ARMA International
13725 W. 109th Street, Suite 101
Lenexa, KS 66215
PH: 913.341.3808 FAX: 913.341.3742

Comments Regarding the Role of Records and Information Management:
Compliance with the Internal Control Provisions of
Section 404 of the Sarbanes-Oxley Act
Submitted by ARMA International
Before the U.S. Securities and Exchange Commission
(File Number 4-497)

On February 7, 2005, the Commission announced that it will host a roundtable discussion and solicit written feedback regarding the experiences of registrants, accounting firms and others in implementing the new internal control requirements under Section 404 of the Sarbanes-Oxley Act of 2002.[1]

ARMA International respectfully submits these comments for the Commission's consideration, based on the observations and experiences of Records and Information Management professionals and consultants involved in Section 404 compliance. ARMA International has also requested an opportunity to participate in the roundtable discussion by letter dated February 25, 2005 from David McDermott, CRM, as President of ARMA International. [2]

About ARMA International

ARMA International (ARMA) is the association of records managers and administrators, whose 10,000 members include records and information managers, imaging specialists, archivists, librarians, and educators in both the public and private sectors. ARMA is also host to the community of service providers and manufacturers who support the Records and Information Management functions in public and private sector organizations.

ARMA serves as an international forum for establishing policies, processes and technology standards to ensure responsible Records and Information Management. Our

[1] Pub. L. 107-204, 116 Stat. 745 (2002). Section 404 of the Sarbanes-Oxley Act is codified at 15 U.S.C. 7262.

[2] See http://www.sec.gov/news/press/4-497/4497-22.pdf.

members are responsible for the efficient maintenance, retrieval, and preservation of vital information created in public and private organizations in all sectors of the economy.

ARMA has long supported policies that provide for the efficient and appropriate management of records and information in all forms and in all settings. ARMA endorses the adoption and implementation of Records and Information Management policies and procedures, based on best practices and established standards which are well known to the profession of records management, and that provide guidance on organizing, retaining, preserving, and appropriately destroying records. Acknowledgement of the importance of Records and Information Management by an organization's leadership and a commitment of resources to support a Records and Information Management program serve as effective internal controls for compliance with business practices as well as statutory and regulatory requirements.

ARMA is a recognized standards developer for the American National Standards Institute (ANSI) towards the development of Records and Information Management standards. ARMA has developed seven ANSI/ARMA publications on Records and Information Management, the most recent of which is ANSI/ARMA 8-2005, "Retention Management for Records and Information".[3]

ARMA is a charter member of International Organization for Standardization (ISO) Technical Committee ISO/TC 46, Information and documentation, Subcommittee SC 11, Archives/records management, and ARMA contributed towards the development of the ISO International Standard, "Information and documentation – records management – Part 1: General" (ISO 15489-1:2001).[4]

<u>The Role of Records and Information Management</u>

[3] The seven ARMA/ANSI publications are: (1) "Glossary of Records and Information Management Terms" (ANSI/ARMA 10-1999, 2nd ed); (2) "Establishing Alphabetic, Numeric and Subject Filing Systems" (ANSI/ARMA 12-2005); (3) "Framework for the Integration of Electronic Document Management Systems and Electronic Records Management Systems Technical Reports" (ANSI/AIIM ARMA TR48-2004); (4) "Records Center Operations, 2nd ed." (ANSI/ARMA TR-01-2002); (5) "Retention Management for Records and Information" (ANSI/ARMA 8-2005); (6) "Requirements for Managing Electronic Messages as Records" (ANSI/ARMA 9-2004); and (7) "Vital Records Programs: Identifying, Managing, and Recovering Business-Critical Records" (ANSI/ARMA 5-2003).

ANSI/ARMA 8-2005 represents long recognized best practices for the retention and disposition of information in the custody of organizations in both the public and private sectors. The Standard in part updates an earlier ARMA publication, entitled "Developing and Operating a Records Retention Program – A Guide", developed under ARMA's standards making process. For excerpts of this document, <u>see</u> "Guidelines for Retention by Industry Program (GRIP)" at www.arma.org/membership/isg/grip.

[4] The ISO Standard on "Information and documentation – records management" is published in two parts. ISO 15489-1:2001, "Information and documentation – records management – Part 1: General", contains the International Standard, and ISO/TR 15489-2:2001, "Information and documentation – records management – Part 2: Guidelines", contains the Technical Report. All references and citations in these comments refer to the International Standards of ISO 15489-1:2001 (hereafter referred to as "ISO Standard").

(1) First and foremost, ARMA recognizes that properly developed and implemented Records and Information Management programs represent an important element of sound business practice.

