*Ensuring the Preservation of Reliable Evidence: A Research Project Funded by the NHPRC**

by WENDY DUFF

Résumé

Le Projet de documents informatiques de l'Université de Pittsburgh, un projet d'une durée de trois ans, financé par la *National Historical Publications and Records Commission*, a identifié une série de dix-neuf conditions fonctionnelles afin d'établir la valeur testimoniale des documents électroniques. Cet article décrit les résultats du projet, ainsi que les exigences fonctionnelles requises pour la garde des documents, les règlements de production, les droits d'auteur, ainsi qu'un modèle méta-informationnel pour des communications et transactions courantes. Cet article fait également état des résultats d'une recherche sur les conséquences de la culture corporative sur les choix des tactiques d'implantation de ces conditions fonctionnelles ainsi que l'influence du droit d'auteur sur l'acceptation de ces conditions par les avocats, les vérificateurs, et de les techniciens de l'information.

Abstract

The University of Pittsburgh Electronic Records Project, a three year project funded by the National Historical Publications and Records Commission, identified a set of nineteen functional requirements for electronic evidence. This paper describes the Project's products, including the functional requirements for record-keeping, the production rules, literary warrant, and a metadata model for business-acceptable communications. The paper also reports on the results of research that investigated the effect of corporate culture on the choice of tactics to implement the functional requirements and the influence of literary warrant on the acceptance of functional requirements by lawyers, auditors, and information technologists.

The often heralded paperless office stands poised to revolutionize organizations as technology gradually overcomes the obstacles to its implementation. Local and wide area networks, client server architecture, electronic mail, and powerful work stations

have infiltrated offices, transforming them with each new technological advancement. The ubiquitous computer coupled with a telecommunications network provides the necessary infrastructure to decentralize the workplace, flatten hierarchical organizational structures, and empower employees by supplying them with the requisite tools for decision-making. These companies eliminate controls that once restricted actions and insured a steady and dependable, but static organization. The new technology "informates" staff, providing up-to-date information on a need-to-know basis, and creates a new knowledge-based workforce.[1] In striving to reach this goal, however, organizations often fail to establish the mechanisms required to ensure that evidence of their actions and decisions are captured and preserved. As new information replaces old, the records needed to ensure an organization's accountability and to maintain its corporate memory are lost.

Records, the fundamental instrument of business transactions, are mutating from a concrete, static, structured document to formless, dynamic data that resides in a computer's memory or on a disk. As records migrate from a stable paper reality to an intangible electronic existence, their physical attributes, vital for establishing the authenticity and reliability of the evidence they contain, are threatened.[2] Electronic records exist only as a series of electronic impulses or signals and the form or format they display is merely a view controlled by software functionality.[3]

Records are utilitarian in nature, and are created to fulfill a business function and document business processes. They are a valuable corporate asset because they provide managers with the ability to extend administrative control beyond their immediate environment by allowing them to know or experience an event without being physically present. They are created in the first instance to control or direct an organization and to help orient staff to a common goal or purpose. They have residual value because they document the outcomes of the directing and controlling activities and because they provide evidence of an organization's rights as well as its obligations to its staff and society.

For records to fulfill these roles, they must be readable, understandable, and trustworthy. Records preserved on a medium that is inaccessible or in a code that is indecipherable do not reveal any evidence of actions. Without access to the content of records (the words, numbers, symbols, and sounds), no information can be communicated, and the records have no value. Nevertheless, to read a record one must have access to more than just the data in the record; to interpret a record, the data must be organized into a structure that makes it understandable and a context that makes it meaningful.

The structure of the record is the form or format that organizes or structures the record and makes it understandable. The layout dictates the format of the data elements and reveals the relationships between them. In a paper world this information is presented implicitly through the layout of the record or the physical format and it may or may not be provided explicitly through the use of terms such as "To:" or "From:" in a memo. Electronic records may carry structural information in the pointers that link physically or logically distinct chunks of information. The elements may be kept in separate files and are brought together when rendered onto a screen or through the metadata.

The context or provenance of the records provides information concerning the business function or activity from which the records emanated. As Duchein has noted, "to appreciate a document it is essential to know exactly where it was created, in the framework of what process, to what end, for whom, when and how it was received by the addressee, and how it came into our hands."[4] This information may be communicated explicitly within the record through words, reference codes, or dates, as well as implicitly within the record-keeping system itself. The record-keeping system captures the documentary relationships between the records. It provides "evidence of how individual records were or could have been used with the record system and thus of what they meant within the context of the business process that they document."[5]

An example may help to illustrate. A receipt, a very common financial record, provides evidence of a payment of money or the transferring of funds. It normally captures the name of the payee, the name of the payer, the date the money was paid, the purpose of the payment or the kinds of services received, and the amount paid or transferred. The different data elements of the record are structured or presented on a paper receipt in a standard format which facilitates the reading of the record and enables someone to determine quickly who paid the money and who received it. The individual data elements may or may not be labelled. A receipt must also identify the function, activity, and transaction that caused it to be created or it is meaningless. Moreover, an understanding of its relationships with other records, and how it was indexed, copied, and transmitted is essential to comprehend the record's meaning.

