Generally Accepted Recordkeeping Principles®

Information Governance Maturity Model

Information is one of the most vital strategic assets any organization possesses. Organizations depend on information to develop products and services, make critical strategic decisions, protect property rights, propel marketing, manage projects, process transactions, serve customers, and generate revenues. In short, well-governed information is critical to the success of any organization.

Despite its importance, there is often uncertainty and disagreement about what constitutes good *information governance* – which Gartner Inc. describes 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 even more uncertainty as to how to achieve it.

Yet, this issue gains in importance daily as regulators, shareholders, courts, and constituents are increasingly concerned about organizations' business practices and the *records* – which are defined as "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" – and the non-record information that support and document those practices.

In addition, society as a whole is concerned about governmental and business transparency and other information-related issues, such as privacy and security of personal information. These concerns are magnified by ever-growing data volumes and complexity that demand increasingly sophisticated governance and management.

To address these needs, ARMA International developed and promulgated the Generally Accepted Recordkeeping Principles® (the Principles).

THE PRINCIPLES
GENERALLY ACCEPTED
RECORDKEEPING PRINCIPLES®

An Information Governance Standard

The Principles identify the critical hallmarks of information governance and provide both a standard of conduct for governing information and metrics by which to judge that conduct. In doing so, they give assurance to the public and society at large that organizations of every kind are meeting their responsibilities with respect to the governance of information.

Because the Principles describe and measure fundamental attributes of information governance, they apply to all sizes of organizations, in all types of industries, and in both the private and public sectors. And, because the Principles are independent of local law and custom, multi-national organizations can use them to establish consistent practices across geographic boundaries.

The Principles are essential for:

- **Administrators and executive management** in determining how to protect their organizations in the use of information assets
- **Legislators** in crafting legislation meant to provide certainty in business and public affairs and to hold organizations accountable to appropriate standards of conduct
- **Information management professionals** in designing comprehensive and effective information governance programs
- **Information workers** in performing their day-to-day duties

A Model for Effective Information Governance

The Generally Accepted Recordkeeping Principles® (the Principles) create a high-level framework of good practice. However, they do not delve into implementation details, such as specific policies and procedures, job descriptions, or specific technologies. The Information Governance Maturity Model (Maturity Model) – which is based on the Principles, as well as the established body of standards, best practices, and legal/regulatory requirements that surround information governance – begins to paint a more complete picture of what effective information governance is.

The Maturity Model goes beyond a mere restatement of the Principles, defining the characteristics of information governance programs at differing levels of maturity, completeness, and effectiveness. For each of the eight principles, the Maturity Model describes characteristics that are typical for its five levels of maturity:

- **LEVEL 1 (Sub-Standard):** This level describes an environment where information governance and recordkeeping concerns are not addressed at all, are addressed minimally, or are addressed in an *ad hoc* manner. Organizations that identify primarily with these descriptions should be concerned that their programs will not meet legal or regulatory scrutiny and may not effectively serve the business needs of the organization.
- **LEVEL 2 (In Development):** This level describes an environment where there is a developing recognition that information governance and prudent recordkeeping have an impact on the organization and that the organization may benefit from a more defined information governance program. However, in Level 2, the organization is still vulnerable to scrutiny of its legal or regulatory and business requirements because its practices are ill-defined, incomplete, nascent, or only marginally effective.
- **LEVEL 3 (Essential):** This level describes the essential, or minimum, requirements that must be addressed to meet the organization's legal, regulatory, and business requirements. Level 3 is characterized by defined policies and procedures and the implementation of processes specifically intended to improve information governance and recordkeeping. Organizations that identify primarily with Level 3 descriptions still may be missing significant opportunities for streamlining business and controlling costs, but they have the key basic components of a sound program in place and are likely to be at least minimally compliant with legal, operational, and other responsibilities.

