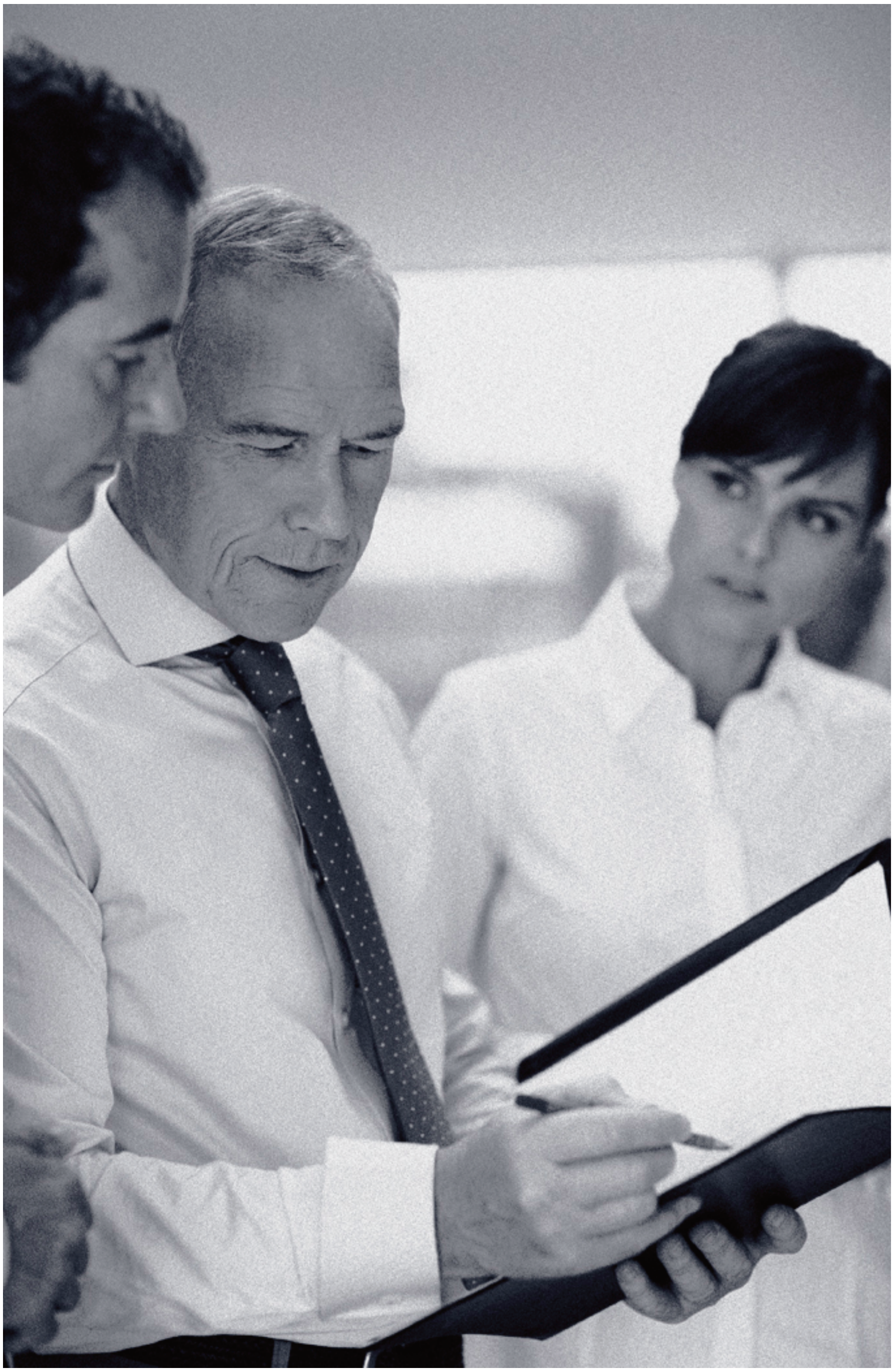
Principles for Improving Internal Audit's Value Proposition



All organizations depend on information to manage day-to-day operations, comply with regulations, gauge financial performance, and monitor strategic initiatives. This critical information resides in the organization's business records. As internal auditors conduct their annual risk assessment, they should consider how well business records are managed and assess the degree to which the risks to this information are understood.

As a key resource in the operation of any organization, records must be created, organized, secured, maintained, and used in a way that effectively supports the activity of that organization. This information facilitates day-to-day operations, supports activities such as budgeting and planning, answers questions about past decisions, and documents compliance with laws, regulations, and standards.