Computer systems were originally designed to perform mathematical computations, tabulate ballots, predict the weather, and make atomic energy calculations. Consequently, the first generation of electronic records consisted of large machine-readable statistical and survey data files. As Terry Cook has suggested, the genesis of electronic records gave rise to theoretical discourses and appraisal practices that emphasized the informational value rather than the evidential value of electronic records and led to the development of procedures and techniques that preserved the data but not the records' structure and context.[6] Computer systems have evolved from the days of mainframes and number crunching to their current primary function of creating and processing documents or records. Frank Gilbane, president of Publishing Technology Management, estimates that currently "at least 80% of corporate electronic information is in the form of documents, as opposed to structured database records."[7] Unfortunately, systems that create and maintain electronic documents often fail to preserve the structure or the context essential for the evidentiary nature of records. This problem is exacerbated when the data in records are moved to a new system but the context and structure are left behind. Migrating records to a new software environment proves detrimental, because as David Bearman has pointed out,

> As long as the information created in the course of work in an electronic environment remains in the software and hardware system in which it was created, it loses none of the contextual information which is critical to its meaning, but the transition, or "migration" of data to a new environment threatens to change the way the information looks, feels or operates, and hence what it means.[8]

The challenges presented by electronic records led the National Association of Government Archives and Records Administrators' (NAGARA) Advanced Institute for Government Archivists to conclude that "archival management of electronic records is probably the most important, and certainly the most complicated, issue currently before the archival profession."[9]

NHPRC's Initiatives to Address Electronic Records Issues

In 1990, staff of the National Historical Publications and Records Commission (NHPRC) studied the issues presented by electronic records and reported that managing electronic records is problematic for three reasons: 1) electronic information is system dependent; 2) electronic information exists on fragile media; and 3) electronic information can be easily erased or changed. Their report posited that "[t]he politics of getting archivists involved in these activities is the first challenge and the difficulties encountered in doing so are related to the archivist's traditionally perceived role as passive custodian and to a general feeling of being undervalued by colleagues."[10] To address the difficulties that arise from the traditional position archivists hold in the organizational hierarchy, it called for "[s]trategies and approaches that provide archivists with the tools to position themselves better in complex organizations to address electronic recordkeeping issues."[11] The report acknowledged the opportunities that electronic records present and suggested archivists seize this opening to build alliances with other professionals. It advised archivists to forge partnerships with lawyers, accountants, programme managers, and information resource management professionals who "are also concerned with many of these issues."[12] It recommended NHPRC take an active role in funding projects dealing with electronic records issues, and suggested the Commission start by organizing a national invitational planning conference to develop a research agenda.

Establishing a Research Agenda to Address Electronic Records Issues

In 1991, the Commission organized a national conference that brought together forty-six individuals from a variety of backgrounds to identify areas of research. The group identified the following ten research questions, listed in priority order:

1. What functions and data are required to manage electronic records in accord with archival requirements? Do data requirements and functions vary for different types of automated techniques?
2. What are the technological, conceptual, and economic implications of capturing and retaining data, descriptive information, and contextual information in electronic form from a variety of applications?
3. How can software-dependent data objects be retained for future use?
4. How can data dictionaries, information resource directory systems, and other metadata systems be used to support electronic records management and archival requirements?
5. What archival requirements have been addressed in major system development projects and why?

6. What policies best address archival concerns for the identification, retention, and preservation, and research use in electronic records?
7. What functions and activities should be present in electronic records programmes and how should they be evaluated?
8. What incentives can contribute to creator and user support for electronic records management concerns?
9. What barriers have prevented archivists from developing and implementing archival electronic records programmes?
10. What do archivists need to know about electronic records?[13]

The report recommended the NHPRC fund studies to answer the first three questions, prior to funding research on the last seven. NHPRC accepted the research agenda and it became the foundation for evaluating grant applications for electronic records research.[14]

University of Pittsburgh Electronic Records Project

Responding to the research agenda, the University of Pittsburgh applied for, and subsequently received, a grant of $360,000 to conduct a three-year research project on electronic records (referred to as the Pittsburgh Project). The Project responded to the first three questions in the research agenda and articulated five separate areas of study:

1. Record-keeping functional requirements for electronic information systems;
2. Variables in organizations that affect the way in which both software and hardware are utilized and which may affect the degree to which archival functional requirements can be adopted;
3. Technical capabilities of organizational software products to satisfy archival requirements;
4. Other means, such as policy and standards, to satisfy archival functional requirements;
5. Effectiveness of technology and policy strategies to ensure that archival interests can be met.[15]

The Project began by conducting an extensive literature review and assembling an Advisory Group of Experts to develop a draft set of functional requirements for record-keeping (see **Appendix**). The requirements are elements necessary to ensure the preservation of evidence in electronic form and not the application requirements for archival or records management systems. The draft requirements were circulated to over one hundred archivists, record managers, and other information professionals and disseminated through conferences, workshops, and a number of publications. Based on comments and suggestions received from the community, the Project revised the requirements and, now in their final form, they serve as elements needed to ensure that credible records are captured, maintained, and used.

These requirements are system independent and could be implemented in either a manual, electronic, or hybrid system. Although identified by experts, the requirements derive from laws, regulations, and best practices of society. The thirteen requirements for record-keeping are grouped into three different categories:

- requirements that relate to the organization—labelled *Conscientious Organization*;
- requirements reflecting specifications for record-keeping systems—classified as *Accountable Record-keeping Systems*;
- requirements that relate to the record—these are grouped in three sub-categories: *Records-Captured*; *Records-Maintained*, and *Records-Usable*.

Conscientious Organization

To ensure an organization's system meets its regulatory obligations, an organization must first identify all relevant legal and administrative requirements with which it must comply. Therefore *Compliant* specifies that an organization must know the laws, regulations, and best practices that have authority over their environment. The records must be linked to a retention rule that references applicable laws and regulations. Updates to the laws, regulations, etc., should be monitored and changes incorporated into current record-keeping instructions. For example, if an organization has a research and development (R&D) function, that is, it invents things and applies for patents, it must comply with stringent procedures for record-keeping. Failure to produce records required to document the procedures may result in the loss of the patent if the organization's right to the patent was challenged in court. To acquire a patent successfully, one must prove the date he/she originally thought of the invention and that she/he has worked on it ever since. In one of the organizations that the Project visited, the patent lawyer, dictated by the law and jurisprudence, requires all scientists in the organization to complete a daily log book of their activities. The day's events are laboriously recorded by hand and all lab books are carefully controlled through a number of detailed procedures. The scientists would like to use electronic lab books, but until the company's lawyer is confident that an electronic system could meet all the requirements for legally admissible records he will veto this substitution.

Not all requirements are regulated by law, however; some are dictated by standards boards or derived from best practices. Today, an organization wishing to become registered as an ISO 9000 company (an important certification for companies conducting business in Europe) must prove, by means of an audit, that it complies with the ISO 9000 guidelines. These guidelines include many references to creating and maintaining records. For example, clause 4.16 of ISO 9001 states that "all quality records shall be legible, and identifiable to the product involved. Quality records shall be stored in such a way that they are readily retrievable in facilities that provide a suitable environment to minimize deterioration or damage and to prevent loss."[16] James Lamprecht suggests that of all the ISO 9000 specifications "the most difficult paragraphs to comply with (at least for many companies), deal with document approval, issue, changes, and modifications."[17]

Accountable Record-keeping Systems

The environment in which records reside can either increase or decrease their reliability and trustworthiness. The courts bestow a high degree of trust in records that are "kept in the regular course of business activity ...as shown by the testimony of the custodian or other qualified witness, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness."[18] The admissibility of records depends upon testimony that verifies the integrity and reliability of the record-keeping system that controlled them. Therefore, the requirements in the second group delineate specifications for the record-keeping system and are labelled *Responsible, Implemented,* and *Consistent. Responsible* describes the need for systems to have documented policies and assigned responsibilities. The methods employed by a system must be defined by routine tasks and the system must have specified procedures for situations in which the primary system fails. *Implemented* refers to the need for a system to be exclusively employed in the normal course of business. It also states that no transaction can take place outside the documented record-keeping system, thereby restricting transactions to a designated system. *Consistent* addresses the consistency of records and specifies that identical processes produce identical outcomes and that the executable system's logic is demonstrable outside of the system.