- **LEVEL 4 (Proactive):** This level describes an organization that has established a proactive information governance program throughout its operations and has established continuous improvement for it. Information governance issues and considerations are routinely integrated into business decisions. The organization is substantially more than minimally compliant with good practice and easily meets its legal and regulatory requirements. The entity that identifies primarily with these descriptions should begin to pursue the additional business and productivity benefits it could achieve by increasing enterprise-wide information availability, mining its information for a better understanding of clients' and customers' needs, and otherwise transforming itself through increased use of its information.
- **LEVEL 5 (Transformational):** This level describes an organization that has integrated information governance into its overall corporate infrastructure and business processes to such an extent that compliance with program requirements and legal, regulatory, and other responsibilities are routine. This organization has recognized that effective information governance plays a critical role in cost containment, competitive advantage, and client service, and it has successfully implemented strategies and tools to achieve these gains on a plenary basis.

As a program progresses, the personnel charged with its management will likewise progress through a spectrum of increasing competence and effectiveness. At the transformational level, the information governance professional has a sophisticated skill set that encompasses a broad range of topics, including information theory and practice, technologies, and legal compliance.

How to Use the Maturity Model

Using the Maturity Model is the first in a series of steps an organization should take to evaluate and improve its information governance programs and practices. An in-depth understanding of the Principles and the Maturity Model levels will help the organization target the optimum level to achieve in relation to each principle.

Based on defined business needs and risk assessments, an organization may choose to target different levels of maturity for each of the eight principles and for different areas of the organization. However, no entity should be satisfied with being at a maturity level of 1 or 2 in any area because this presents substantial risk to the overall organization.

After deciding whether to evaluate the entire organization or a portion of it (e.g., department, division, or geographic location), the following initial steps are recommended:

1. Based on a thorough understanding of the Principles, the Maturity Model, and the organization's operating needs, target a specific maturity level for each of the principles.
2. Using the Maturity Model, determine the maturity level of current practices and identify the gap between the current practices and the desired maturity level for each principle.
3. Based upon the greatest maturity gaps, most available improvement opportunities, and other relevant information, assess the risk(s) to the organization and the opportunities for greatest benefit.
4. Develop priorities and assign accountability for suitable remediation and improvement strategies and processes.
5. Implement a process to ensure continuous improvement through routine monitoring and periodic assessments.

Since referencing the Maturity Model alone is a high-level evaluation, a more in-depth analysis likely will be necessary in order to develop the most effective improvement strategy. Obtaining the desired improvement will require a continuous focus, commitment to an ongoing improvement process, and periodic evaluations of the program against the Maturity Model.

Information Governance Maturity Model

The Principle	LEVEL 1 (Sub-Standard)	LEVEL 2 (In Development)
Accountability A senior executive (or 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.	No senior executive (or person of comparable authority) is responsible for records or information. The records manager role is largely non-existent, or it is an administrative and/or clerical role distributed among general staff. Information assets are managed in a disparate fashion or not at all.	No senior executive (or person of comparable authority) is involved in or responsible for records or information. The records manager role is recognized, although the person in that role is responsible only for tactical operation of the existing records management program, which is concerned primarily with managing records rather than all information assets. In many cases, the existing records management program covers paper records only. The information technology function or department is the *de facto* lead for storing electronic information, and the records manager is not involved in discussions about electronic systems. Information is not stored in a systematic fashion. The organization is aware that it needs to govern its broader information assets.
Transparency An organization's business processes and activities, including its information governance program, shall be documented in an open and verifiable manner, and the documentation shall be available to all personnel and appropriate interested parties.	It is difficult to obtain timely information about the organization, its business, or its records management program. Business and records and information management processes are not well-defined, and no clear documentation regarding these processes is readily available. There is no emphasis on transparency. The organization cannot readily accommodate requests for information, discovery for litigation, regulatory responses, freedom of information, or other requests (e.g., from potential business partners, investors, or buyers). The organization has not established controls to ensure the consistency of information disclosure.	The organization realizes that some degree of transparency is important in its business processes and records and information management program for business or regulatory needs. Although a limited amount of transparency exists in areas where regulations demand it, there is no systematic or organization-wide drive to transparency. The organization has begun to document its business and records and information management processes.
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.	There are no systematic audits or defined processes for showing the authenticity of a record or information, meaning that its origin, time of creation or transmission, and content are what they are purported to be. Various organizational functions use *ad hoc* methods to demonstrate authenticity and chain of custody, as appropriate, but their trustworthiness cannot easily be guaranteed.	Some organizational records and information are stored with their respective metadata that demonstrate authenticity; however, no formal process is defined for metadata storage and chain of custody. Metadata storage and chain of custody methods are acknowledged to be important, but they are left to the different departments to handle as they determine is appropriate.
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, essential to business continuity, or that otherwise require protection.	No consideration is given to information protection. Records and information are stored haphazardly, with protection taken by various groups and departments and with no centralized access controls. Access controls, if any, are assigned by the author.	Some protection of information assets is exercised. There is a written policy for records and information that require a level of protection (e.g., personnel records). However, the policy does not give clear and definitive guidelines for all information in all media types. Guidance for employees is not universal or uniform. Employee training is not formalized. The policy does not address how to exchange these records and information among internal or external stakeholders. Access controls are implemented by individual content owners.

