Generally Accepted Recordkeeping Principles®

http://www.arma.org/r2/generally-accepted-br-recordkeeping-principles

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.

Preamble

Information, and the systems and records containing it, are inextricably linked with any organized activity. They are a key element in the functioning of any organization, supporting, facilitating, and documenting:

- Day-to-day operations
- Predictive activities, such as budgeting and planning
- Responses to questions about past decisions and activities
- Compliance with applicable laws, regulations, and standards
- Accountability and transparency

In view of its importance, information must be created, organized, secured, maintained, and used in a way that effectively supports the activity of that organization and complies with any governance or information management duties it may have.

This can be achieved only if *information governance* – which Gartner defines as "an accountability framework that "includes the processes, roles, standards, and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals" – and *records* management – which ARMA International defines as the management of "any recorded information, regardless of medium or characteristics, made or received and retained by an organization in pursuance of legal obligations or in the transaction of business" – are:

- Objective processes
- Fully insulated from individual, organizational, political, or other biases
- Conducted through robust and repeatable processes
- Protected with suitable controls

This means that organizations, regardless of their type or activities, must subscribe to and implement governance standards and principles for governing information in all formats and on all media. Without adherence to these standards and principles, organizations can neither conduct their operations in the most efficient and effective manner possible, nor can they ensure or demonstrate that they are compliant with legislative and other legal requirements, as well as with other duties and responsibilities.

The Generally Accepted Recordkeeping Principles®

The principles of information governance, known as the Generally Accepted Recordkeeping Principles® (the Principles), are well-developed and well-understood by information governance and information management practitioners. The Principles, which are grounded in practical experience and based on extensive consideration and analysis of legal doctrine and information theory, form the basis upon which every effective information governance program is built , measured, and – regardless of whether or not an organization or its personnel are aware of them – will one day be judged.

Therefore, it is in the best interest of all organizations, and of society itself, to be fully aware of the Principles and to manage records and information assets in accordance with them.

ARMA International developed and published the Principles to foster general awareness of information governance standards and principles and to assist organizations in developing information management systems that comply with them.

The Principles are comprehensive in scope, but general in nature. They are not addressed to a specific situation, industry, country, or organization, nor are they intended to set forth a legal rule for compliance that must be strictly adhered to by every organization in every circumstance.

They are intended to set forth the characteristics of an effective information governance program, while allowing flexibility based upon the unique circumstances of an organization's size, sophistication, legal environment, and resources.

Thoughtful consideration of the Principles, combined with a reasonable approach when applying them, will yield sound results for any organization: a responsive, effective, and legally compliant information governance program and recordkeeping system.

Principle of Accountability
A senior executive (or a person of comparable authority) shall oversee the information governance program and delegate program 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.

- The senior executive in charge should establish a method to design and implement a structure to support the records and information governance program.
- Governance structure should be established for program development and implementation.
- Necessary components include an accountable person and a developed program.
- A records and information governance program should have documented and approved policies and procedures to guide its implementation.
- The records and information governance program should be structured for auditability as a means of demonstrating that the organization is meeting its obligations to both internal and external parties.

A basic premise of sound information governance is that within each organization, someone in a senior-level position is formally designated as responsible for the overall program. This does not have to be a full-time responsibility, but it must be held by a senior-level executive to ensure program implementation across the organization. The accountable senior executive will oversee the information governance program, although this person often will assign or designate other personnel to fill roles and do tasks, including managing the records and information management program.

A major responsibility for this executive is program development. Best practices require that the information governance program be monitored for compliance and to identify any areas requiring improvement. The matters identified during monitoring lead to program improvements, which the senior executive will oversee at the appropriate level.

Governance should be established throughout the organization, assigning defined roles and responsibilities to different staff so it is clear where responsibilities reside and how the chain of command works to build, implement, and upgrade the information governance program. For example, sub-committees can be designated to help build policies, define and implement technology, or improve the records and information management program.

For employees to know how to implement the information governance program, it is essential to have program policies and procedures that are documented, formally approved, and communicated to them. Updates to the policy and procedures should be available to staff, as should information governance training. All of this is designed to further standardize the program across the organization. This standardization enhances staff's efforts to effectively implement the information governance program.