Records

The requirements in the third category specify characteristics that records must have and are arranged into three subgroups: *Captured Records, Maintained Records*, and *Usable Records.*

Captured Records

Captured records must be *Comprehensive, Identifiable, Complete*, and *Authorized.* The *Comprehensive* requirement states that records must be created for all business transactions. If the creation of records is arbitrary rather than comprehensive, it casts doubts about why a particular record exists and therefore calls into question the credibility of the records. Although a record must be captured for all transactions, its preservation is not required. The second requirement in the group, *Identifiable*, states that a record must be unique and linked to the transaction that it represents. It must bind together all the parts of the record or all the data that was used by a particular transaction. The third requirement in the category of *Captured Records* is *Complete*, and it specifies that a record must be *Accurate, Understandable*, and *Meaningful. Accurate* states that the data in the record accurately reflect the data of the transaction. *Understandable* requires that the system ensures that the relationships between elements are represented in a manner that communicates the record's intended meaning and that the system supports the software functionality invoked by data values. *Meaningful* specifies that information needed to understand correctly the transaction that created and used the record be linked to the record.

The final requirement under the rubric of *Captured Records* is *Authorized.* To fulfil this requirement, records must emanate from an identified source that has authority to create records or to carry out transactions. Records created by someone lacking the required authority are not valid records of an organization. Accordingly, a cheque or contract signed by someone without appropriate signing authority would not be legally binding.

Maintained Records

Once records are captured, they must be maintained over time. Therefore, the functional requirements for record-keeping contain specifications for migrating records to new hardware and software environments. To be preserved, records must maintain their content, structure, and context regardless of the software and hardware controls under which they exist. Therefore, the functional requirement *Preserved* is divided into three separate sub-requirements: *Inviolate, Coherent,* and *Auditable. Inviolate* specifies that the content of the record must be protected from damage or destruction and that no alteration or modification is permitted. If changes are made, a new record is created. *Coherent* dictates that the record must be reconstructible when migrated to new software environments and the logical boundaries of the record preserved. *Auditable* states that all uses of the record are transactions and these uses must be documented by means of an audit trail.

The final requirement under the category *Preserved* is *Removable* and it specifies that records must be removable only by authorized individuals who can delete the content and structure of records but not their contextual audit trails.

Usable Records

The last group of requirements relates to characteristics required for a record to be usable over time. The first, *Exportable*, relates to the software independence of the records and specifies that the records must be portable from one system to another without loss of information. The second requirement in this category, *Accessible*, establishes the need for the system to output the record's content, structure, and context and consists of the three sub-requirements *Available, Renderable*, and *Evidential. Available* specifies that the system must be able to retrieve the record. *Renderable* requires that the system renders or outputs records as they first appeared when captured or in a way that a person can translate how they first appeared. *Evidential* specifies that a human readable audit trail which documents a record's creation and use must accompany it. Finally the record must be *Redactable,* which means that the system must be able to mask part of the record. This last requirement is particularly important for systems that carry personal or proprietary information.

Production Rules

David Bearman and Ken Sochats, two members of the Project staff, have borrowed a technique from the field of artificial intelligence to express formally each functional requirement in the language of production rules. This formal language enabled the

Project to state each specification in such a way that it is recognizable as well as observable, and therefore can be tested when implemented in a system. The production rules also ensure that the specifications have the following characteristics:

- unambiguous, rather than abstract;
- as precise as possible;
- consistency of expression;
- defined to a specificity that is measurable.[19]

The production rules provide a measure for testing the degree to which record-keeping systems comply with the requirements.

Metadata Model

David Bearman, the Project's consultant, has used the production rules and functional requirements to delineate the type of metadata that should accompany each record and has grouped the metadata into a model for a metadata encapsulated record. Metadata has been simply defined as "data about data." It encompasses a variety of *types* of data. For example, the data resident in data dictionaries, data directories, and systems documentation are all metadata. His reference model describes how the documentation of the content and structure of a record can be linked to, and retained with metadata that describes the context of the business transaction that caused the record to be created. The metadata "guarantees that the record will be usable over time, only accessible under the terms and conditions established by the creator, and have the properties required to be fully trustworthy for purposes of executing business."[20] This reference model lays the foundation for business-acceptable communications that are metadata encapsulated records, although they need not be stored that way. The metadata is clustered into six layers:

- The Handle Layer declares the data that follows to be a record, assigns values indicating the provenance of the record, and provides terms by which the contents of the record can be discovered.
- The Terms and Conditions layer invokes controls over access to, and use and disposition of a record. Identifies restrictions imposed on access and use and where to resolve them.
- The Structural layer consists of metadata about data structure designed to permit the record to remain evidential over time and to be migrated to new software and hardware dependencies as necessary.
- The Contextual layer identifies the provenance (i.e., the person, system, or instrument that is responsible for generating the record) of the record and provides data that supports its use as evidence of a transaction.
- The Content layer contains the actual data engaged in the transaction.
- The Use History layer documents evidentially significant uses of the record subsequent to creation; typically these will include indexing, redacted releases, and record disposition/destruction under record retention authority, but other

uses (for eyes only viewing, etc.) may be recorded. This layer occurs at the end of the physical record to permit adding of entries without having to open the record.[21]

Developing systems that comply with this reference model will ensure the preservation and accessibility of understandable and trustworthy records over time. The functional requirements, production rules, and the metadata model provide organizations with a set of measurable specifications for designing record-keeping systems that ensure the creation, maintenance, and use of credible records.

