are far more significant (Gibson as cited in Adler et al., 2009).

Practices related to the requirements of the GARP® *Principle of Transparency*.

In order for organizations to demonstrate compliance with internal and external recordkeeping requirements, and so that stakeholders can have confidence in organizational record creation and maintenance, transparency is needed (ARMA International, 2009d). This means that both the recordkeeping system and the organization processes surrounding the records management function be clearly defined, accurate, reasonable, and apparent to all interested parties (ARMA International, 2010c).

Practice #22: Establish data provenance queries. To achieve transparency from a system perspective, clearly designed workflows, well-defined inputs and outputs, and an open and discernable structure are required (ARMA International, 2010c). Transparency is needed so that users, reviewers, auditors and regulators are able to verify that the processes that resulted in a set of information comply with various requirements, that the results were derived independently from restricted sources, and that the information was captured with precision (Moreau, Groth, Miles, Vazquez-Salceda, Ibbotson, Jiang, Munroe, Rana, Schreibner, Tan, & Varga, 2008). Traditionally however, electronic data sources do not contain the supporting historical information needed to assist the various constituencies in these roles (Moreau et al., 2008).

To address the limitations of traditional data systems Moreau et al. (2008) propose that computer applications should be made provenance-aware so that data provenance is retrievable for analysis by users. Building from traditional definitions of provenance, Moreau et al. define data provenance as, "the source (or derivation) of an object and the record of the derivation" (p. 54). To achieve data provenance as defined, it is necessary to capture a variety of additional information describing what occurred at all stages of data execution (Moreau et al., 2008). A provenance-aware application creates and captures the necessary process documentation and stores it in a "provenance store" with persistent, long-term storage (Moreau et al., 2008, p. 55). Depending on the needs and resources of the organization, the provenance store can be a single, independent service or a more scalable federation of distributed stores (Moreau et al., 2008).

Once the data provenance information is captured, users can query the provenance store for specific data items related to the documented events associated with a data set (Moreau et al., 2008). With the full provenance of the data set available, users will be able to determine the

materials and data sources used in creating a set of information, and if required the provenance of those sources as well (Moreau et al., 2008). By having the full and transparent history of the information created and used by the organization, stakeholders will gain confidence in the data, its sources, and the associated processes (Moreau et al., 2008). This transparency thereby results in confidence in the organization itself (ARMA International, 2010c).

Practice #23: Adopt the "Information Management Compliance" methodology. Transparency of organizational processes surrounding the records management function is as important as the transparency of information systems (ARMA International, 2010c), and is essential for organizations to meet their obligations in a compliant manner (Kahn & Blair, 2009). Kahn and Blair (2009) posit that, in the aftermath of the corporate scandals at the turn of the 21st century, the proper management of records and information has become inextricably linked with organizational accountability and transparency. This is because organizational accountability and transparency are dependent upon reliable records (Kahn & Blair, 2009) as only reliable records can demonstrate that the organization has taken clear, appropriate, and compliant actions (ARMA International, 2010c).

To achieve appropriate levels of transparency throughout the organization, a comprehensive strategy is needed. Kahn and Blair (2009) introduce their methodology entitled *Information Management Compliance* (IMC) to achieve comprehensive and compliant information management practices, and in so doing, achieve the transparency outlined by GARP®. Based on the Federal Sentencing Guidelines, Kahn and Blair (2009) identify the "keys" that make up the IMC methodology:

- Good policies and procedures
- Executive-level program responsibility

- Proper delegation of program roles and components
- Program communication and training
- Auditing and monitoring to measure program compliance
- Effective and consistent program enforcement
- Continuous program improvement

A close read of the Kahn and Blair IMC methodology demonstrates significant alignment with the ARMA GARP® principles in their entirety. When the requirements of the GARP® *Principle of Transparency* are achieved, the final essential element of the necessary framework is attained, thereby creating a cohesive recordkeeping management program.

References

ACM, Inc. (2010). *ACM Fact Sheet – About ACM*. Retrieved May 17, 2010 from http://www.acm.org/about/fact_sheet

Adam, A. (2008). *Implementing electronic document and record management systems*. New York, NY: Auerbach Publications.

Adler, G., Howard, G. & Lona, M. (Eds.). (2007, October). *Electronic discovery and retention guidance for corporate counsel 2007.* New York, NY: Practising Law Institute.

Adler, G., Howard, G. & Lona, M. (Eds.). (2009, October). *Electronic discovery guidance 2009: What corporate and outside counsel need to know.* New York, NY: Practising Law Institute.