Increasingly, organizations must defend their recordkeeping practices to regulatory and other oversight organizations and respond to discovery demands. The risks are significant for those organizations with too much, too little, or incomplete information within their recordkeeping systems.

Excessive discovery costs for records that should have been disposed, regulatory sanctions against organizations that cannot produce required documentation, or poor business decisions based on incorrect or incomplete information are all risks that can be managed by effective records management processes.

Like any critical business process, these processes should be assessed as a part of the annual risk assessment and assured from time to time. Moreover, the assurance of an organization's recordkeeping processes provides an opportunity for internal audit to demonstrate how it can add value to this critical area of any business entity.

The Generally Accepted Recordkeeping Principles® (the Principles) and its Information Governance Maturity Model (IGMM) – both of which are consistent with The Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing (IAA Internal Audit Standards)* – are two broadly applicable frameworks designed to complement the internal audit risk assessment and assurance processes.

The Principles and IGMM, which are scalable to any size organization in any industry sector, are essential tools for the internal auditor to support any assurance or consulting engagements for an organization's records management processes.

An Overview of Internal Audit Standards

The IAA *Internal Audit Standards* has increased the focus over the past decade on the requirement to assure the risk management processes within an organization. Consider the definition of internal audit: "Internal auditing is an independent, objective assurance and consulting activity designed to *add value and improve an organization's operations.* It helps an organization accomplish its objectives by bringing *a systematic, disciplined approach to evaluate and improve the effectiveness of risk management,* control, and governance processes." [Emphasis added].

This definition is considered a mandatory part of the IIA *Internal Audit Standards,* so it is essential for internal auditors to consider holistically all risks to the organization as they perform their annual risk assessment out of which the annual audit plan will be developed.

IAA *Internal Audit Standards* "Performance Standard 2010 – Planning" expands on this definition of internal audit and requires that: "The chief audit executive must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization's goals."

The interpretation of this standard goes further: "The chief audit executive is responsible for developing a risk-based plan. The chief audit executive takes into account the organization's risk management framework…"

The critical information residing in the organization's business records poses significant risk if its governance has not been defined and communicated throughout the organization. Therefore, internal auditors have an opportunity to improve their value proposition by assessing the risks and assuring that the organization has robust records management processes with roles defined, understood, and supported by standards and metrics.

The IAA *Internal Audit Standards* provides the internal auditor specific direction in performance "Standard 2120 - Risk Management": "The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes."

The IAA *Internal Audit Standards* goes further in standard 2120.A1, which states: "The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:

- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations and programs;
- Safeguarding of assets; and
- Compliance with laws, regulations, policies, procedures, and contracts."

Standard 2120.A1 is very clear that financial and operational information integrity, how assets are safeguarded, and how compliance imperatives are met must be assessed for risk. All three of these areas are highly reliant on efficient and effective recordkeeping to protect organizations in the use of information.

Internal auditors can gain some insights into the maturity of the recordkeeping processes as they perform assurance and consulting engagements for operational and compliance processes. However, a recordkeeping process that provides reasonable assurance that risks are managed within an organization's risk appetite should be enterprise-wide. It is this enterprise-wide recordkeeping process that internal audit would be wise to assess.

The assurance of an organization's recordkeeping processes provides an opportunity for internal audit to demonstrate how it can add value to this critical area of any business entity.

Examples of Financial, Compliance Risks

There are several well-known examples of exposures in organizations' recordkeeping processes that have resulted in unnecessary expense, penalties levied by the courts, or fines imposed by regulatory bodies.

Cost of Producing More ESI than Needed

According to "Getting a Handle on eDiscovery" by information management solution provider StoredIQ, companies with $1 billion or more in revenue spend between $2.5 million and $4 million a year on legal discovery of electronic files alone. (Discovery is the legal process that companies in litigation are required to go through to produce relevant documents for the court to consider.)

Technology has contributed to the proliferation of electronically stored information (ESI) – and as much as 90 percent of it is unstructured and unmanaged, according to StoredIQ. Organizations without well-defined recordkeeping policies to manage the growth of this data will be at risk for significant litigation costs when they have to sort through it to respond to discovery requests.

A record retention policy that prescribes when to delete records can help manage discovery costs and limit corporate liability. As an example, StoredIQ pointed to a large court case involving DuPont. In an analysis afterward, DuPont estimated that more than half of the documents it produced for the case had exceeded their required retention period. Although DuPont had a retention policy, it didn't enforce it – and it cost the company $12 million for attorneys to review documents it should have previously disposed of.

