Records Management or Information Governance?

William Saffady, Ph.D, FAI

Editor's note: This article was excerpted from the upcoming third edition of *Records and Information Management: The Fundamentals of Professional Practice*, which will be published by ARMA International this fall. Taken from Chapter 1, which examines the purpose and scope of records management as a business discipline, it defines records management and information governance, placing records management within the context of an information governance program.

Records management is a specialized discipline that is concerned with the systematic analysis and control of information created, received, maintained, or used by an organization pursuant to its mission, operations, and activities. By definition, records management is concerned with information that is recorded or "written down" as opposed to merely memorized or exchanged verbally.

A comprehensive records management program includes policies, procedures, and processes that address significant recordkeeping issues, specifically:

- Determining how long recorded information needs to be kept to satisfy an organization's requirements
- Ensuring compliance with recordkeeping laws and regulations in all locations where an organization has business operations
- Managing inactive records in a cost-effective manner
- Organizing active records for retrieval when needed

- Protecting recorded information that supports mission-critical business operations

These programmatic aspects are embodied in Generally Accepted Recordkeeping Principles® (Principles), which were issued by ARMA International in 2009 to foster general awareness of records management systems and standards and to assist organizations in developing effective programs for records management programs and information governance. The set of eight recordkeeping principles are paraphrased below:

Accountability

A senior executive should be in charge of the records management program. The accountable executive will delegate program responsibility to appropriate individuals, adopt records management policies and procedures to guide program personnel, and ensure that the program can be audited for compliance. A governance structure must be established for program development and implementation.

Transparency

An organization's recordkeeping processes and activities must be documented in an open and verifiable manner. Such documentation must confirm that the organization's recordkeeping policies and practices comply with applicable legal requirements and accurately and completely reflect the organization's activities. The documentation must be available to employees and appropriate interested parties.

Integrity

An organization's records must have a reasonable and suitable guarantee of authenticity and reliability. Recordkeeping processes, including audit processes, must provide reasonable assurance that the origin, time or creation or transmission, and content of recorded information are what they are claimed to be.

Records management is an important component of an information governance program, but it is not the only component.

Protection

An organization's records management program must protect records that are private, confidential, privileged, secret, or essential to business continuity. Recordkeeping procedures must provide appropriate protection controls from creation through final disposition of recorded information.

Compliance

An organization's records management program must comply with applicable laws, regulations, industry-specific rules of conduct, and other binding authorities related to creation, storage, retrieval, retention, disposition, dissemination, and protection of recorded information, as well as with the organization's own recordkeeping policies, procedures, and rules.

Availability

An organization's records must be organized, indexed, stored, and maintained in a manner that ensures timely, efficient, and accurate retrieval of information when needed.

Retention

An organization must retain records for an appropriate period of time to satisfy legal, regulatory, fiscal, operational, and historical requirements.

Disposition

An organization must provide secure and appropriate disposition for records that no longer need to be kept. In this context, disposition may involve destruction of records, transfer of records to another organization as part of a divestiture or other transaction, transfer of records to an archives or other scholarly repository, or transfer of records to clients or other parties who are the subjects of the records.

Records Management and Information Governance

According to the *OECD Glossary of Statistical Terms*, which was assembled by the Organization for Economic Cooperation and Development from documents issued by various international organizations, *governance* is the process by which decisions are made and implemented.

ISO/IEC 38500, *Information Technology – Governance of IT for the Organization* defines *governance* as "a system of directing and controlling."

ISO/IEC TR 38502, *Information Technology – Governance of IT – Framework and Model* defines a *governance framework* as the "strategies, policies, decision-making structures and accountabilities through which the organization's governance arrangements operate."

Similarly broad definitions are presented in other ISO standards – such as ISO 21500, *Guidance on Project Management,* and ISO/IEC 27000, *Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary* – and in various other sources, including dictionaries of business terminology.

Building on these definitions, *information governance* can be viewed as a system for directing and controlling an organization's information assets. As such, information gover-

Information governance is a collaborative initiative that requires the involvement and expertise of multiple stakeholders.

nance is a component or subset of organizational governance. Published definitions provide additional details.

ARMA TR 22-2012, *Glossary of Records and Information Management Terms*, for example, defines *information governance* as "a strategic framework composed of standards, processes, roles and metrics that hold organizations and individuals accountable to create, organize, secure, maintain, use, and dispose of information in ways that align and contribute to the organization's goals."

