

# ARMA International Draft Maturity Model

GARP <sup>SM</sup>	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
<p><b>Accountability</b> An organization shall assign a senior executive who will oversee a recordkeeping program and delegate program responsibility to appropriate individuals, adopt policies and procedures to guide personnel, and ensure program audit ability.</p>	<p>No senior executive(s) responsible for the records management program. Records manager role is at worst largely non-existent or at best an administrative and/or clerical role distributed amongst general staff.</p>	<p>No senior executive(s) involved or responsible for the program. Corporate records manager role is recognized and he/she responsible for tactical operation of the existing program. In many cases, this covers paper records only. The Information technology department is the de facto lead for storing electronic information, but this is not done in a systematic fashion.</p>	<p>Corporate Records Manager is an officer role and responsible for tactical operation of ongoing program. He/she is actively engaged in strategic information and record management initiatives with other corporate officers of the organization. Senior management is aware of the program.</p>	<p>Corporate records manager is a senior officer responsible for all tactical and strategic aspects of the program. Stakeholder committee represented by all business units and chaired by the records manager meets on a periodic basis to review disposition eligibility lists and other records management related issues. Records management activities fully sponsored by senior executives of the organization.</p>	<p>Same as level 4 or alternately, the Chief Risk and Compliance Officer is responsible for the RM function. Alternately, there is a Chief Corporate Records Officer. The C level executives and the board place great emphasis on the importance of the program.</p>
<p><b>Transparency</b> The processes and activities of an organization's record-keeping program shall be documented in an understandable manner and be available to all personnel and appropriate interested parties.</p>	<p>It is virtually impossible to obtain information about the organization or its records in a timely fashion. There is no clear documentation and it is not readily available . . . There is no emphasis on transparency. It is not clear how the organization operates. Public requests for information, discovery for litigation or regulatory purposes, or other requests such as from potential business partners, investors or buyers cannot be readily accommodated.</p>	<p>The organization realizes that some degree of transparency is important in their recordkeeping either for business or regulatory needs. In certain areas where regulations demand transparency. There is no systematic drive to transparency.</p>	<p>Transparency is taken seriously and information is readily and systematically available when needed. There is a policy with regard to transparency and employee education is in place.</p>	<p>Same as 3. In addition, transparency is part of the corporate culture and is emphasized in training. Compliance is monitored on a regular basis. The company recognizes how transparency helps them with their business, legal, and compliance issues.</p>	<p>Same as 4. In addition, the C level and board consider transparency as key component of information governance. There is a continuous improvement process in place. Software tools are in place to assist transparency.</p>
<p><b>Integrity</b> A recordkeeping program shall be constructed so the records and information generated or managed by or for the organization have a reasonable and suitable guarantee of authenticity and reliability.</p>	<p>There are no systematic audits, and no defined process for showing the origin and authenticity of a record. Various organizational functions use ad hoc methods to demonstrate authenticity and chain of custody, as appropriate, but their trustworthiness cannot be easily guaranteed.</p>	<p>Some organizational records are stored with their respective metadata that demonstrates authenticity, however, no formal process is defined for such metadata storage and chain of custody, as appropriate. It is done differently in various departments within the organization.</p>	<p>Organization has a metadata taxonomy definition for use by all systems and processes as required to demonstrate authenticity and an established chain of custody policy.</p>	<p>There is a clear definition of metadata requirements for all systems, business applications, and paper records that are needed to ensure the authenticity of records. This includes security/signature requirements and chain of custody, as appropriate requirements to demonstrate authenticity. This process is an integral part of the records management practice in the organization.</p>	<p>Same as level 4, but in addition, there is a process for introduction of new record generating systems and the capture of their meta data and other authenticity requirements, including chain of custody, as appropriate.</p>
<p><b>Protection</b> A recordkeeping program shall be constructed to ensure a reasonable level of protection to records and information that are private, confidential, privileged, secret, or essential to business continuity</p>	<p>No consideration is given to record privacy. Records are stored haphazardly, with protection taken by various groups and departments with no centralized access controls. Access controls, if any, are assigned by the author.</p>	<p>Some protection of records is exercised. There is a written policy for records that require a level of protection, such as personnel records, however the policy does not give clear and definitive guidelines for all records in all media types. Guidance for employees is not universal or uniform. The policy does not address how to exchange these records between employees. Employee training is not formalized. Access controls are still implemented by individual record owners.</p>	<p>The organization has a formal written policy for protecting records and centralized access controls. Confidentiality and privacy are well defined. Importance of chain of custody, as appropriate, is defined. Training for employees is available. No auditing for compliance is done.</p>	<p>Same as level 3. In addition, there are systems in place 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.</p>	<p>Same as level 4, but in addition, executives and the board place great value in the protection of information. Audit information is regularly examined and continuous improvement is undertaken.</p>
