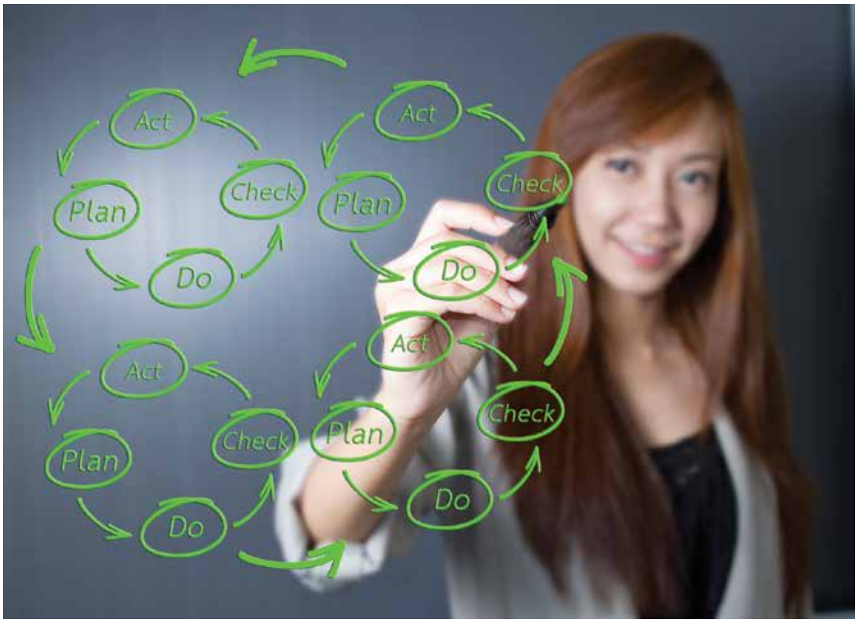
Elements to Be Assessed in a RIM Audit

ARMA International Standards Workgroup



The classic 20th century teachings of W. E. Deming, Ph.D., heralding the "plan-do-check-act" continuous feedback loop remain a bulwark of management science, despite the passing of many decades. Today, through the audit process, records and information management (RIM) professionals can heed Deming's imperative by monitoring the organization's compliance with RIM program policies and procedures. Opportunities for quality and performance improvement are brought to the fore, and the organization's risk exposure level is assessed. The RIM program and the organization can jointly benefit from these activities.

The Focus of the RIM Audit

In accordance with the approved RIM audit plan, data, documents, records, and other items are gathered during the course of the RIM audit. The audit should focus on an assessment of:

- The completeness of RIM policies and procedures with consideration of all records, regardless of format/media, as managed throughout the lifecycle
- The currency of RIM policies and procedures per RIM standards and best practices
- The efficiency/effectiveness of RIM-related software/hardware/systems
- The organization's compliance with RIM policies and procedures and legal obligations
- The organization's RIM-related risk exposure
- Recommendations for areas possibly benefitting from changes/improvements

For the RIM program, these findings and quality-focused suggestions are essential facets of the audit, providing stepping stones to a higher level of functioning. At the audit's conclusion, all results (including findings and suggestions) are included in the written audit report.

Legal Considerations

Legal Requirements

An organization can be subject to many legal mandates relative to its RIM program, including laws, statutes, regulations, and ordinances. As a result, professional legal advice may be warranted prior to undertaking a RIM audit. While the audit cannot always determine whether an organization is compliant with *all* relevant legal requirements, it is an opportunity to make a "good faith effort" to identify such requirements and document the organization's attempts to fulfill its responsibilities. The audit should also assess the adequacy of the organization's mechanisms and protocols to monitor ongoing compliance with related processes, such as legal holds and e-discovery, in its day-to-day operations.

Sources of legal mandates affecting the RIM program may include, but are not limited to:

- International laws or treaties
- Federal law
- State, municipal, and/or local stat utes, regulations, and ordinances
- Standards and best practices and/or guidance advisories developed by certifying or licensing bodies and/or specific industry or sector-related groups

Other organizational departments are commonly affected by legal requirements, necessitating collaboration with RIM professionals to facilitate appropriate recordkeeping. As a result, representatives from diverse departments or units, such as those listed here, often participate in RIM audit activities:

- Accounting and Taxation
- E-commerce
- Finance
- Human Resources/Labor Practices
- Insurance/Risk Management
- IT (information technology security, privacy, and confidentiality)
- Legal and Compliance
- Physical Facilities/Environmental Management

Legal Holds. In the United States, when an organization faces potential litigation, preservation of appropriate paper and electronic records and nonrecords is an obligation per the *Federal Rules of Civil Procedures* (FRCP). Organizations should have legally defensible policies and procedures regarding legal holds and should monitor ongoing compliance. Failure to monitor and comply with a hold order can result in spoliation and/or sanctions ranging from monetary penalties to investigation by various government entities.