American National Standards Institute. (n.d.). About ANSI overview. Retrieved May 6, 2010 from http://www.ansi.org/about_ansi/overview/overview.aspx?menuid=1

ARMA International. (2003). *Vital records programs: Identifying, managing and recovering business critical records (ANSI/ARMA 5-2003)*. Lenexa, KS: ARMA International.

ARMA International. (2004). *Requirements for managing electronic messages as records (ANSI/ARMA 9-2004)*. Lenexa, KS: ARMA International.

ARMA International. (2005). *Establishing alphabetic, numeric, and subject filing systems (ANSI/ARMA 12-2005).* Lenexa, KS: ARMA International.

ARMA International. (2007a). *The digital records conversion process: Program planning, requirements, procedures (ANSI/ARMA 16-2007)*. Lenexa, KS: ARMA International.

ARMA International. (2007b). *Glossary of records and information management terms, 3rd edition.* Lenexa, KS: ARMA International.

ARMA International. (2007c). *Procedures and issues for managing electronic messages as records (ANSI/ARMA TR 02-2007)*. Lenexa, KS: ARMA International.

ARMA International. (2007d). *Records management responsibility in litigation support*. Lenexa, KS: ARMA International.

ARMA International. (2008). *Job descriptions for records and information management.* Lenexa, KS: ARMA International.

ARMA International. (2009a, April 1). *ARMA International challenges organizations to implement better recordkeeping* [Press release]. Retrieved April 13, 2010 from http://www.arma.org/press/Pdf/GARP_Media_Release.pdf

ARMA International. (2009b). *Evaluating and mitigating records and information risks*. Lenexa, KS: ARMA International.

ARMA International. (2009c). *Contracted destruction for records and information media*. Lenexa, KS: ARMA International.

ARMA International. (2009d). *The generally accepted recordkeeping principles (GARP®)* [full version]. Retrieved March 30, 2010, from http://www.arma.org/garp/garp.pdf

ARMA International. (2009e). *Records and information management for information technology professionals*. Lenexa, KS: ARMA International.

ARMA International. (2009f). *Using DoD 5015.2-STD outside the federal government sector.* Lenexa, KS: ARMA International.

ARMA International. (2010a). *ARMA International Maturity for Information Governance* [a.k.a. GARP® Maturity Model]. Retrieved May 15, 2010 from http://www.arma.org/garp/Garp%20maturity%20Model.pdf

ARMA International. (2010b) ARMA.org help – General ARMA – What does ARMA stand for? Retrieved May 6, 2010 from http://www.arma.org/help/index.cfm

ARMA International. (2010c) *Course notes: Generally accepted recordkeeping principles®: Overview* [Online course handouts]. Retrieved May 25, 2010 from http://www.courses.learnsomething.com/scormcourses/o5642c9adab5b4668a3e5d59ba5bbdf18/p62ab316db617435e999f6e420a7bc86d/data/resources/GARP%20Course%20Notes%5fFinal%5f2010%2d4%2d30%2epdf?download=true

ARMA International. (n.d.). Generally accepted recordkeeping principles®: Overview online course. Retrieved May 10, 2010 from http://www.arma.org/learningcenter/onlinecourses/garp.cfm

AXS-One, Inc. (2007). *Change to the federal rules of civil procedure – Understanding the impact on your organization* [White paper]. Retrieved April 17, 2010 from http://www.axsone.com/pdf/FRCP_V8_2007.pdf

Baye, L. (2007) Strategies for implementing information security systems. In P. Brown (ed.), *Information technology law institute: Systems security, record retention and the rise of information life cycle management.* New York, NY: Practising Law Institute.

Bell, C. & Smith, T. D. (2009, May 19). *Critical evaluation of information sources*. Retrieved April 26, 2010 from UO Libraries: http://libweb.uoregon.edu/guides/findarticles/credibility.html

Brown, P. (Ed.). (2007, March). *Information technology law institute: Systems security, record retention and the rise of information life cycle management.* New York, NY: Practising Law Institute.

Burns, R. & Peterson, Z. (2010). Security constructs for regulatory-compliant storage. *Communications of the ACM*, *53*(1), 126-130. Retrieved April 1, 2010, from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=buh&AN=47220623&loginpage=Login.asp&site=ehost-live&scope=site.