New York Life: A Model of Excellence

There are organizations that recognize the need for a robust records management system and have partnered with internal audit to assure the records management process appropriately manages risks. New York Life is one of those organizations, and in 2008, it received for its efforts the Cobalt Award for organizational excellence in records and information management. The Cobalt award was created to recognize each year an organization that has excelled in embracing proper records and information management as a cornerstone of its compliance with laws and regulations, a critical element of its risk and asset management, and the foundation for its success.

New York Life has developed a records management policy that outlines roles and responsibilities of all stakeholders in the records management process. This policy maps to Generally Accepted Recordkeeping Principles® with a special focus on accountability, integrity, retention, and disposition, and it is applicable to both physical and electronic records.

New York Life created the Business Resilience Department in 2004 to centralize the oversight of records management that had previously been left to the individual business units to manage. Those business units still have accountability for their own records, but Business Resilience has responsibility to develop and monitor the records management policies and practices.

The small staff participates in employee orientation for all new employees in the New York area to brief them on records management policy. In addition, it works with all business areas to ensure consistency across the enterprise and relies on internal audit to assure the process on a three-year cycle, according to Jason Stearns, CRM, Corporate Records Manager for New York Life.

Danielle Arminio, Director-Audits, commented, "We have a records management audit program that is applied to most general audits to ensure compliance with corporate records management policies. We test to determine that New York Life business units and subsidiaries are holding and disposing of records according to corporate guidelines, with an emphasis on third parties acting on our behalf; New York Life takes records management very seriously." Arminio added that internal audit works closely with Corporate Records Management to report trends and raise issues as appropriate.

Failure to Find Relevant ESI

Morgan Stanley agreed to pay $15 million to settle a civil action brought by the U.S. Securities and Exchange Commission (SEC) for failing to produce tens of thousands of e-mails requested during SEC investigations from 2000 to 2005. In its complaint, the SEC said Morgan Stanley "did not diligently search for back-up tapes containing responsive e-mails until 2005. Morgan Stanley also failed to produce responsive e-mails because it overwrote back-up tapes."

William Malcolm, a data protection specialist with Pinsent Masons, the law firm behind *out-law.com*, says others should treat this as a wake-up call for good records management.

Adding to the problem of the explosive growth in records are the *Federal Rules of Civil Procedure (FRCP)* requirements for the production of ESI, as UBS Warburg learned when it was fined $29.2 million for failing to produce all relevant ESI.

In *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 312 (S.D.N.Y. 2003), what began as an employment discrimination action in federal court escalated after UBS Warburg produced only 100 e-mails in response to the plaintiff's request to produce "all documents concerning any communication by or between UBS employees concerning Plaintiff."

The plaintiff learned that UBS Warburg had not searched its back-up tapes containing archived e-mails, which provoked a long battle that resulted not only in monetary sanctions against UBS Warburg, but also an "adverse inference" instruction at trial.

Frameworks for Assuring Quality Recordkeeping Processes

It is incumbent, then, on internal auditors to be able to assure a company that its recordkeeping processes are consistent across all business units and that records are secured consistent with the regulatory and company policy requirements. As noted in the sidebar on page 3, New York Life exemplifies this approach – and it was recognized with the Cobalt Award for its excellence in records and information management. There are several tools available to internal auditors for assuring recordkeeping processes.

COSO ERM Framework

The Committee of Sponsoring Organizations of the Treadway Commission's (COSO) *Enterprise Risk Management - Integrated Framework* provides guidance for internal auditors to assess the four broad risk categories: strategic, reporting, operational, and compliance.

APQC Process Classification Framework

The APQC Process Classification Framework (PCF) is the world's most widely used process framework and allows organizations to speak a common language about functions, processes, and activities independent of structure. It is a broad inventory of processes that internal auditors can use to map their own auditable universe. With such a mapping, internal audit can determine where processes and risks to those processes might reside in their own organizations.

While performing the annual risk assessment, the chief audit executive should assess COSO's four risk categories and determine if coverage rules suggest a review of what the PCF Section 7.0 "Manage Information Technology," Part 7.4.4.3 labels: "Manage retention, revision, and retirement of enterprise information." (See *www.apqc.org.*)

The Principles and the IGMM

Internal audit's annual risk assessment should examine the risks within records management processes, and the Principles (see back of this page) provide the auditor with a robust framework to examine an organization's information governance risk and, ultimately, perform an assurance or consulting engagement.

The Principles enumerate eight concepts that are used in conjunction with the IGM (see *www.arma.org/principles*) to evaluate recordkeeping programs and practices. Together, they can be used to provide initial input to internal audit's risk assessment.

For each of the eight principles, the IGMM associates various characteristics that are typical for each of the five information governance maturity levels in the model: Level 1 – sub-standard, Level 2 – in development, Level 3 – essential, Level 4 – proactive, and Level 5 – transformational.