Literary Warrant

The Pittsburgh Project identified the functional requirements for record-keeping, but the justification for the requirements are codified in the laws, standards, customs, and best practices of society. The Project turned to the sources that contain society's requirements for record-keeping, such as the law, regulations, case law, auditing standards, the ISO 9000 suite of standards, and information technology standards to help build a case for the functional requirements. We wanted to ground the requirements on a "literary warrant" based on a foundation of statements from authoritative sources that other stakeholders appreciated and trusted. We started by compiling a list of authoritative sources which relate to professional practices and dictate requirements for record-keeping.[22] The authority of each source was evaluated by experts in the field of law, information technology, and auditing—only highly authoritative sources were retained for further consultation. Each source was scanned for relevant passages that illustrate the functional requirements and these statements, along with their citations, were entered into a database. Each passage was classified according to the profession to which it relates and the functional requirement that it supports. The project then used these statements to gauge the probable acceptance of each of the requirements. For example, we found that the need for accurate and authorized records was well established and supported, while the requirements for preserving a record's structure or context was not as well understood or accepted.

The warrant also provided us with the language that other professionals use to express the concepts inherent in the functional requirements. This led us to the hypothesis that the requirements presented with their relevant statements would meet with greater acceptance than the requirements presented on their own. The research on source credibility and persuasion demonstrates that highly credible sources and messages that contain evidence from other trustworthy sources are more influential than messages from less credible sources. This led to speculation that statements from highly authoritative sources would wield more authority than the opinion of a group of archivists and records managers; the warrant could increase the credibility of the functional requirements and result in their greater acceptance. My dissertation tests this hypothesis; specifically, my research addresses the following questions:

- Can a warrant increase the credibility of the functional requirements for record-keeping?
- Is one type of warrant—that is, a warrant drawn from legal, auditing, or information technology literature—more influential than others?

- Is the warrant from a person's professional literature more powerful than other warrants?[23]

To answer these questions, four research instruments were created, each containing five requirements accompanied by legal warrant, five requirements accompanied by auditing warrant, five requirements accompanied by information technology warrant, and five requirements presented on their own. Each instrument contains the same requirements accompanied by a different type of warrant. For example, one instrument contains the first requirement accompanied by legal warrant, the next instrument contains the first requirement accompanied by auditing warrant, the third instrument contains the first requirement accompanied by information technology warrant and the last group contains the first requirement without warrant. Sixty research subjects—twenty lawyers, twenty auditors, and twenty information technologists—were recruited and randomly assigned to four groups. Each group was presented with each requirement, told that the requirement was derived from the warrant that accompanied it, and asked to evaluate the importance of having systems comply with it. The subjects were told that the requirements without warrant were suggested by a group of archival and records management experts. At the time of writing this article, the data collection was finished but the data analysis was not yet complete.

Tactics for the Functional Requirements

The Pittsburgh Project posited that requirements can be met by one of four tactics: *design*, *policy*, *implementation*, and *standards*. *Design* necessitates the incorporation of archival specifications into the design of record-keeping systems. *Policy* requires the writing of policy on how to use the electronic record-keeping system, while *implementation* provides guidelines on methods of implementation. *Standards* have often been seen as the solution to the problems of long-term preservation of records and require that the organization identify international, national, or institutional standards. The project hypothesized that a person's choice of tactics will depend upon the technical environment existing in an organization, as well as an individual perspective on the organizational culture.

To measure an individual's and an organization's acceptance of the requirements and to test the hypothesis, two doctoral students conducted interviews with employees in three different organizations: a university, a county government, and a research and development arm of a Fortune 500 company. Lawyers, controllers, line managers, information systems managers, and records managers (approximately ten individuals in each organization), provided their insights into the organization's culture, their evaluations of the functional requirements, and the best tactic for implementing them in the particular organization. The students collected information in two semi-structured interviews: one that gathered information about the culture of the institution and one that presented and explained each functional requirement. They then solicited feedback on the importance of the functional requirements and tactics for implementing them in the particular institution.