Auditing is the process designed to prove the program is accomplishing its goals and to identify areas for improvement to further protect the organization and its information. Auditing should determine whether:

- Employees are able to demonstrate program awareness

- Information is being retained for the right amount of time and disposed of when no longer required
- Policies are up-to-date and cover all records media

An organization's information governance audit should be reported to the board of directors, its audit committee, or other appropriate governing body to show program adherence in accordance with documented policies and procedures, other requirements, and the organization's goals.

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

Integrity of records and information, which is expected by investors and government regulators alike, is directly related to the organization's ability to prove that they are *authentic*, meaning that their origin, time of creation or transmission, and content are what they are purported to be. It is necessary to maintain the authenticity of records in all media over time.

Integrity of records and information should include the following:
- Correctness of and adherence to the organization's policies and procedures
- Reliability of the information management and governance training and direction given to the employees who interact with all systems
- Reliability of the records and information created
- An acceptable audit trail
- Reliability of the systems that control information, including hardware, software, and infrastructure

Information Governance Policies and Procedures
Adherence to formal information governance policies and procedures that have been approved by senior management is essential to an organization's ability to achieve legal and regulatory compliance. If formal support has not been obtained, records may be at risk of not being accepted as having evidentiary value.

Reliability of Information Management and Governance Training
The organization shall provide training to all employees on the meaning and importance of and compliance with corporate policies and procedures.

Reliability of the Records Created
To ensure records are created, used, stored, and managed in the usual and ordinary course of business, organizations must have consistent information governance practices throughout the records life cycle.

Acceptable Audit Trails
Audit trails are essential in proving reliability of the information. Acceptable audit and quality assurance processes should be in place.

Reliability of the System
The information system must be reliable to prove reliability and integrity of the content. A record is only as trustworthy as the system in which it is maintained, so hardware, network infrastructure, software, and storage should be monitored. Media and systems migration, including all appropriate metadata, should be a part of maintaining a reliable information environment.

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

Information generated by an organization in the course of business requires various degrees of protection, as mandated by laws, regulations, or corporate governance. An organization's corporate governance would, for example, mandate protection to ensure that information critical to its continued operation during or after a crisis is available.

An information governance program must ensure that appropriate protection controls are applied to information from the moment it is created to the moment it undergoes final disposition. Therefore, every system that generates, stores, and uses information should be examined with the protection principle in mind.

Information protection takes multiple forms. First, each system must have an appropriate security structure so only personnel with the appropriate level of security or clearance can gain access to the information. This includes protecting electronic systems, as well as physical ones, using such measures as key card access restrictions and locked cabinets. This also requires that as personnel change jobs, their access controls are changed appropriately and immediately.

Second, this requires protecting information from "leaking" outside the organization, either by physical or electronic means. This includes ensuring that electronic information cannot be inappropriately e-mailed, downloaded, uploaded, or otherwise proliferated – intentionally or inadvertently – by people with legitimate access to the system. It is prudent to have such safeguards clearly defined in organizational policy and, if necessary, to monitor online sites for any postings that may violate this rule.

Where appropriate, controls and procedures for declassification of confidential and privileged information should be clearly defined and understood. There may be instances, however, when it is necessary to allow security clearance exceptions. For example, outside counsel engaged to assist with a litigation action may need to access records that they otherwise would not be cleared to access.

Security and confidentiality must be integral parts of the final disposition of information. Whether that disposition is an accession to an archive, transfer to another organization, preservation for permanent storage, or destruction, the Principle of Protection must be considered in defining the process. For example, the disposition of confidential paper files should be handled only by employees with appropriate clearance and in a manner that renders the information unrecoverable. As another example, classified government records must retain their classification for the appropriate number of years even if they are transferred to an archive.

Finally, an organization's audit program must have a clear process to determine whether sensitive information is being handled in accordance with the organization's policies and procedures.

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.

It is the duty of every organization to comply with applicable laws, including those for maintaining records and information. An organization's credibility and legal standing rest upon its ability to demonstrate that it conducts its activities in a lawful manner. The absence or poor quality of the records and information required to demonstrate this damages an organization's credibility and may impair its standing in legal matters or jeopardize its right to conduct business.