This assessment will determine the level of risk an organization has related to its information governance practices, and when an assurance engagement is performed, it can confirm that the organization will be able to defend its recordkeeping practices when required to do so by, for example, regulatory bodies, such as the U.S. Health and Human Services (related to the Health Information Portability and Accountability Act), Federal Deposit Insurance Corp., SEC (related to SOX), Environmental Protection Agency, and the Occupational Safety and Health Administration.

An Opportunity for Internal Audit

Records management is an area frequently overlooked when performing the annual risk assessment, yet excessive discovery costs, regulatory sanctions, and poor business decisions are risks that can be managed by effective records management processes. So, chief audit executives may want to reconsider how effectively their organizations protect their information assets and include the critical records management business process in their annual risk assessment.

The IGMM, which is based on the Principles, provides the tool and opportunity for internal auditors to demonstrate their value proposition. The IGMM will assist internal auditors and others to identify the gaps between an organization's current practices and the desirable level of information governance maturity. Most important for the internal auditor, the IGMM will assess the risks based on the largest gaps. The internal auditor can then determine what additional analysis may be required, perhaps scheduling an assurance or consulting engagement.

> **... excessive discovery costs, regulatory sanctions, and poor business decisions are risks that can be managed by effective records management processes.**

About the Author

James C. Key served as Director – Internal Audit for North America and Asia Pacific at IBM, as well as other internal audit roles, from 1987 – 1997. He has been the managing partner of Shenandoah Group since 1997, consulting on governance, risk management, and compliance solutions. Key is active in The Institute of Internal Auditors (IIA) in volunteer leadership roles, course development and delivery, and as primary facilitator in its executive development course for chief audit executives. He serves on a public company national bank board and sits on the audit, compliance, and risk committees. Key also serves on the audit committee of a not-for-profit organization. He can be contacted at jckey@hargray.com.

Generally Accepted Recordkeeping Principles®

Records and recordkeeping are inextricably linked with any organized activity. As a key resource in the operation of any organization, records must be created, organized, secured, maintained, and used in a way that effectively supports the activity of that organization, including:

- Facilitating and sustaining day-to-day operations
- Supporting predictive activities such as budgeting and planning
- Assisting in answering questions about past decisions and activities
- Demonstrating and documenting compliance with applicable laws, regulations, and standards

These needs can be fulfilled only if recordkeeping is an objective activity, insulated from individual and organizational influence or bias, and measured against universally applicable principles. To achieve this transparency, organizations must adhere to objective records and information management standards and principles, regardless of the type of organization, type of activity, or the type, format, or media of the records themselves. Without adherence to these standards and principles, organizations will have poorly run operations, legal compliance failures, and – potentially – a mask for improper or illegal activities.

Principle of Accountability

A senior executive (or a person of comparable authority) shall oversee the information governance program and delegate responsibility for records and information management to appropriate individuals. The organization adopts policies and procedures to guide personnel and ensure that the program can be audited.

Principle of Integrity

An information governance program shall be constructed so the information generated by or managed for the organization has a reasonable and suitable guarantee of authenticity and reliability.

Principle of Protection

An information governance program shall be constructed to ensure a reasonable level of protection for records and information that are private, confidential, privileged, secret, classified, or essential to business continuity or that otherwise require protection.

Principle of Compliance

An information governance program shall be constructed to comply with applicable laws and other binding authorities, as well as with the organization's policies.

Principle of Availability

An organization shall maintain records and information in a manner that ensures timely, efficient, and accurate retrieval of needed information.

Principle of Retention

An organization shall maintain its records and information for an appropriate time, taking into account its legal, regulatory, fiscal, operational, and historical requirements.

Principle of Disposition

An organization shall provide secure and appropriate disposition for records and information that are no longer required to be maintained by applicable laws and the organization's policies.

Principle of Transparency

An organization's business processes and activities, including its information governance program, shall be documented in an open and verifiable manner, and that documentation shall be available to all personnel and appropriate interested parties.

11880 College Blvd., Overland Park, KS 66210
913.341.3808 • 800.422.2762 • fax: 913.341.3742
headquarters@arma.org • www.arma.org/audit

*ARMA International (*www.arma.org*) is a not-for-profit professional association and the authority on managing records and information. Formed in 1955, ARMA International is the oldest and largest association for the records and information management profession and is known worldwide for setting records and information management (RIM) standards and best practices, and for providing comprehensive education, publications, and information on the efficient maintenance, retrieval, and preservation of information created in public and private organizations in all sectors of the economy.*