The organizational profiles served to tease out variables that affect the choice of tactics. The findings indicated that some functional requirements lend themselves to certain tactics, e.g., individuals overwhelmingly choose policy or implementation to

meet the requirement *Conscientious*, and that certain professional groups demonstrate a preference for certain tactics, e.g., information systems managers favour the tactic *design*.[24]

Two other doctoral students have fleshed out a pure form of each tactic to test the viability of each of the tactics. The purpose of the "pure form" was to define the policy, implementation, design, and standards approach that would satisfy each requirement. This work has revealed that certain requirements are best met by particular tactics and that the requirements are dependent upon each other.

The University of Pittsburgh Electronic Records Project has developed a number of tools to assist in the capture, maintenance, and use of credible electronic records.[25] The primary work of the Project is complete and the Project's concepts are now being incorporated into other research projects and designed into systems. For example, the University of Indiana is evaluating its current systems against the functional requirements, the World Bank used the warrant to evaluate a number of document management systems, and the City of Philadelphia is presently purchasing a system that creates metadata encapsulated objects based on the metadata model.

The task of preserving evidence in a software- and hardware-dependent environment challenges archivists to develop new techniques and new ways of thinking about what to capture and how to preserve it. The development of the functional requirements, including the production rules, the literary warrant, and the metadata reference model, is a first step toward solving some of the most pressing problems that archivists face in the new electronic world. Archivists need to continue to test their assumptions and engage in research projects that will ensure that records essential for a vibrant democratic society are properly protected and accessible.

Notes

* The author wishes to thank Richard Cox and David Bearman, whose comments and ideas have greatly improved the paper, and David Wallace, for delivering a version of this article and responding to questions at the 1995 ACA conference.

1 An organization's ability to create a more empowered workforce, using technology to informate rather than automate, is described in Shoshana Zuboff, *In the Age of the Smart Machine: The Future of Work and Power* (United States, 1988).

2 For a review of the study of diplomatics and its use in establishing the authenticity of records, see Luciana Duranti, "Diplomatics: New Uses for an Old Science," *Archivaria* 27-33.

3 Charles M. Dollar, *Archival Theory and Information Technologies: The Impact of Information on Archival Principles and Methods* (Macerta, 1992).

4 Michael Duchein, "Theoretical Principles and Practical Problems," *Archivaria* 16 (Summer 1983), p. 17.

5 David Bearman, "Record-Keeping Systems," *Archivaria* 36 (Autumn 1993), p. 18.

6 Terry Cook, "Easy to Byte, Harder to Chew: The Second Generation of Electronic Records Archives," *Archivaria* 33 (Winter 1991-92), p. 204.

7 Cited in Andy Reihardt, "Managing the New Document," *Byte* (August 1994), p. 91.

8 David Bearman, "Archival Principles and the Electronic Office," in Angelika Menne-Haritz, ed., *Information Handling in Offices and Archives* (Munchen, 1993), p. 190.

9 National Association of Government Archives and Records Administrators, *Archival Administration in the Electronic Age: An Advanced Institute for Government Archivists* (cosponsored by the School of Library and Information Science, University of Pittsburgh, and funded by the Council on Library Resources) (Pittsburgh, 1990), p. 2.

10 United States, National Historical Publications and Records Commission, *Electronic Records: A Report to the Commission, Commission Reports and Papers* 4 (Washington, D.C., 1990), p. 7.