Busch, De Maret, Flynn, Kellum, Le, & Meyers. (2005). Conceptual analysis. Colorado State University Writing Guide. Retrieved from http://writing.colostate.edu/guides/research/content/com2b1.cfm

BusinessDictionary.com. (2010a) *Accuracy*. Retrieved May 8, 2010 from http://www.businessdictionary.com/definition/accuracy.html

BusinessDictionary.com. (2010b) *Availability*. Retrieved May 8, 2010 from http://www.businessdictionary.com/definition/availability.html

BusinessDictionary.com. (2010c). *Best practice*. Retrieved April 17, 2010 from http://www.businessdictionary.com/definition/best-practice.html

BusinessDictionary.com. (2010d). *Compliance*. Retrieved April 24, 2010 from http://www.businessdictionary.com/definition/compliance.html

BusinessDictionary.com. (2010e). *Consistent*. Retrieved May 8, 2010 from http://www.businessdictionary.com/definition/consistent.html

BusinessDictionary.com. (2010f). *Governance*. Retrieved May 9, 2010 from http://www.businessdictionary.com/definition/governance.html

BusinessDictionary.com (2010g). *Practice*. Retrieved June 12, 2010 from http://www.businessdictionary.com/definition/practice.html

BusinessDictionary.com. (2010h) *Privacy*. Retrieved May 8, 2010 from http://www.businessdictionary.com/definition/privacy.html

BusinessDictionary.com. (2010i). *Requirements*. Retrieved April 24, 2010 from http://www.businessdictionary.com/definition/requirements.html

BusinessDictionary.com. (2010j). *Transparency*. Retrieved April 24, 2010 from http://www.businessdictionary.com/definition/Transparency.html

Chosky, C. (2008). Where RM should report to ensure effective electronic records management. *The Information Management Journal, 42(2),* 58-61.

Creswell, J. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches, 3rd Edition*. Thousand Oaks, CA: Sage Publications.

Determann, L. & Hwang, J.D. (2009). Data security requirements evolve: From reasonableness to specifics. *Computer & Internet Lawyer*, *26*(9), 6-17. Retrieved April 1, 2010, from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=buh&AN=43819063&loginpage=Login.asp&site=ehost-live&scope=site

Dictionary.com (2010). *Dictionary.com Unabridged* [iPad edition]. New York, NY: Random House Inc.

DLM Forum. (2008a). *MoReq2: Model requirements for the management of electronic records, v1.04*. Retrieved May 15, 2010 from http://www.dlmforum.eu/index.php?option=com_jotloader&view=categories&cid=10_f56391a0c9ea9456bf24e80b514f5dda&Itemid=36&lang=en

DLM Forum. (2008b). *MoReq2: Model requirements for the management of electronic records, v1.04 Appendix 9 – Metadata model*. Retrieved May 15, 2010 from http://www.dlmforum.eu/index.php?option=com_jotloader&view=categories&cid=10_f56391a0c9ea9456bf24e80b514f5dda&Itemid=36&lang=en

DLM Forum. (2009). *About the DLM forum – History and traditions*. Retrieved May 15, 2010 from http://www.dlmforum.eu/index.php?option=com_content&view=article&id=13&Itemid=14&lang=en

Doyle, J., Viktor, H., & Paquet, E. (2009). Long-term digital preservation: Preserving authenticity and usability of 3-D data. *International journal on digital libraries, 10(1),* 33-47. Retrieved May 16, 2010 from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=cph&AN=38608860&loginpage=login.asp&site=ehost-live&scope=site

Etalle, S. & Winsborough, W.H. (2007, June) A posteriori compliance control. *Proceedings of the 12th ACM symposium on access control models and technologies (SACMAT),* p.11-20. Retrieved June 24, 2010 from http://doi.acm.org/10.1145/1266840.1266843

Fresko, M. (2008, July). MoReq2: The new model for developing, procuring electronic records management systems. *The Information Management Journal, 42(4),* p 62-66.

Gable, J. (2002, November). Everything you wanted to know about DoD. *The Information Management Journal, 36(6),* p 32-38.

Gibson, S.M. (2007). Litigation holds: Turning on – and off – the switch to avoid sanctions and costly e-discovery blunders. In G.A. Adler, G.M. Howard and M.A. Lona (eds.), *Electronic discovery and retention guidance for corporate counsel 2007.* New York, NY: Practising Law Institute.

Gibson, S.M. (2009). Six steps to litigation readiness. In G.A. Adler, G.M. Howard & M.A. Lona (eds.), *Electronic discovery guidance 2009: What corporate and outside counsel need to know.* New York, NY: Practising Law Institute.

Hayden, L. (2009, November). Designing common control frameworks: A model for evaluating information technology governance, risk and compliance control rationalization strategies. *Information security journal: A global perspective, 18(6)* 297-305. Retrieved May 16, 2010 from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=cph&AN=49232884&loginpage=login.asp&site=ehost-live&scope=site

International Organization for Standardization. (2001a). *Information and documentation – Records management part 1: General (ISO 15489-1)*. Geneva: ISO.