Records and Information Management principles dictate that all relevant business records remain accessible for the duration of a record's life-cycle. The ISO Standard codifies this assertion –

> "Records are created, received and used in the conduct of business activities. To support the continuing conduct of business, comply with the regulatory environment and provide necessary accountability, organizations should create and maintain authentic, reliable and useable records, and protect the integrity of those records for as long as required."[5]

Records and Information Management programs create firm-wide, cost-effective processes and procedures for assuring the validity and accessibility of vital records and compliance with voluntary and legally required retention policies.

Records are initially created for the purpose of conducting business, documenting and fulfilling business obligations and facilitating decision-making processes. Businesses have obligations and requirements that affect how they keep their records, independent of the need to demonstrate compliance with statutory or regulatory requirements. By following good records management principles, organizations can rely on the integrity and authenticity of the records they create and use in all aspects of their operations.[6]

Records and Information Management governs the practice of both records managers and of any person who creates or uses records in the course of their business activities.

The ISO Standard recognizes the value proposition of records management –

> "Records contain information that is a valuable resource and an important business asset. A systematic approach to the management of records is essential for organizations and society to protect and preserve records as evidence of actions. A records management system results in a source of information about business activities that can support subsequent activities and business decisions, as well as ensuring accountability to present and future stakeholders."[7]

[5] See ISO 15489-1:2001, Clause 7.1, "Principles of records management programmes".

[6] Likewise, auditing firms and regulatory bodies can rely on the integrity and authenticity of records captured in a properly implemented Records and Information Management program.

[7] See ISO 15489-1:2001, Clause 4, "Benefits of records management".

The ISO Standard also speaks to the regulatory environment –

> "All organizations need to identify the regulatory environment that affects their activities and requirements to document their activity. The policies and procedures of organizations should reflect the application of the regulatory environment to their business processes. An organization should provide adequate evidence of its compliance with the regulatory environment in the records of its activities."[8]

Several other elements of Records and Information Management applicable to the Section 404 internal controls merit attention.

Management Involvement. The importance of executive level support is reflected in ANSI/ARMA standards related to various aspects of records management programs. For example, Section 4.0 of ANSI/ARMA 9-2004, "Requirements for Managing Electronic Messages as Records" states: "The executive management of an organization seeking to conform to this standard shall establish, document, maintain**,** and promote policies, procedures, and practices for managing electronic messages and electronic messaging systems that ensure the organization's business needs are met." Section 5.0 of ANSI/ARMA 8-2005, "Retention Management for Records and Information" reinforces the importance of top management support: "The ultimate authority for all decisions relating to retention of records resides with the senior management of the organization." Section 5.2 of the same standard states: "In addition to the information retention and disposition policy statement, senior management should issue specific directives as necessary to ensure support for the information retention and disposition program."[9]

Records management programs are greatly enhanced and effective when the executives demonstrate active support of its requirements. Likewise, records management programs are greatly weakened if the executive level support falls short of providing needed resources, and making financial allocations to enable comprehensive implementation and monitoring.

[8] See ISO 15489-1:2001, Clause 5, "Regulatory environment".

[9] Clause 6.3 of the ISO Standard recognizes that while all employees in an organization have some responsibility for the manner in which organizations keep their records, the level of responsibility and accountability will vary. The standard states: "Records management responsibilities and authorities should be defined and assigned, and promulgated throughout the organization so that, where a specific need to create and capture records is identified, it should be clear who is responsible for taking the necessary action. These responsibilities should be assigned to all employees of the organization, including records managers, allied information professionals, executives, business unit managers, systems administrators and others who create records". Clause 6.3(b) adds more detail specific to executives by stating, "[e]xecutives are responsible for supporting the application of records management policies throughout the organization"

Training: As with all policies and procedures, training is an essential element of any Records and Information Management program. Section 10 of ANSI/ARMA 9-2004 states: "Organizations should provide an ongoing program of user training to facilitate and achieve effective electronic message management. The policy should be communicated to users so that all users are aware of the intent and boundaries of the policy." Section 9.2 of ANSI/ARMA 8-2005 also references the importance of ongoing training in the implementation of an organization's retention and disposition program.[10]

In today's distributed work environments, a wide variety of individuals create records and must therefore take responsibility to ensure those records are captured, identified and preserved. It is no longer enough to train administrative staff and assume they will make sure the records end up in the records management program. All members of management, employees, contractors, volunteers and other individuals share the responsibility for capturing records so they can be properly managed throughout the length of their required retention period.