Note: Records management terms used in the Generally Accepted Recordkeeping Principles® Information Governance Maturity Model are defined in the *Glossary of Records and Information Management Terms, 3rd Edition* (ARMA International, 2007).

LEVEL 3 (Essential)	LEVEL 4 (Proactive)	LEVEL 5 (Transformational)
The records manager role is recognized within the organization, and the person in that role is responsible for the tactical operation of the established records management program on an organization-wide basis. The organization includes electronic records as part of the records management program. The records manager is actively engaged in strategic information and records management initiatives with other officers of the organization. Senior management is aware of the records management program. The organization envisions establishing a broader-based information governance program to direct various information-driven processes throughout the enterprise. The organization has defined specific goals related to accountability.	The organization has appointed an information governance professional, who also oversees the records management program. The records manager is a senior officer responsible for all tactical and strategic aspects of the records management program, which is an element of an information governance program. A stakeholder committee representing all functional areas meets on a periodic basis to review disposition policy and other records management-related issues.	The organization's senior management and its governing board place great emphasis on the importance of information governance. The records manager directs the records management program and reports to an individual in the senior level of management, (e.g., chief information governance officer) The chief information governance officer and the records manager are essential members of the organization's governing body. The organization's initial goals related to accountability have been met, and it has an established process to ensure its goals for accountability are routinely reviewed and revised.
Transparency in business and records and information management is taken seriously, and information is readily and systematically available when needed. There is a written policy regarding transparency in business and records and information management. Employees are educated on the importance of transparency and the specifics of the organization's commitment to transparency. The organization has defined specific goals related to information governance transparency. Business and records and information management processes are documented. The organization can accommodate most requests for information, discovery for litigation, regulatory responses, freedom of information, or other requests (e.g., from potential business partners, investors, or buyers).	Transparency is an essential part of the corporate culture and is emphasized in training. The organization monitors compliance on a regular basis. Business and records and information management process documentation is monitored and updated consistently. Requests for information, discovery for litigation, regulatory responses, freedom of information, or other requests (e.g., from potential business partners, investors, or buyers) are managed through routine business processes.	The organization's senior management considers transparency as a key component of information governance. The software tools that are in place assist in transparency. Requestors, courts, and other legitimately interested parties are consistently satisfied with the transparency of the processes and the organization's responses. The organization's initial goals related to transparency have been met, and it has an established process to ensure its goals for transparency are routinely reviewed and revised.
The organization has a formal process to ensure that the required level of authenticity and chain of custody can be applied to its systems and processes. Appropriate data elements to demonstrate compliance with the policy are captured. The organization has defined specific goals related to integrity.	There is a clear definition of metadata requirements for all systems, business applications, and records that are needed to ensure the authenticity of records and information. Metadata requirements include security and signature requirements and chain of custody as needed to demonstrate authenticity. The metadata definition process is an integral part of the records management practice in the organization.	There is a formal, defined process for introducing new record-generating systems, capturing their metadata, and meeting other authenticity requirements, including chain of custody. Integrity controls of records and information are reliably and systematically audited. The organization's initial goals related to integrity have been met, and it has an established process to ensure its goals for integrity are routinely reviewed and revised.
The organization has a formal written policy for protecting records and information, as well as centralized access controls. Confidentiality and privacy considerations are well-defined within the organization. The importance of chain of custody is defined, when appropriate. Training for employees is available. Records and information audits are conducted only in regulated areas of the business. Audits in other areas may be conducted, but they are left to the discretion of each functional area. The organization has defined specific goals related to records and information protection.	The organization has implemented systems that provide for the protection of the information. Employee training is formalized and well-documented. Auditing of compliance and protection is conducted on a regular basis.	Executives and/or senior management and other governing bodies (e.g., board of directors) place great value in the protection of information. Audit information is regularly examined, and continuous improvement is undertaken. Inappropriate or inadvertent information disclosure or loss incidents are rare. The organization's initial goals related to protection have been met, and it has an established process to ensure its goals for protection are routinely reviewed and revised.

