Auditing for Records and Information Management Program Compliance

Auditing for Records and Information Management Program Compliance

ARMA International TR 25-2014

A Technical Report prepared by ARMA International and registered with ANSI
January 26, 2014
**Table of Contents**

Acknowledgments ........................................................................................................ v

Foreword ....................................................................................................................... vi

1 Introduction .............................................................................................................. 1
   1.1 Purpose ............................................................................................................. 1
   1.2 Scope ............................................................................................................... 2

2 Definitions ............................................................................................................... 2

3 The RIM Audit – Elements To Be Assessed .............................................................. 6
   3.1 The Focus of the RIM Audit ........................................................................... 6
   3.2 Legal Considerations ....................................................................................... 6
      3.2.1 Legal Requirements .............................................................................. 6
      3.2.2 Legal Holds ........................................................................................... 7
      3.2.3 E-Discovery .......................................................................................... 7
   3.3 Business Continuity, Disaster Management Planning, and Vital Records .......... 8
   3.4 Secure Records Storage .................................................................................... 9
   3.5 Secure Records Storage during the RIM Audit .................................................. 9
   3.6 Electronic Records Management Systems Design ........................................... 9

4 Structuring a RIM Audit ............................................................................................ 11
   4.1 Incorporating the RIM Audit into the RIM Program ......................................... 11
   4.2 The RIM Audit and the Records Lifecycle ....................................................... 11
   4.3 ARMA International’s Generally Accepted Recordkeeping Principles® ............ 12
   4.4 RIM Audit Policies and Procedures ................................................................. 12
   4.5 Obtaining Management Approval for the RIM Audit ...................................... 13
   4.6 Using an In-House or Outsourced Auditor ..................................................... 13
      4.6.1 Characteristics of an Effective RIM Auditor ........................................... 13
      4.6.2 Determining Whether to Outsource ......................................................... 13
      4.6.3 Working with an In-House Auditor ......................................................... 14
      4.6.4 Choosing an Outsourced Auditor ......................................................... 14
      4.6.5 Working with an Outsourced Auditor ..................................................... 14
   4.7 The RIM Audit Plan ......................................................................................... 15
      4.7.1 Developing the RIM Audit Plan ............................................................... 15
      4.7.2 Training Considerations ......................................................................... 16
      4.7.3 The Communications Plan ....................................................................... 16
      4.7.4 Obtaining Management Approval for the RIM Audit Plan ....................... 16
      4.7.5 Determining Required Resources (Material, Personnel, Fees) ................. 16

5 Other Audit-Related Tasks ...................................................................................... 17
   5.1 Writing the RIM Audit Report ........................................................................ 17
      5.1.1 Audit Report Description ........................................................................ 17
      5.1.2 Audit Report Findings and Recommendations ......................................... 17
      5.1.3 Restricting Distribution of the RIM Audit Report ................................... 18
      5.1.4 Retaining RIM Audit Materials ................................................................. 18

© 2014 ARMA International. Purchaser of this PDF file is entitled to print one copy for reference. Other reproductions or redistribution is prohibited.
5.2 Soliciting Feedback as Part of the RIM Audit ................................................................. 18
5.3 Effecting Change after the RIM Audit ................................................................. 18
5.4 Updating Training Materials and Activities ................................................................. 19

6 Summary .................................................................................................................. 19

Appendix A: ISO Publications (Standards, Technical Reports, Technical Specifications)
Related to Auditing and of Interest to RIM Professionals ........................................... 20
Appendix B: Sample Questions – Soliciting Feedback from Internal Stakeholders as Part of the RIM Audit ................................................................. 21
Appendix C: ARMA International Information Governance Maturity Model ................................................................. 22
Bibliography .................................................................................................................. 23
About ARMA International ............................................................................................ 26
Acknowledgments

ARMA International gratefully acknowledges the generous contributions from the following individuals and groups without whose time, effort, and expertise this publication would not have been possible. Affiliations listed are those on record with ARMA International at the time of printing.

Project Workgroup Leader:
Sandra Broady-Rudd, CRM, Wells Fargo, Madison, WI

Project Workgroup Members:
Mark Conrad, National Archives and Records Administration, Rocket Center, WV
Michelle Ganz, CA, Lincoln Memorial University, Harrogate, TN
Glenn P. Gercken, CRM, Ungaretti & Harris, LLP, Chicago, IL
Sharon Llewellyn, Sterling, VA
Daniel McCormack, CA, Town of Burlington, Burlington, MA
Tanya Marshall, Vermont State Archives & Records Administration, Montpelier, VT
Bernard Reilly, Center for Research Libraries, Chicago, IL
Natasha Zwarich, University of Quebec, Montreal, Quebec, Canada

Special Contributors:
Thank you to members of the ARMA International RIM Review Group who graciously contributed to vetting and reviewing this technical report.