Communication. Closely related to training, is the necessity of communicating the records management program throughout the organization. This theme is reiterated in Section 4.0 of ANSI/ARMA 9-2004: "The designated records personnel must ensure that the policy is communicated and implemented throughout the company." The Section also requires that records management policies be published and circulated throughout the organization and that responsibilities for compliance be assigned to every user and each individual with a recordkeeping role, including database administrators and information or network technology support personnel. Section 9.1 of ANSI/ARMA 8-2005 also references the best practice of establishing a manual or processes and procedures relative to records management that is provided to departments and managers throughout an organization.[11]

Monitoring and Auditing. Records and Information Management best practices also require ongoing monitoring and auditing. Section 4.1 of ANSI/ARMA 9-2004 requires that Records and Information Management programs be "regularly reviewed at

[10] Clause 11 of the ISO Standard addresses the need for training within an organization seeking to comply with the standard. It recognizes that the records management training for employees should be customized to their particular responsibilities and accountability within the program.

[11] Section 9.1 of ANSI/ARMA 8-2005 further requires that a letter from the chief executive officer of the organization stating the purpose of the information retention and disposition program and the need for compliance with the policy from all departments and staff. Clause 6.1 of the ISO Standard, addressing policy and responsibilities, states: "An organization seeking to conform to this part of ISO 15489 should establish, document, maintain and promulgate policies, procedures, and practices for records management to ensure that its business need for evidence, accountability and information about its activities is met." Clause 6.2 of the ISO Standard requires that "Organizations should ensure that the policy is communicated and implemented at all levels in the organization. The policy should be adopted and endorsed at the highest decision-making level and promulgated throughout the organization. Responsibilities for compliance should be assigned."

designated intervals and revised, as needed, to reflect current compliance requirements. Section 7.2 of ANSI/ARMA 8-2004 requires that records management policies authorize individuals within the organization to “monitor equipment, systems, electronic message traffic at any time for security and network maintenance purposes” and that the organization retain authority to “audit networks and systems on a periodic basis to ensure policy compliance”.[12]

Section 9.3 of ANSI/ARMA 8-2005 states: “Compliance with the information retention and disposition program is the responsibility of the organization and all employees. Employees should be aware of the program and its requirements – especially the effects of inappropriate or premature disposition of records…Compliance with the information retention and disposition program should be reviewed on a regular basis, determined by organization policy”.

Management of Change. The ANSI/ARMA standards recognize that it is important to document the policies and procedures on which the records management program is based, and that it is important to maintain corporate integrity of the information management environment by periodically assessing the policies, systems and practices that are in place to ensure they are still relevant to a changing business environment. Nearly everything in the information management environment is subject to frequent change (legal requirements, organizational infrastructure, technology, regulations and business process changes).[13]

Retention Periods. The determination of retention periods for various record types within an organization is a complex process involving data gathering, analysis, and decision-making as the basis for the retention and disposition schedule. The various elements of this process are further specified in ARMA International’s most recent standard, “Retention Management for Records and Information” (ANSI/ARMA 8-2005).[14]

Without being comprehensive, the above references should adequately demonstrate that the importance of executive level support, communication, training, change management

[12] Clause 10 of the ISO Standard states: “Compliance monitoring should be regularly undertaken to ensure that the records systems procedures and processes are being implemented according to the organizational policies and requirements and meet the anticipated outcomes. Such reviews should examine organizational performance and user satisfaction with the system….Modifications to the records systems and records management processes should be made if these are found to be unsuitable or ineffective.”

[13] Clause 6.2 of the ISO Standard states: “Policies should be regularly reviewed to ensure that they reflect current business needs.” Clause 8.4.(h), addressing post-implementation review, states: “Gather information about the performance of the records system as an integral and ongoing process…. Review and assess the performance of the system, initiate and monitor corrective action and establish a regime of continuous monitoring and regular evaluation.”

[14] The ISO Standard devotes the majority of Clause 9 to the analytical process behind analyzing business activities, determining the various uses of the records and determining how long to keep them.

and auditing and compliance are well recognized in Records and Information Management standards at both the national and international level. These are the same hallmarks that will lend additional credibility for covered entities wishing to maximize the use of records management as an internal control mechanism supporting their Section 404 compliance.

(2) A properly implemented Records and Information Management program will contribute to the assurances expected of an organization's internal controls.

Records and Information Management will ensure that the Section 404 internal controls are not isolated, but are considered as a function of the entire company. Many companies, in their efforts to comply with Section 404, have been so occupied with developing a system for financial reporting that other systems and operations may be overlooked. ARMA believes that it is best to develop a whole system, rather than a fragmented system. Focusing on one particular area at the expense of others, may create more problems in the future. Utilizing recognized standards of Records and Information Management will help integrate departmental functions and system responsibilities, identifying the records and users and capturing the entire organization's informational asset structure.