Information Governance Maturity Model

The Principle	LEVEL 1 (Sub-Standard)	LEVEL 2 (In Development)
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.	There is no clear understanding or definition of the information or records the organization is obligated to keep. Information is not systematically managed. Groups and units within the organization manage information as they see fit based upon their own understanding of their responsibilities, duties, and what the appropriate requirements are. There is no central oversight or guidance and no consistently defensible position on information governance. There is no formally defined or generally understood process for imposing legal, audit, or other information production processes. The organization has significant exposure to adverse consequences from poor compliance practices.	The organization has identified some of the rules and regulations that govern its business and introduced some compliance policies and good information management practices around those policies. Policies are not complete, and there are no structured accountability processes or controls for compliance. There is a hold process, but it is not well-integrated with the organization's information management and discovery processes, and the organization does not have full confidence in it.
Availability An organization shall maintain records and information in a manner that ensures timely, efficient, and accurate retrieval of needed information.	Records and other information are not readily available when needed, and/or it is unclear who to ask when there is a need for it to be produced. It takes time to find the correct version, the signed version, or the final version of information, if it can be found at all. The records and other information lack finding aids, such as various indices, metadata, and other methodologies. Legal discovery and information requests are difficult because it is not clear where information resides or where the final copy is located.	Records and information retrieval mechanisms have been implemented in some parts of the organization. In those areas with retrieval mechanisms, it is possible to distinguish among official records, duplicates, and non-record information. There are some policies on where and how to store official records and information, but a standard is not imposed across the organization. Responding to legal discovery and information requests is complicated and costly due to the inconsistent treatment of information.
Retention An organization shall maintain its records and information for an appropriate time, taking into account its legal, regulatory, fiscal, operational, and historical requirements.	There is no current, documented records retention schedule or policy. Rules and regulations that should define retention are not identified or centralized. Retention guidelines are haphazard, at best. In the absence of retention schedules and policies, employees either keep everything or dispose of records and information based on their own business needs, rather than organizational needs.	A retention schedule and policies are available, but they do not encompass all records and information, did not go through an official review, and are not well known around the organization. The retention schedule and policies are not regularly updated or maintained. Education and training about the retention policies are not available.
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.	There is no documentation of the processes (if there are any) used to guide the transfer or disposition of records and information. The process for suspending disposition in the event of investigation or litigation is non-existent or is inconsistent across the organization.	Preliminary guidelines for disposition are established. There is a realization of the importance of suspending disposition in a consistent manner, when required. There may not be enforcement and auditing of disposition.

Note: Records management terms used in the Generally Accepted Recordkeeping Principles® Information Governance Maturity Model are defined in the *Glossary of Records and Information Management Terms, 3rd Edition* (ARMA International, 2007).