<p><b>Compliance</b> The recordkeeping program shall be constructed to comply with applicable laws and other binding authorities, as well as the organization's policies.</p>	<p>There is no clear definition of the records that the organization is obligated to keep. Records and other business documentation are not systematically managed according to records management principles. Various groups of the organization define this to the best of their ability based on their interpretation of rules and regulations. There is no central oversight and no consistently defensible position.</p>	<p>The organization has identified the rules and regulations that govern its business and introduced some compliance policies and record keeping practices around those policies. However, the policies are not complete and there is no apparent or well defined accountability for compliance.</p>	<p>The organization has identified all relevant compliance laws and regulations. Record creation and capture are systematically carried out and in accordance with records management principles. In addition, the organization has a strong code of business conduct which is also incorporated into the business. Compliance and the records that demonstrate that compliance are highly valued and measurable.</p>	<p>Same as level 3. In addition, there are systems in place that help capture and protect records. The records are linked with metadata used to demonstrate and measure compliance. Employees are trained appropriately and audits are conducted regularly. Records of the audits and training are available for review. Lack of compliance is remedied through various avenues.</p>	<p>Same as level 4. In addition, the importance of compliance and the records that demonstrate it are recognized clearly at the C and board levels. Auditing and continuous improvement processes are well established.</p>
<p><b>Availability</b> An organization shall maintain records in a manner that ensures timely, efficient, and accurate retrieval of needed information.</p>	<p>Records are not readily available when needed and/or it is unclear who to ask when records need to be produced. It takes time to find the correct version, the signed version or the final version if it can be found at all. The records lack finding aides: indices, metadata, and locators. Record inventories are practically non-existent. Discovery is difficult since it is not clear where information resides or where the copy of record is.</p>	<p>Record retrieval mechanisms have been implemented in certain areas of the organization. In those areas, record inventories are up to date and it is possible to distinguish between official records, duplicates, and non-record materials. However, this is inconsistent throughout the organization. There are some policies on where and how to store 'official' records, but the standard is not readily imposed. Discovery is complicated by the inconsistent treatment of information.</p>	<p>There is a definition of where and how records are stored and official information is protected and available. Record retrieval mechanisms are consistent and timely Most of the time it is clear to the organization where to find the authentic and final version. Discovery is a well defined and systematic business process.</p>	<p>There are clearly defined policies re storage of final records. There are clear guidelines and a data map that define systems of record. Appropriate systems are in place for discovery and automation is adopted.</p>	<p>Same as level 4. In addition, there is C level and board level support to continually upgrade the processes that effect record availability. There is an organized training and continuous improvement program.</p>
<p><b>Retention</b> An organization shall maintain its records and information for an appropriate time, taking into account legal, regulatory, fiscal, operational, and historical requirements.</p>	<p>There is no current documented records retention schedule. Rules and regulations that should define retention are not identified or centralized. Retention guidelines are haphazard at best. In the absence of retention schedules, employees either keep everything or dispose of records based upon individual rather than organizational needs.</p>	<p>A retention schedule is available, but it does not encompass all records, did not go through official review, and it is not well known around the organization. Education and training about the retention policies is not available.</p>	<p>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 schedule and they understand their personal responsibilities for records retention.</p>	<p>Same as 3. In addition, it is clear to employees how to classify records appropriately and 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 retention is a major corporate concern.</p>	<p>Same as 4. In addition, retention is important item at the C and board levels. Retention is looked at holistically, and is applied, not just to official records, but to all content in an organization.</p>
<p><b>Disposition</b> An organization shall provide secure and appropriate disposition for records that are no longer required to be maintained by applicable laws and the organization's policies.</p>	<p>There is no documentation of the processes, in any, that are used to guide their transfer or disposition of records. The process for suspending disposition in the event of investigation or litigation is not consistent across the organization.</p>	<p>Preliminary guidelines for disposition are established; realization of importance of suspending disposition in a consistent manner, repeatable by certain legal groupings. There may or may not be enforcement and auditing of disposition.</p>	<p>Official procedures for disposition and transfer are developed. Official policy and procedures for suspending disposition have been developed. However, these policies and procedures are still not standardized across the organization. Individual departments have devised alternative procedures to suit their particular business needs.</p>	<p>Disposition procedures are understood by all and are consistently applied across the enterprise. The process for suspending disposition due to legal holds is defined, understood, and used consistently across the organization. Legal holds are considered to be effective. Electronic information is expunged and not just deleted in accordance with retention policies.</p>	<p>Disposition process covers all records and information in all media. Disposition is assisted by technology and is integrated into all application, data warehouses and repositories. Processes for suspending disposition is regularly evaluated and improved.</p>