International Organization for Standardization. (2001b). *Information and documentation – Records management part 2: Guidelines (ISO TR 15489-2)*. Geneva: ISO.

International Organization for Standardization. (2010a). About ISO. Retrieved May 8, 2010 from http://www.iso.org/iso/about.htm

International Organization for Standardization. (2010b). Discover ISO. Retrieved May 8, 2010 from http://www.iso.org/iso/about/discover-iso_isos-name.htm

International Organization for Standardization. (2010c). ISO – FAQs – Information security. Retrieved May 11, 2010 from http://www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/information_security.htm

Interwoven, Inc. (2004). *Zubulake v. UBS – The significance for records management: New risks-New remedies* [White paper]. Retrieved April 17, 2010 from http://www.interwoven.com.cn/documents/whitepapers/wp_zub.pdf

Kahn, R. & Blair, B. (2005). *Information nation warrior: Information management compliance bootcamp*. Silver Spring, MD: AIIM.

Kahn, R. & Blair, B. (2009). *Information nation: Seven keys to information management compliance, second edition*. Indianapolis, IN: Wiley Publishing Inc.

Kamel, I. (2009). A schema for protecting the integrity of databases. *Computers & Security, 28*(7), 698-709. Retrieved April 1, 2010, from Computer Source Database.

Kennedy, J.B. & Kennedy, A.E. (2007). Legal aspects of data migration: Data security and preservation requirements that companies should know about. In P. Brown (ed.), *Information technology law institute: Systems security, record retention and the rise of information life cycle management.* New York, NY: Practising Law Institute.

Launchbaugh, C. (2004). E-Records management: A sad state of affairs or golden opportunity? *The Information Management Journal, 38(5),* 48-52.

Leedy, P. & Ormrod, J. (2005). *Practical research: Planning and design 8th Edition*. Upper Saddle River, NJ: Pearson Merrill Prentice Hall.

Lewis Owens, L. (2007). Ethical issues arising from corporate record retention. In P. Brown (ed.), *Information technology law institute: Systems security, record retention and the rise of information life cycle management.* New York, NY: Practising Law Institute.

Marcella, A. (2008). Electronically stored information and cyberforensics. *Control: The ISACA Journal [Online Edition], 5*. Retrieved March 31, 2010 from http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=52106&TEMPLATE=/ContentManagement/ContentDisplay.cfm

Mattox, A. (2007). Solving the unmanaged content conundrum. *The Information Management Journal, 41(6),* 60-63.

Moreau, L., Groth, P., Miles, S., Vazquez-Salceda, J., Ibbotson, J., Jiang, S., Munroe, S., Rana, O., Schreibner, A. Tan, V., & Varga, L. (2008). The provenance of electronic data. *Communications of the ACM, 51*(4), 52-58. Retrieved April 1, 2010, from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=buh&AN=31663006&loginpage=Login.asp&site=ehost-live&scope=site

Obenzinger, H. (2005). *What can a literature review do for me?* Retrieved March 30, 2009 from Stanford University: http://ual.stanford.edu/pdf/uar_literaturereviewhandout.pdf

OneSearch. (n.d.). *UO Libraries*. Retrieved April 26, 2010 from http://onesearch.uoregon.edu/databases/database/ORG00265

Padayachee, K. & Eloff, J.H.P. (2009). Adapting usage control as a deterrent to address the inadequacies of access controls. *Computers & Security*, *28*(7), 536-544. Retrieved April 1, 2010, from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=cph&AN=44469629&loginpage=login.asp&site=ehost-live&scope=site

Paylago, S.U. (2007). Introduction to information security programs. In P. Brown (ed.), *Information technology law institute: Systems security, record retention and the rise of information life cycle management.* New York, NY: Practising Law Institute.

Penn, I., Pennix G. & Coulson, J. (1994). *Records management handbook, 2nd Edition*. Burlington, VT: Ashgate.

Practising Law Institute. (2010). *About PLI*. Retrieved May 15, 2010 from http://www.pli.edu/public/about/default.asp

Robek, M., Brown, G. & Stephens, D. (1995). *Information and records management: Document-based information systems, 4th Edition*. Woodland Hills: Glencoe/McGraw-Hills Forth

Saffady, W. (2009). *Managing electronic records, 4th Edition.* Lenexa, KS: ARMA International.