The duty of compliance affects a recordkeeping system in two ways:

1. The recordkeeping system must contain information showing that the organization's activities are conducted in a lawful manner.
2. The recordkeeping system is itself subject to legal requirements, such as maintaining tax or other records.

It follows from this that every organization must:

- Know what information must be entered into its records to demonstrate that its activities are being conducted in a lawful manner
- Enter that information into its records in a manner consistent with the law
- Maintain its records in the manner and for the time prescribed by law

An organization that is subject to codes of conduct, ethics rules, or other authorities is subject to a duty to comply with them as well. To the extent that recordkeeping is required to demonstrate compliance or that the organization's records system is itself subject to them, the organization's records must be maintained in accordance with these codes, rules, or authorities.

Policies are internal rules of conduct for the organization and the organization's own statements of what it deems to be correct conduct. By its nature, a policy imposes a duty of compliance upon the organization and its personnel. To comply with laws and other authorities, an organization must adopt and enforce suitable policies.

The precise manner and duties of compliance will vary from organization to organization. Some organizations may be subject to multiple laws and legal doctrines, as well as codes of ethics and other authorities. This may, in turn, require the organization to adopt and enforce multiple and stringent policies for information governance.

An organization that is subject to fewer regulations may need fewer information governance policies to maintain compliance. Every organization, however, should draft and enforce its policies and conduct its activities in a manner reasonably calculated to ensure compliance with the totality of authorities applicable to it.

The Principle of Availability

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

A successful and responsible organization must have the ability to identify, locate, and retrieve the records and information required to support its ongoing business activities. These records and information are used by:

- Individuals and groups to reference, share, and support their work
- Legal and compliance authorities for discovery and regulatory review purposes
- Numerous corporate functions to validate management decisions and account for the organization's resources

Having the right information available at the right time depends upon an organization's ability to nimbly search through enormous volumes of data. But, as more routine business transactions are being conducted in diverse electronic environments, effective information retrieval is becoming increasingly difficult to sustain. The individual flexibility these environments offer for organizing information also makes locating and retrieving it expensive, time-consuming, and labor-intensive. This is further complicated when the needed information was organized by departed employees or vendors who previously had custody of it.

Pinpointing complete and accurate information depends on having an efficient and intuitive set of methods and tools, including those described below, to organize it and providing employees and agents with sufficient training to utilize these tools successfully.

Metadata
Success begins with describing information during the capture, maintenance, and storage processes in such a way as to make retrieval effective and efficient. A routine approach for capturing this descriptive information, or *metadata*, must be documented and utilized in all applicable systems.

Backups, Conversion, Migration
Because media on which electronic information is recorded is inherently fragile and impermanent, this information needs to be backed up routinely to ensure that it can be restored if there is a disaster, a system malfunction, or data corruption. It also needs to be periodically migrated to current supported hardware and/or converted with current software to new versions and/or formats to sustain its on-going accessibility.

Routine Disposition
To effectively manage the availability of its information assets at a reasonable cost, an organization should – in the normal course of business – regularly remove obsolete or redundant records and information. This will make the remaining information, which has on-going value to the organization, more identifiable and accessible, enhance system performance, and reduce the maintenance costs of storage, backup, and migration.

However, removing unneeded information should occur in adherence with the organization's information retention policies, which should also provide for suspending its disposition in the event of pending or ongoing legal process, audit, or, where appropriate, freedom of information requests.

Well-Designed Storage
An organization's personnel are more likely to retrieve and use information for better decision making and more effective work if it has well-designed storage processes and access to understandable, retrievable, relevant, and consistent information. With properly structured information, personal productivity is improved, storage costs are minimized, and the reliability and speed of retrieval are optimized.

Further, complete and accessible records and information in a well-managed environment minimize inconsistent and erroneous interpretation of the facts, simplify legal processes and regulatory investigations, and protect valuable information from being lost, corrupted, or stolen.

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.

Records and information document an organization's business operations and are essential to effectively managing that business. The ability to properly and consistently retain all information is especially important today, as organizations are creating and storing enormous quantities – most of it in electronic form.