Areas examined during the RIM audit and pertaining to legal holds usually include:

- Documentation of the legal hold process in RIM policies and procedures
- Electronic systems used for recordkeeping and legal holds activities, e.g., electronic records management systems, electronic document management systems, or other specialized electronic information management systems utilized in legal settings
- Identification of individual(s) responsible for the legal hold process, i.e., establishment of a "point of contact"
- Method(s) by which the legal hold is initiated and rescinded
- Method(s) by which the legal hold is confirmed by the recipient
- Method(s) by which records and nonrecords, as applicable, are identified for legal hold
- Method(s) by which records and nonrecords, as applicable, are tracked when multiple holds are in place
- Preservation of paper and electronic records and nonrecords, as applicable, during the legal hold period
- International, federal, regional, industry, and/or sector-specific laws, statutes, regulations, and ordinances affecting legal holds

Given their importance, legal holds should be included in the RIM audit. A representative sample of cases involving legal holds may be investigated to ensure they were managed in a compliant manner. Alternatively, if the volume of legal hold cases was small, all cases could be examined as part of the audit. The organization's RIM professional(s) should work closely with the auditor(s) to ensure there is an adequate understanding of the legal hold process.

Given their importance, legal holds should be included in the RIM audit.

Benchmarking against industry best practices for legal holds allows the auditor(s) to pinpoint areas where improvements are recommended. *The Sedona Conference® Commentary on Legal Holds: The Trigger and the Process* and the ARMA International guideline *Records Management Responsibility in Litigation Support* provide further guidance.

E-Discovery. E-discovery is the process by which electronically stored information (ESI) is uncovered and extracted for evidentiary purposes. ESI should be preserved and protected from loss.

Business Continuity, Disaster Management Planning, and Vital Records

The RIM program should incorporate strategies for business continuity/disaster management planning, including vital records management. The RIM audit should investigate these program components, assessing their viability and conformance with recognized and accepted RIM standards and best practices. The auditor(s) should also evaluate the organization's RIM-related system(s) and make recommendations, as needed, pertaining to business continuity/disaster management preparedness.

RIM professionals should update planning documents on an ongoing basis, communicating revisions to the appropriate individuals within the organization and conducting training, as needed.

Vital records are needed for the everyday functioning of the business. These are the records that are essential to the continuity of the organization. The audit can determine whether vital records have been thoroughly identified and if they are being managed appropriately per the program's policies and retention schedule(s). Backups are recommended for all vital records, regardless of record format and storage media. For instance, many organizations now use electronic storage options, such as cloud-based services, to provide redundant, offsite preservation. The audit should examine all vital records backup policies and procedures.

Well-formulated business continuity/disaster management planning allows for any number of contingencies or unforeseen events—both natural or man-made, intentional or unintentional.

Depending upon the business setting, the auditor(s) may need to address organization-specific characteristics when evaluating disaster management/business continuity preparedness including, but not limited to:

- Applicable legal mandates
- Socio-political, economic, and/or cultural considerations affecting the organization's operations on a temporary or long-standing basis

- Special or unique processes, specific to an organization's business or its setting, required for record retrieval or restoration
- The organization's physical location(s) and topography/ geography
- The type of organization, i.e., for-profit, not-for-profit, or government

ARMA International provides an American National Standard on the topic of vital records management: *Vital Records Programs: Identifying, Managing, and Recovering Business-Critical Records* (ANSI/ ARMA 5-2010). The National Fire Protection Association (NFPA) and Underwriters Laboratories, Inc. (UL) have produced standards focusing uniquely on fire protection: *Standard for the Protection of Records* (NFPA 232, 2012 Edition) and *Standard for Tests for Fire Resistance of Vault and File Room Doors* (ANSI/UL 155:2009).

In addition, various disaster preparedness topics are covered in online information available from the Disaster Recovery Institute International (DRII), the Federal Emergency Management Agency (FEMA), the Library of Congress, the National Archives and Records Administration (NARA), and the Northeast Document Conservation Center (NDCC).

The RIM audit should examine the RIM program's security operations.

Secure Records Storage

Records need to be secure (protected) to ensure their authenticity, integrity, and reliability; this is a hallmark of an effective RIM program. All records, regardless of format, should be protected against loss, misuse, and inappropriate/unlawful alteration. In addition, records containing personal or confidential information are subject to special handling and enhanced security measures.

Records security encompasses in-place safeguards designed to thwart physical damage (e.g., fire or other acts of nature) and virtual hazards (e.g., inappropriate access or malicious code infections).

Accordingly, the RIM audit should examine the RIM program's applicable security operations, including procedures, according to industry standards and best practices in the areas of:

- Levels of protection offered to different types of records, e.g., Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations require specific access and storage requirements for health records
- Physical protection of paper records including, but not limited to, procedures/tools/ construction materials applicable to buildings, e.g., records centers; records storage-related equipment, e.g., file cabinets and vaults; and monitoring devices, e.g., temperature/humidity control instruments and surveillance cameras
- Virtual protection of electronic records including, but not limited to, access procedures/tools, cloud storage-related activities, malware prevention/detection processes, and software/systems design and functioning

The RIM audit should examine the organization's ability to secure its records according to RIM program policies and procedures and RIM/non-RIM standards and best practices, as well as applicable legal mandates.