The American Health Information Management Association (AHIMA) defines *information governance* as "an organization-wide framework for managing information throughout its lifecycle and supporting the organization's strategy, operations, regulatory, legal, risk, and environmental requirements."

According to the *Commentary on Information Governance* issued by the Sedona Conference in December 2013, *information governance* is "an organization's coordinated, interdisciplinary approach to satisfying information compliance requirements and managing information risks while optimizing information value."

ISO/TS 14265, *Health Informatics – Classification of Purposes for Processing Personal Health Information* and ISO/TR 11633-1, *Health Informatics – Information Security Management for Remote Maintenance of Medical Devices and Medical Information Systems – Part 1: Requirements and Risk Analysis* define *information governance* as "processes by which an organization obtains assurance that the risks to its information, and thereby the operational capabilities and integrity of the organization, are effectively identified and managed."

An *information governance framework*, sometimes described as an information governance model, defines strategies, policies, decision-making structures, and accountabilities for creation, storage, use, analysis, distribution, disclosure, retention, disposition, and protection of information.

Records management is involved, to some degree, with all of those information-related activities. Records management is an important component of an information governance program, but it is not the only component.

Information Governance Stakeholders

Information governance is a collaborative initiative that requires the involvement and expertise of multiple stakeholders. Adapting a definition presented in ISO/Guide 73, *Risk Management – Vocabulary*, a *stakeholder* is a business unit or a functional area that is involved with or affected by an organization's information assets.

In addition to records management, information governance stakeholders include, but are not necessarily limited to, information technology, information security, risk management, legal affairs, compliance, risk management, and the individual departments or other organizational units that have recorded information in their custody or under their supervisory control.

An information governance framework specifies roles and responsibilities that promote interaction, cooperation, and consultation among the following stakeholders, which are widely acknowledged to play key roles in defining the strategic direction for management of information assets in government agencies, companies, not-for-profit entities, and other organizations.

Records Management

Records management develops and communicates policies, procedures, and guidelines for lifecycle management of an organization's information assets as discussed in subsequent chapters. Information governance is not synonymous with records management, which focuses on the day-to-day execution of specific operations or activities that involve recorded information. These operations and activities are performed within the strategic framework defined by information governance.

Information Technology

Information technology creates and operates the technological infrastructure for processing, storage, retrieval, and distribution of an organization's information assets. It optimizes the utilization of technological resources for cost-effective management of information assets, provides backup protection and disaster recovery capability for recorded information, and provides the technological expertise and support required to implement information management policies developed by other stakeholders.

Information Security

Information security deals with issues related to confidentiality, data protection, and disclosure of an organization's information assets. It develops and communicates data protection and privacy policies to prevent unauthorized access to recorded information, monitors and evaluates situations or events that may threaten information assets, responds to security breaches that involve recorded information, and works with other stakeholders to identify information assets that require special security arrangements.

Risk Management

Risk management identifies, analyzes, and quantifies risks that may affect, are attributable to, or are otherwise related to creation, storage, retrieval, distribution, disclosure, retention, disposition, or protection of an organization's information assets. It develops and communicates policies and procedures to mitigate the adverse impact of specific information management policies and practices.

Legal

Legal affairs is concerned with legal issues and concerns that relate to recorded information. It reviews record retention policies and schedules for legal acceptability. It establishes and communicates policies related to legal proceedings that involve recorded information. It provides opinions and advice to other stakeholders about legal issues related to recorded information.

Compliance

Compliance is concerned with ensuring that an organization's practices comply with external requirements, including laws, regulations, and industry-specific guidelines that specify retention and security requirements for recorded information, and with the organization's internal policies and directives for creation, storage, distribution, retention, disposition, and protection of information assets. Compliance will investigate suspected violations of organizational policies and present the findings with recommendations for corrective action.

Business Units

Individual organizational units are responsible for day-to-day management of information in full compliance with applicable policies, procedures, guidelines, and directives. They must identify and dispose of recorded information with elapsed retention periods, determine access privileges and restrictions that apply to specific information assets, organize information assets for retrieval when needed, and protect information assets from loss, damage, or improper disclosure.

In conjunction with the Principles, ARMA International has issued an Information Governance Maturity Model (Maturity Model) that defines and describes five levels of program development – from sub-standard to transformational – for each of the eight principles. Organizations can use the Maturity Model for program evaluation and development, benchmarking, gap analysis, and risk assessment. **END**

William Saffady, Ph.D., FAI, can be contacted at wsaffady@aol.com*. See his bio on page 47.*