To control information volume, an organization needs a records retention program that will define for it what information to retain, how long to maintain it, and when and how to dispose of it when it is no longer required. This is based on the concept that information has a *life cycle*, which begins at its creation and ends at its final disposition.

As part of its retention program, an organization must develop a *records retention* schedule, which specifies what business records and information must be retained and for what length of time. Retention decisions

are based on the information content and the organization's legal, regulatory, fiscal, operational, and historical requirements for that content.

- **Legal and regulatory** – Local, national, and international laws mandate the retention of records and information for a specific (generally, the minimum) period of time. To comply with these extensive laws and regulations, an organization must conduct legal research in consultation with legal counsel to determine all retention requirements. Failure to comply may result in costly penalties and loss of legal rights.

- **Fiscal –** Records and information that have financial or tax value must be retained to ensure the timely payment of obligations and the proper receipt of receivables, as well as to support the organization's financial audits and tax returns. Legal research and consultation with legal counsel must be completed to satisfy fiscal retention requirements.

- **Operational** –An organization must determine how long records and information are needed to satisfy its business needs. This is usually determined by interviewing those most knowledgeable about the operational value of each record type.

- **Historical –** Records and information that depict the history of an organization should be preserved for the life of that organization. Examples of historical records include articles of incorporation, bylaws, charters, and boards of directors' minutes. Historical records normally constitute a very small percentage of an organization's total records volume.

Once the retention requirements listed above are determined, an organization must conduct a risk assessment to determine the appropriate retention period for each type of record. Retention decision makers must be aware that the presence or absence of records can be either helpful or harmful to the organization. Therefore, to minimize risks and costs associated with retention, it is essential to immediately dispose of records and information after their retention period expires.

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.

At the completion of their retention period, an organization's records and information must be designated for disposition. In many cases, the appropriate disposition will be destruction of the information, in which case the organization must ensure that it is transported securely and destroyed completely and irreversibly.

In other cases, the records and information may be returned to clients, transferred to another organization in connection with a divestiture, or transferred for ongoing preservation to an historical archives, library, or museum. The disposition of records and information by transferring to an historical archives, library, or museum should be governed by appraisal by a qualified professional. All transfers should be documented as part of the organization's retention policy

If records and information are converted or migrated to new media, disposition of the previous media may also be warranted. In all instances, the organization must make a reasonable effort to ensure that all versions and copies of the records and information are accounted for in the disposition. The organization must also document its disposition process.

A duty to suspend disposition may arise in the event of litigation or a regulatory action. The organization should designate records and information that are to be held pending resolution of the litigation or audit and notify all affected personnel when a hold is issued and when it is released.

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.

Many parties have a legitimate interest in understanding the program activities and processes that govern an organization's records and information. In addition to the organization itself and its personnel, those parties include, but are not limited to, government authorities, auditors and investigators, litigants, and, for some organizations, the general public.

It should be evident, then, that it is in an organization's best interest to ensure that its:

- Activities are conducted in a lawful and appropriate manner
- Records and information management system accurately and completely records its activities
- Records and information management system is structured in a lawful and appropriate manner
- Records and information management program activities are conducted in a lawful and appropriate manner

The clearest and most durable evidence of the organization's operations, decisions, and activities are records and information. A records and information management program includes recordkeeping policies and procedures and control over its transactional records. To ensure the confidence of interested parties, records documenting the records and information management program must themselves adhere to the fundamentals of records management. They should:

- Document the principles and processes that govern the program
- Accurately and completely record the activities undertaken to implement the program
- Be written or recorded in a manner that clearly sets forth the information recorded
- Be readily available to legitimately interested parties

The information documented in these records and the extent to which they are available to interested parties will vary depending upon the circumstances of the organization.

An organization that is subject to open records laws may need to make all records available to any person upon request. Other organizations may have a legitimate need to protect confidential or proprietary information, and they may therefore reasonably put in place procedures designed to control access to information.

Complex and highly regulated records and information management systems may require extensive records documenting them. Simple systems may require only a few. In each case, however, the rationales and outcomes should be clear to legitimately interested parties.

Every organization must therefore create and manage the records documenting its records and information management program and program activities to ensure that its structure, processes, and activities are apparent, understandable, and reasonably available to legitimately interested parties.