The Sedona Conference®, (2007, March*). Best practices commentary on the use of search & information retrieval methods in e-discovery.* Retrieved May 28, 2010 from http://www.thesedonaconference.org/content/miscFiles/publications_html

The Sedona Conference®, (2007, November). *The Sedona guidelines: Best practice guidelines & commentary for managing information & records in the electronic age, Second edition.* Retrieved May 8, 2010 from http://www.thesedonaconference.org/content/miscFiles/publications_html

The Sedona Conference®, (2008, March). *Commentary on ESI evidence & admissibility.* Retrieved May 28, 2010 from http://www.thesedonaconference.org/content/miscFiles/publications_html

The Sedona Conference®, (2009, May). *Commentary achieving quality in the e-discovery process.* Retrieved May 28, 2010 from http://www.thesedonaconference.org/content/miscFiles/publications_html

Scholz, J. (2009). Securing critical IT infrastructure. *Information security journal: A global Perspective, 18(1),* 33-39. Retrieved May 16, 2010 from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=cph&AN=36353501&loginpage=login.asp&site=ehost-live&scope=site

Song, S. & JaJa, J. (2009). Techniques to audit and certify the long-term integrity of digital archives. *International Journal on Digital Libraries, 10*(2/3), 123-131. Retrieved April 1, 2010, from http://dx.doi.org/10.1007/s00799-009-0056-2

Stephens, D. O. (2001, July). The world's first international records management standard. *Information Management Journal,35(4)* 68-70.

Stephens, D. O. (2009). *The ten biggest issues in records management today* [PowerPoint slides]. Retrieved April 17, 2010 from www.armanortheast.org/TenBiggestIssuesinRMTodayWesternNYSeminar.ppt

Stephens, D. & Wallace, R. (2003). *Electronic records retention: New strategies for data Life cycle management*. Lenexa, KS: ARMA International

U.S. Department of Defense. (2007). *DoD5015.2-STD, Electronic records management software applications design criteria standard.* Retrieved March 31, 2010 from http://jitc.fhu.disa.mil/recmgt/p50152stdapr07.pdf

United States Government Accountability Office (2009). *Federal information system controls audit manual (FISCAM)*. [Washington, D.C.]: U.S. Govt. Accountability Office. Retrieved April 1, 2010, from http://www.gao.gov/new.items/d09232g.pdf.

United States Government Accountability Office (n.d.). *About GAO*. Retrieved May 25, 2010 from http://www.gao.gov/about/index.html

Ward, B., Purwin, C., Sipior, J., & Volonino, L. (2009). Recognizing the impact of e-discovery amendments on electronic records management. *Information Systems Management, 26(4),* 350-356. Retrieved May 16, 2010 from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=cph&AN=44820810&loginpage=login.asp&site=ehost-live&scope=site

Weitzner, D., Abelson , H., Berners-Lee, T., Feigenbaum, J., Hendler, J., & Sussman, G. (2008). Information accountability. *Communications of the ACM, 51*(6), 82-87. Retrieved April 1, 2010, from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=buh&AN=32801384&loginpage=Login.asp&site=ehost-live&scope=site

Wesleyan University Library. (2009). Writing a literature review [online tutorial]. Retrieved May 14 from http://www.wesleyan.edu/libr/tut/litrev/writing.html#general

(ISC)^2. (2010). *About (ISC)^2*. Retrieved May 16, 2010 from http://www.isc2.org/aboutus/default.aspx

Appendix A

Record of Preliminary Searches

Search engine / database	*Search terms*	*# of results*	*Quality*	*Comments*
Computer Source	data AND accountability	353	Good	This database produces consistently relevant and timely results. Most searches produce a fairly high number of results, including several irrelevant results. More recent searches, however, show very relevant articles.
	data AND governance	325	Good	
	data AND audit	673	Good	
	data AND integrity	881	Good	
	data AND media AND migration	28	Fair – there are a few potentially highly relevant sources	
	data AND security AND best practice	114	Good	
	data AND preservation	252	Good	
	data AND retention	439	Good	
	data AND preservation	252	Good	
	Records management	1234	Good	
	policy AND records	459	Good	
	policy AND best practice	106	Fair	
Bing	Electronic AND records management	84,700,000	Poor	This search engine is poor for general searches, it has been very useful for locating specific resources listed in bibliographies and for locating timely statistics and facts that support the topic

Google	Electronic AND records management	4,200,000	Poor	While this search engine is poor for general searches, it is very useful for locating specific resources listed in bibliographies and for locating timely statistics and facts that support the topic
Academic Search Premier	records AND best practice	257	Poor	Few relevant sources. May be useful for more specific searches.
Business Source Premier	records AND best practice	291	Poor – highly repetitive of Academic Search Premier	Few relevant sources. May be useful for more specific searches tied to specific business needs or processes.
	Electronic records AND management	4427	Poor – highly repetitive of Academic Search Premier and this researchers personal collection of RIM related resources	