LEVEL 3 (Essential)	LEVEL 4 (Proactive)	LEVEL 5 (Transformational)
The organization has identified key compliance laws and regulations. Information creation and capture are in most cases systematically carried out in accordance with information management principles. The organization has a code of business conduct that is integrated into its overall information governance structure and policies. Compliance is highly valued and measurable, and suitable records and information demonstrating the organization's compliance are maintained. The hold process is integrated into the organization's information management and discovery processes for the critical systems, and it is generally effective. The organization has defined specific goals related to compliance. The organization's exposure to adverse consequences from poor information management and governance practices is reduced.	The organization has implemented systems to capture and protect information for all key repositories and systems. Records are linked with the metadata used to demonstrate and measure compliance. Employees are trained appropriately, and audits are conducted regularly. Lack of compliance is consistently remedied through implementation of defined corrective actions. Records of audits and training are available for review. The legal, audit, and information production processes are well-managed and effective, with defined roles and repeatable processes that are integrated into the organization's information governance program. The organization is at low risk of adverse consequences from poor information management and governance practices.	The importance of compliance and the role of records and information in it are clearly recognized at the senior management and governing body levels (e.g., board of directors). Auditing and continuous improvement processes are well-established and monitored by senior management. The roles and processes for information management and discovery are integrated, and those processes are well-developed and effective. The organization suffers few or no adverse consequences based on information governance and compliance failures. The organization's initial goals related to compliance have been met, and it has an established process to ensure its goals for compliance are routinely reviewed and revised.
There is a standard for where and how records and information are stored, protected, and made available. There are clearly defined policies regarding the handling of records and information. Records and information retrieval mechanisms are consistent and contribute to timely retrieval. Most of the time, it is easy to determine where to find the authentic and final version of any information. Legal discovery and information request processes are well-defined and systematic. Systems and infrastructure contribute to the availability of records and information. The organization has defined specific goals related to availability of records and information.	Information governance policies have been clearly communicated to all employees and other parties. There are clear guidelines and an inventory that identify and define the systems and their information assets. Records and information are consistently and readily available when needed. Appropriate systems and controls are in place for legal discovery and information requests. Automation is adopted to facilitate the consistent implementation of the hold and information request processes.	The senior management and governing body (e.g., board of directors) provide support to continually upgrade the processes that affect records and information availability. There is an organized training and continuous improvement program across the organization. There is a measurable return on investment to the organization as a result of records and information availability. The organization's initial goals related to availability have been met, and it has an established process to ensure its goals for availability are routinely reviewed and revised.
The organization has instituted a policy for records and information retention. A formal retention schedule that is tied to rules and regulations is consistently applied throughout the organization. The organization's employees are knowledgeable about the retention policy, and they understand their personal responsibilities for records and information retention. The organization has defined specific goals related to retention.	Employees understand how to classify records and information appropriately. Retention training is in place. Retention schedules are reviewed on a regular basis, and there is a process to adjust retention schedules, as needed. Records and information retention is a major organizational objective.	Retention is an important item at the senior management and governing body level (e.g., board of directors). Retention is looked at holistically and is applied to all information in an organization, not just to official records. Information is consistently retained for appropriate periods of time. The organization's initial goals related to retention have been met, and it has an established process to ensure its goals for retention are routinely reviewed and revised.
Official procedures for records and information disposition and transfer have been developed. Official policy and procedures for suspending disposition have been developed. Although policies and procedures exist, they may not be standardized across the organization. The organization has defined specific goals related to disposition.	Disposition procedures are understood by all and are consistently applied across the enterprise. The process for suspending disposition is defined, understood, and used consistently across the organization. Records and information in all media are disposed of in a manner appropriate to the information content and retention policies.	The disposition process covers all records and information in all media. Disposition is assisted by technology and is integrated into all applications, data warehouses, and repositories. Disposition processes are consistently applied and effective. Processes for disposition are regularly evaluated and improved. The organization's initial goals related to disposition have been met, and it has an established process to ensure its goals for disposition are routinely reviewed and revised.

ARMA INTERNATIONAL®

www.arma.org

For education and resources on the Generally Accepted Recordkeeping Principles®, visit ***www.arma.org/principles.***

ARMA International has a variety of additional resources and assessment tools that are designed to help organizations improve their information governance practices available at ***www.arma.org***.