11 Ibid., p. 4.
12 Ibid., p. 6.
13 United States, National Historical Publications and Records Commission, *Research Issues in Electronic Records* (St. Paul, 1991), pp. 7-8.
14 In 1992 the Commission adopted a long-range plan which included as one of its level one objectives the carrying out of the Working Meeting on Research Issues in Electronic Records' recommendations. Since that time the Commission has supported a number of research projects related to electronic records including the New York State Archives and Records Administration's Building Partnership Project and the Indiana University Electronic Records Project, designed to test the Pittsburgh Project's Functional Requirements for Recordkeeping.
15 Richard J. Cox, "Re-Discovering the Archival Mission: The Recordkeeping Functional Requirements Project at the University of Pittsburgh," (unpublished paper included in University of Pittsburgh Recordkeeping Functional Requirements Project: Reports and Working Papers [LIS055/LS94001]), September, 1994, p. 10.
16 International Standards Organization, *Quality Management and Quality Assurance Standards: Guidelines for Selection and Use*, paragraph 4.16.
17 James Lamprecht, *Implementing ISO 9000* (New York, 1993), p. 49.
18 United States, *Federal Rules of Evidence*, Rule 803.
19 David Bearman and Ken Sochats, "Formalizing Functional Requirements," (unpublished draft paper included in University of Pittsburgh Recordkeeping Functional Requirements Project: Reports and Working Papers, LIS055/LS94001), September 1994.
20 David Bearman, "Virtual Archives," (unpublished paper included in University of Pittsburgh Recordkeeping Functional Requirements Project: Reports and Working Papers [LIS057/LS95001]), March 1995, p. 176.
21 David Bearman, "Towards a Reference Model for Business Acceptable Communications," (unpublished paper included in University of Pittsburgh Recordkeeping Functional Requirements Project: Reports and Working Papers [LIS057/LS95001]), March 1995.
22 Examples of sources the project consulted include:
Performance Guideline for the Legal Acceptance of Records Produced by Information Technology Systems: "Part 1: Performance Guideline for Admissibility of Records Produced by Information Technology, Systems as Evidence;" *Technical Report AIIM TR31-1992*, Association for Information and Image Management;
Electronic Industry Data Exchange. ASC 12 Convention: Version 3: Electronic Industry Data Guidelines; Washington Publishing Co., 1994;
"Guideline for the Analysis of Local Area Network Security" Category: Computer Security; Subcategory: Risk Analysis and Contingency Planning. Federal Information Processing Standards Publication 191 (U.S. Department of Commerce/Technology Administration and National Institute of Standards and Technology, 9 November 1994);
"Good Security Practices for Electronic Commerce, Including Electronic Data Interchange" by Roy G. Saltman, Editor. Computer Systems Laboratory, National Institute of Standards and Technology, December 1993. U.S. Department of Commerce. NIST Special Publication 800-9;
21 CFR Part 11 Electronic Signatures, Electronic Records, 11.10;
41 CFR Sec. 201 - 9.103;
Federal Rules of Evidence. 1990. Rule 803;
McCannan v. Tolfree et al. 198 N.W. 197;
36 CFR PART 1234 — Electronic Records Management. Subpart C — Standards for the Creation, Use, Preservation, and Disposition of Electronic Records;
American Institute of Certified Public Accountants. Statements on Auditing Standards 55. Consideration of the Internal Control Structure in a Financial Statement Audit.
23 Wendy Duff, "The Influence of Literary Warrant on the Acceptance and Credibility of the Functional Requirements for Recordkeeping," (Ph.D. Dissertation, University of Pittsburgh, 1996). An article that describes the dissertation research will appear in *Archives and Museum Informatics: Cultural and Heritage Information Quarterly* 10, no. 4 (Winter 1996).
24 Wendy Duff and David Wallace, "Organizational Cultures," in University of Pittsburgh Recordkeeping Functional Requirements Project: Reports and Working Papers (LIS055/LS94001), September 1994 and Wendy Duff and Debra Rhodes "Organizational Culture as a Predictor of Tactic Preference," in Ibid., (LIS057/LS95001), March 1995, pp. 45-53.
25 I have published two sets of working papers, which are available on the project's web server at http://www.lis.pitt.edu/nhprc.

Appendix

Functional Requirements for Evidence Within Record-Keeping

1. Compliant

ACCOUNTABLE RECORD-KEEPING SYSTEM

2. Responsible
3. Implemented
4. Consistent

CAPTURED RECORDS

5. Comprehensive
6. Identifiable
7. Complete
   - 7a. Accurate
   - 7b. Understandable
   - 7c. Meaningful
8. Authorized

MAINTAINED RECORDS

9. Preserved
   - 9a. Inviolate
   - 9b. Coherent
   - 9c. Auditable
10. Removable

USABLE RECORDS

11. Exportable
12. Accessible
    - 12a. Available
    - 12b. Renderable
    - 12c. Evidential
13. Redactable

Organization: Conscientious

1. *Compliant*: Organizations must comply with the legal and administrative requirements for record-keeping within the jurisdictions in which they operate, and they must demonstrate awareness of best practices for the industry or business sector to which they belong and the business functions in which they are engaged.

1a. External record-keeping requirements are known.

1a1. Laws of jurisdiction with authority over the record creating organizations are known.

1a2. Regulatory issuances of entities with administrative authority over the record creating organizations are known.

1a3. Best practices of record-keeping established by professional and business organizations within the industry and business functions of the organization are known.

1b. Records created by organizational business transactions which are governed by external record-keeping requirements are linked to an internal retention rule referencing the documented law, regulation, or statement of best practice.

1c. Laws, regulations, and statements of best practice with requirements for record-keeping are tracked so that changes to them are reflected in updated internal record-keeping instructions.

Record-Keeping Systems: Accountable

2. *Responsible*: Record-keeping systems must have accurately documented policies, assigned responsibilities, and formal methodologies for their management.

2a. System policies and procedures are written and changes to them are maintained and current.

2b. A person or office is designated in writing as responsible for satisfying record-keeping requirements in each system.

2c. System management methods are defined for all routine tasks.

2d. System management methods are defined for events in which the primary system fails.

3. *Implemented*: Record-keeping systems must be employed at all times in the normal course of business.