(3) Records and Information Management will help address and reduce costs of compliance.

Records and Information Management can and does reduce the costs of compliance. The very basis of Records and Information Management is compliance based on a set of firm-wide processes and procedures to enable every day business practices to comply with business-specific as well as statutory and regulatory requirements. The Sarbanes-Oxley Act has merely added another compliance requirement to the many that a business incorporates in its operations and control procedures everyday, all of which should be integrated into the covered entity's existing Records and Information Management framework. ARMA recognizes that the Sarbanes-Oxley Act creates the need to identify work-flow processes and records to provide evidentiary support of compliance. One particular discipline of Records and Information Management is to review work-flow processes and identify alternative records retention methodologies to be employed in order to provide better utilization of assets and to simplify the process. This reduces costs in all areas and will achieve cost efficiencies for compliance with the Sarbanes-Oxley Act.

Comments and Observations Regarding Section 404 and Current Rule

ARMA believes that the processes and procedures provided by a properly implemented Records and Information Management program must play an integral role in the internal controls of entities covered by Section 404. Such a program can become an element of the basis of management's assessment, the auditing firm's review, and the Commission's oversight.

(1) Section 404 of the Sarbanes-Oxley Act requires that each annual report of a covered entity state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting.[15]

As a general proposition, ARMA believes that Records and Information Management creates a structure and set of procedures around the records relied upon for purposes of meeting the financial reporting requirements for covered entities. This structure and its procedures can and should be relied upon by covered entities and auditing firms in meeting their respective responsibilities under Section 404.

Ensuring that records are maintained and retained in a manner required by a regulatory agency is the mandate of records managers, with the help of various departments and individuals, such as technology, legal, finance, and business line executives. Simply because the records happen to be financial records does not shift them from the purview of records managers to accountants and auditors; instead, these records are another aspect of a records management program that has delineated statutory and regulatory requirements.

(2) Section 404 of the Sarbanes-Oxley Act requires that each annual report of a covered entity contain an assessment of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.[16]

As a general proposition, ARMA believes that management's assessment must rely upon the structure and procedures created by a Records and Information Management program, in addition to other internal controls.

ARMA believes that the assessment should include a review and confirmation of an organization's Records and Information Management program. The evaluation of effectiveness must be measured against some type of criteria in order to be deemed effective or deficient. These criteria, or standards, having been identified in the audit procedures, will enable the covered entity to efficiently identify problematic areas, provide solutions to correct any deficiencies, and follow-up with a methodology to ensure the corrections have been made.

(3) The Commission has defined "internal controls" to mean a process designed "to provide reasonable assurance regarding the reliability of financial reporting and the

[15] See Section 404(a)(1) of the Sarbanes-Oxley Act (15 U.S.C. 7262(a)(1)).

[16] See Section 404(a)(2) of the Sarbanes-Oxley Act (15 U.S.C. 7262(a)(2)).

preparation of financial statements for external purposes in accordance with generally accepted accounting principles".[17]

There is significant ambiguity concerning the meaning of "reasonable assurance".[18] Records and Information Management professionals and consultants have reported that this ambiguity forces management to make in many cases unnecessarily costly investments in the Section 404 auditing process. In many of these instances these investments would more properly support a firm-wide Records and Information Management program that is incorporated in the company's Section 404 internal control procedures. The ambiguity also leaves too much to the uncertainties of specific enforcement actions and litigation. ARMA believes that greater clarity regarding what processes and procedures will meet Section 404 requirements is needed. ARMA would recommend that the Commission include in any recitation of acceptable internal control processes a specific reference to a clearly defined, authorized and fully implemented Records and Information Management program.

(4) The Commission has defined "internal controls" to mean a process that includes policies and procedures that pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the registrant.[19]

The Commission appears to anticipate that Records and Information Management is a process and regime that will be a part of a covered entity's internal controls. A properly developed and implemented Records and Information Management program will provide significant assurances for management, auditing firms, and the Commission. A Records and Information Management program can also provide the necessary review of retention methodologies to ensure that the records are retained on the most appropriate media and preserved for the required retention period ensuring the trustworthiness of the record.

[17] See Title 17 of the Code of Federal Regulations, Section 270.30a-3(d). See also discussion in Section II.A.3 of Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports (Release Nos. 33-8238; 34-47986; IC-26068; June 5, 2003) ("Final Rule").