Thanks, also, to the ARMA International Standards Development Program standards consultant, Nancy D. Barnes, Ph.D., CRM, CA, who served as project manager for the development of this publication, and to Vicki Wiler, Director of Publications, ARMA International.
Foreword

Publication of this Technical Report has been approved by ARMA International. This document is registered as a Technical Report according to the latest version of the American National Standards Institute (ANSI) Procedures for the Registration of Technical Reports. This document is not an American National Standard and the material contained herein is not normative in nature. Comments on the content of this document should be sent to:

ARMA International
Attn: Standards
11880 College Boulevard, Suite 450
Overland Park, Kansas 66210
standards@armaintl.org

Users of this document are advised that its content, in whole or in part, does not supersede laws, statutes, regulations, or ordinances applicable to certain business types, sectors, settings, and/or entities.

Rationale

This technical report about auditing organizational records and information management (RIM) programs is informative and educational. It is useful to RIM practitioners and educators, archivists, consultants, information technology professionals, and RIM product and service vendors. This publication may complement the international standard ISO 15489-1, Information and documentation – Records management – Part 1: General.

It is incumbent upon each organization and its RIM professional(s) to determine the RIM and non-RIM standards and best practices advice deemed most pertinent, appropriate, and feasible for that organization. To assist in identifying these, Appendix A contains a roster of selected ISO standards and best practices publications for further consideration. Other sources for RIM-related standards and best practices can be found in the Bibliography.
1 Introduction

1.1 Purpose

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.

As part of the audit process, there are many RIM standards and best practices against which RIM professionals can evaluate their RIM program’s currency and comprehensiveness. Many such standards and best practices are mentioned in this publication, including ARMA International’s Generally Accepted Recordkeeping Principles®, circa 2009 with updates in 2013, which outline structural elements of an effective RIM program. Given their nascent, the Principles have not yet been widely referenced in the RIM literature. However, they were mentioned in recent media releases pertaining to the Pacific Gas & Electric pipeline rupture and fire in San Bruno, California; Duller and North’s 2012 work utilized the Principles in providing a retrospective analysis of Pacific Gas & Electric’s RIM-related activities. The Principles and the ARMA International Information Governance Maturity Model (Maturity Model), which was created to operate in tandem with the Principles, offer
a robust information governance (IG) architecture and are useful assessment tools. (See Section 4.3 and Appendix C.)

This technical report serves an educational purpose. It expands RIM professionals’ knowledge and provides implementation-based advice related to the RIM audit. This publication aims to encourage innovation, spur improvement, strengthen information governance efforts, and bolster compliance for all organizations.

1.2 Scope
Each organization’s RIM program should incorporate audit-related activities to ensure all program components are operationally sound from a RIM perspective and in keeping with appropriate information governance requirements. This publication’s scope embraces a broad-based investigation of the audit function as deployed in the RIM context and with respect to the records lifecycle. The definition of audit used in this publication may be found in Section 2 and is derived from the ARMA International Glossary of Records and Information Management Terms, 4th edition (ARMA TR 22-2012).

While it is recognized that industry and/or sector-specific legal mandates also affect compliance within the RIM sphere, this publication does not address those unique requirements. In addition, this publication does not address audits centered on non-RIM purposes such as tax audits, financial audits, and audits supporting certification, accreditation, or licensure of any organization or entity. Therefore, although this technical report’s content is not prescriptive, its high-level approach is applicable to a wide range of organizations operating in a variety of business settings.

2 Definitions

access
The right, opportunity, or means of finding, viewing, using, or retrieving information.

archives
The noncurrent records created or received and accumulated by a person or organization in the course of the conduct of affairs and preserved because of their continuing or enduring value.

audit
1. A review of information-related activities to ensure that sufficient policies, procedures, and controls are in place and compiled to meet all operational, legal, and regulatory obligations and to identify where and how improvements should be made.
2. Any action to confirm that an item has not been altered or changed from the original item.

audit trail
A record that allows for a sequence of activities to be reconstructed, reviewed, and examined. Also referred to as audit log or tracking.

authenticity
The sum of the qualities of a record that establishes the origin, reliability, trustworthiness, and correctness of its content.

backup
A copy of information or data to be used for recovery and created as a precaution in the event that the original is intentionally or inadvertently lost or destroyed.

benchmarking
The act of measuring against specified standards or references.

best practices
The procedures and guidelines that are widely accepted because experience and research have demonstrated that they are optimal and efficient means to produce a desired result.