3a. Business transactions are conducted only through the documented record-keeping system and its documented exception procedures.

3b. No records can be created in the record-keeping systems except through execution of a business transaction.

3c. Record-keeping systems and/or documented exception procedures can be demonstrated to have been operating at all times.

4. *Consistent*: Record-keeping systems must process information in a fashion that assures that the records they create are credible.

4a. Identical data processes permitted by the system must produce identical outcomes regardless of the conditions under which they are executed.

4b. Results of executing systems logic are demonstrable outside the system.

4c. All operational failures to execute instructions are reported by the system.

4d. In the event of system failures, processes under way are recovered and re-executed.

Records: Captured

5. *Comprehensive*: Records must be created for all business transactions.

5a. Communications in the conduct of business between two people, between a person and a store of information available to others, and between a source of information and a person, all generate a record.

5b. Data interchanged within and between computers under the control of software employed in the conduct of business creates a record when the consequence of the data processing function is to modify records subsequently employed by people in the conduct of business.

6. *Identifiable*: Records must be bounded by linkage to a transaction which used all the data in the record and only that data.

6a. There exists a discrete record, representing the sum of all data associated with a business transaction.

6b. All data in the record belongs to the same transaction.

6c. Each record is uniquely identified.

7. *Complete*: Records must contain the content, structure, and context generated by the transaction they document.

7a. **Accurate**: The content of records must be quality controlled at input to ensure that information in the system correctly reflects what was communicated in the transaction.

7a1. Data capture practices and system functions ensure that source data is exactly replicated by system or corrected to reflect values established in system authority files.

7b. **Understandable**: The relationship between elements of information content must be represented in a way that supports their intended meaning.

7b1. Meaning conveyed by presentation of data are retained or represented.

7b2. System defined views or permissions are retained and the effects are reflected in the record represented.

7b3. Logical relations defined across physical records are retained or represented.

7b4. Software functionality invoked by data values in the content of the record are supported or represented.

7c. **Meaningful**: The contextual linkages of records must carry information necessary to understand correctly the transactions that created and used them.

7c1. The business rules for transactions, which minimally locate the transaction within a business function, are captured.

7c2. A representation of the source and time of the transaction which generated a record is captured.

7c3. Links between transactions which comprised a single logical business activity are captured.

8. *Authorized*: An authorized records creator must have originated all records.

8a. All records have creators which are documented.

8b. Records creators must have been authorized to engage in the business transaction that generated the record.

Records: Maintained

9. *Preserved:* Records must continue to reflect content, structure, and context within any systems by which the records are retained over time.

9a. Inviolate: Records are protected from accidental or intended damage or destruction and from any modification.

9a1. No data within a record may be deleted, altered, or lost once the transaction which generated it has occurred.

9b. Coherent: The information content and structure of records must be retained in reconstructible relations.

9b1. If records are migrated to new software environments, content, structure, and context information must be linked to software functionality that preserves their executable connections or representations of their relations must enable humans to reconstruct the relations that pertained in the original software environment.

9b2. Logical record boundaries must be preserved regardless of physical representations.

9c. Auditable: Record context represents all processes in which records participated.

9c1. All uses of records are transactions.

9c2. Transactions which index, classify, schedule, file, view, copy, distribute, or move a record without altering it are documented by audit trails attached to the original record.

9c3. Transactions which execute a records disposition instruction, whether for retention or destruction, are documented by audit trails attached to the original record.

10. *Removable:* Records content and structure supporting the meaning of content must be deletable.

10a. Authority for deletion of record content and structure exists.

10b. Deletion transactions are documented as audit trails.

10c. Deletion transactions remove the content and structural information of records without removing audit trails reflecting context.

Records: Usable

11. *Exportable:* It must be possible to transmit records to other systems without loss of information.

11a. Exporting protocols should be reversible.

11b. Functionality should be represented in a fashion that produces the same result in the target system as in the originating environment.

12. *Accessible*: It must be possible to output record content, structure, and context.

12a. Available: Records must be available.

12b. Renderable: Records must display, print, or be abstractly represented as they originally appeared at the time of creation and initial receipt.

12b1. The structure of data in a record must appear to subsequent users as it appeared to the recipient of the record in the original transaction or a human-meaningful representation of that original rendering should accompany the presentation of the original context.

12c. Evidential: Record's representations must reflect the context of the creation and use of the records.

13. *Redactable*: Records must be masked when it is necessary to deliver censored copies and the version as released must be documented in a linked transaction.

13a. The release of redacted versions of a record is a discrete business transaction.

13b. The fact of the release of a redacted version of a record is an auditable use of the original record and therefore results in creation of an audit trail with a link to the transaction which released the redaction.