Further standards and best practices guidance on security matters related to RIM practices, including cloud-based storage, internal and external environmental factors for records stored on physical media, and records center operations, may be obtained from ARMA International's *Guideline for Outsourcing Records Storage to the Cloud* and *Records Center Operations* (ARMA TR 01-2011).

Other sources include: the InterNational Committee for Information Technology Standards (INCITS), the American National Standards Institute (ANSI), the International Organization for Standardization (ISO), and the National Institute of Standards and Technology (NIST).

Secure Records Storage During the RIM Audit

An onsite room or office, with a lock for security purposes, should be provided for the auditors' use during the RIM audit. Records used by the auditor(s) may be kept in that space until the audit's close. A checklist or log should be maintained to track the location and utilization of physical records examined as part of the audit. Electronic records stored in various automated systems, databases, or other locations may be involved in audit activities. Computer access to records should be password protected with appropriate safeguards, such as encryption, to ensure records' continuing authenticity, integrity, and reliability. For electronic records, access-related metadata should be logged and retained. Upon completion of the audit, the chain of custody detailing the transfer of physical and electronic records to/from the auditor(s) should be documented in the audit report and retained per the retention schedule.

Electronic Records Management Systems Design

ARMA International's *Glossary of Records and Information Management Terms*, 4th edition (ARMA TR 22-2012) defines an *electronic records management system* (ERMS)—which is sometimes referred to as an electronic recordkeeping system or electronic records management application— as "a system consisting of software, hardware, policies, and processes to automate the preparation, organization, tracking, and distribution of records regardless of media."

The definition also notes that such a system includes retention scheduling and disposition capabilities. The way(s) organizations choose to design and implement these systems are examined in the RIM audit. While other types of information systems proliferate, including those uniquely designed for content and/or document management within the organization, this discussion is limited to systems characterized as ERMS.

As part of the audit … ERMS issues should be considered.

As part of the audit, these ERMS issues should be considered:

System Scope:

- Do policies and procedures delineate what records should—and should not—be stored in the system, as well as who should file them and when they should be filed?
- What steps are taken to ensure that policies and procedures are properly executed?

Records Identification:

- Does the system allow for the designation of a file stored in the system as a record (i.e., one file equals one record)?
- Does the system allow for the designation of a set of files stored in the system as one or more records (i.e., one file contains multiple records, multiple files contain the components of one record, or multiple files contain the components of multiple records)?
- Can the system demonstrate, via report generation, that every file and/or record in the system is associated with one or more record(s) and/or file(s)?

File Plans:

- Are file plans in place?
- Does the system allow every record to be linked to an item in a file plan?
- Can the system demonstrate, via report generation, that every record in the system is linked to an item in a file plan?

Records Disposition:

- Does the system allow every record stored in the system to be linked—either directly or via the file plan—to disposition instructions?
- Can the system demonstrate, via report generation, that every record and/or file stored in the system is linked to disposition instructions?
- Can the system identify, via report generation, all records and/or files subject to a particular set of disposition instructions?
- Can the system ensure that every file associated with more than one set of disposition instructions is retained for the longest retention period in any of those disposition instructions?
- Are policies and procedures in place to ensure that only authorized personnel can execute disposition instructions within the system?
- Is the system monitored to ensure disposition instructions are properly executed for all records in the system?

Legal Holds:

- Does the system allow for the suspension of disposition instructions for records subject to a legal hold?
- Are policies and procedures in place to ensure that no records under a legal hold order are destroyed?

Conversion/Migration Strategy:

- Can the system easily export records and their associated metadata if conversion to another system is necessary?
- Are policies and procedures in place to periodically assess the need to migrate records and associated metadata to a new system?

Within the past two decades, the U.S. Department of Defense (DoD) created DOD 5015.2-STD, *Design Criteria Standard for Electronic Records Management Applications.* This *de facto* standard provides advice for ERMS deployment, and the U.S. National Archives and Records Administration (NARA) supports its use by all federal government agencies. ARMA International's technical report *Using DoD 5015.2-STD Outside the Federal Government Sector* (ARMA TR 04-2009) offers assistance when using this standard in other types of organizations.

Increasingly, organizations are amassing large collections of data and information, whether via social media tools, electronic messaging applications, and/or cloud-based platforms. Sometimes, these content caches exist beyond the boundaries of traditional ERMS. In conducting an audit, it is important to investigate how the RIM program handles these other data and information sources to ensure that all records are properly identified, managed, and stored, regardless of point of origin.

ARMA International's American National Standard *Implications of Web-based Collaborative Technologies in Records Management* (ANSI/ARMA 18-2011) and its related technical report *Using Social Media in Organizations* (ARMA TR 21-2012) are useful reference publications for this purpose.

Learn More

For a comprehensive discussion of auditing a RIM program, see the technical report *Auditing for Records and Information Management Program Compliance* (ARMA International TR 25-2014). It is available for purchase at *www.arma.org/bookstore.* **END**

The ARMA International Standards workgroup leader was Sandra Broady-Rudd, CRM; members were Mark Conrad; Michelle Ganz, CA: Glenn P. Gercken, CRM; Sharon Llewellyn: Daniel McCormack, CA: Tanya Marshall; and Bernard Reilly. See their bios on page 47.