[18] A survey authorized by ARMA International found that only 7 percent of Chief Financial Officers surveyed in public companies in the United States felt that the provisions of Sarbanes-Oxley were clear. "CFO Records Management Study" (International Communications Research/ICR: October 2003) is available from ARMA International. The study also found that 81 percent of those surveyed said that the new requirements would place significant burdens on their companies, and 95 percent indicated that they would expect to make changes to their records management procedures in order to comply with Sarbanes-Oxley. ARMA believes that this acknowledges the role that Records and Information Management must play in meeting the Section 404 requirements and that further guidance from the Commission is needed to direct companies where best to make their investments.

[19] See Title 17 of the Code of Federal Regulations, Section 270.30a-3(d). See also discussion in Section II.A.3 of the Final Rule.

While not every covered entity will have the same subset of records, once the requisite records are identified in the development and/or revision of retention schedules, then "generic" categories could provide samples of the types of records expected to be found in such categories.

ARMA believes that the development of suitable assessment procedures and standards to ensure that records systems are properly set up and properly maintained and have the appropriate controls over them will provide significant guidance to covered entities.

Better guidance would be found in the identification of specific standards, either developed by recognized bodies or by the Commission, with further identification by the Commission of the precise records that should be retained for purposes of confirming compliance.

Recommendations

(1) The Commission should identify specific regimes and processes that covered entities can rely upon for compliance.[20]

The current rule requires management to make its evaluation of the effectiveness of internal controls on a "suitable, recognized control framework that is established by a body or group that has followed due-process procedures, including the broad distribution of the framework for public comment". The Commission observes that "[t]he use of standard measures that are publicly available will enhance the quality of the internal control report and will promote comparability of the internal control reports of different companies". The Commission states that "a suitable framework must: be free from bias; permit reasonable consistent qualitative and quantitative measurements of a company's internal control; be sufficiently complete so that those relevant factors that would alter a conclusion about the effectiveness of a company's internal controls are not omitted; and be relevant to an evaluation of internal control over financial reporting".[21]

[20] ARMA notes that the Commission has addressed this issue in part in Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports Frequently Asked Questions (Office of the Chief Accountant, Division of Corporation Finance: revised October 6, 2004). In response to Question 18: "What sources of guidance are available to management to assist them in fulfilling their responsibilities regarding management's assessment and documentation of the internal control over financial reporting?", the Commission states: "Several sources of guidance are available on the topic of management's assessment of internal control including, for example: the existing books and records requirements; the Commission's final rule on Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports (Release No. 34-47986); and, as referenced in the release on the final rule, the reports published by the Committee of Sponsoring Organizations of the Treadway Commission on internal control."

[21] See discussion in Section II.B.3.a of the Final Rule.

ARMA suggests that the Commission acknowledge the role of the ANSI/ARMA and ISO standards referenced above as an acceptable element of a organization's internal controls. These standards will help covered entities identify the internal control structures for financial reporting and will provide requirements for all records and systems within an organization, not just a select few, providing compliance not only for Section 404, but for all statutory and regulatory requirements.

ARMA would urge the Commission to identify any specific control framework, by an appropriate body, that includes such a standard measure that the Commission believes will attest to compliance. This should include the ANSI/ARMA and ISO standards relative to a Records and Information Management program that incorporates a covered entity's internal controls. This would serve as important guidance for covered entities. Without such guidance, covered entities are left to costly efforts that provide no absolute assurances. As a result, the risk management tendency is to either do more than is either necessary or helpful, or to create a separate layer of processes and procedures not tied to other entity-wide practices.

(2) The Commission should identify specific records that could provide organizations with further compliance guidance.

As with the identification of standards and processes referenced above, identification of specific records required for demonstrating compliance with Section 404 will provide much needed guidance for covered entities.

ARMA urges the Commission to identify specific records to serve as guidance for covered entities. ARMA envisions specific references to records to serve as benchmarks for entities making their best efforts to comply with the Section 404 requirements.

ARMA also recommends that the Commission establish retention schedules for specified records and required documentation.

Conclusion

ARMA appreciates this opportunity to provide comments regarding the experience of Records and Information Management professionals and consultants involved in Section 404 compliance. ARMA is committed to the well-recognized principles of Records and Information Management and is available to the Commission to provide further comments and to make recommendations regarding the role of Records and Information Management in the implementation of Section 404.

ARMA firmly believes that Records and Information Management must be integrated into the Section 404 internal controls.

Finally, ARMA offers its considerable expertise and would welcome the opportunity to make available its resources to the Commission towards developing applicable Records and Information Management elements for the Section 404 internal controls.

Respectfully Submitted,

ARMA INTERNATIONAL
David McDermott, CRM
President

April 1, 2005