The relationship between an organization’s information-handling practices and the impact those practices have on its ability to respond to electronic discovery is recognized in the Electronic Discovery Reference Model (EDRM). But the EDRM falls short of describing standards or best practices that can be applied to the complex issues surrounding the creation, management, and governance of electronic information. ARMA International’s Generally Accepted Recordkeeping Principles® and its information Governance Maturity Model are designed specifically to provide a scalable, broadly applicable framework to address these issues.

Note: Subsequent to this paper’s first publication, the EDRM developed the Information Governance Reference Model (IGRM), which depicts a framework for unified information governance and complements the metrics defined by ARMA International’s Information Governance Maturity Model. Learn more at www.edrm.net/projects/igrm.
The Information Governance Maturity Model (the Model) offers an approach to records management that may be of assistance to any organization, private or public, in protecting itself in the use of information assets, complying with applicable legislative and regulatory mandates, and designing and implementing effective records management programs. It focuses on the internal needs of organizations, including their obligation to respond to government investigations and to engage (or be engaged) in litigation. This white paper looks to the Model in the context of both investigations and litigation.

An Overview of Government Investigations

For many organizations, government investigations are a fact of life. The statutory and regulatory net is wide and, depending on the nature of an organization, there may be multiple investigations at one time. The reader should think of a spectrum in the context of investigations. Organizations in heavily regulated industries (such as energy and pharmaceutical) are routinely subject to government oversight and inquiry. At the other end of the spectrum may be organizations that do not routinely draw the attention of elected officials, regulators, or law enforcement. Even at this end, however, inquiries into workplace safety or employment practices should not be unexpected.

What investigations have in common are their potential broad sweep and the lack of judicial intervention to limit any such sweep. For example, in FTC v. Church & Dwight Co., 2010 WL 4283998 (D.D.C. Oct. 29, 2010), the court enforced a subpoena and civil investigative demand that called for the production of documents and electronically stored information (ESI) from a Canadian subsidiary of Church & Dwight Co. related to an antitrust investigation of a domestic market. In doing so, the court recognized the broad scope of authority conferred on the Federal Trade Commission and found that the information sought was of “reasonable relevance” to the investigation. Nothing more was needed.

For another example of the broad deference given to government agencies, look to In re Subpoenas, 2010 WL 841258 (W.D. Va. Mar. 10, 2010), in which the court found investigative subpoenas into possible federal violations arising out of the marketing of a drug and related health fraud to be “reasonable” under the Fourth Amendment as the information sought was relevant to the investigation.

Government investigations can require the production of large volumes of information – in the form of paper or ESI – and courts are unlikely to intervene in favor of an organization under investigation. The Model provides a process that may help an organization organize its information assets and respond to investigatory demands.

An Overview of Litigation

An organization must foresee participation in litigation, be it as a plaintiff, a defendant, or a nonparty subject to a subpoena. Litigation, so defined, may be rare or frequent. Nevertheless, we live in a litigious society. The Model, once again, provides a means by which an organization can respond to the imperatives of litigation, be it pending or reasonably anticipated.

To understand those imperatives, think of a spectrum, illustrated for the purposes of this white paper by the Electronic Discovery Reference Model (EDRM) shown below.

The EDRM recognizes the spectrum of information management in the context of litigation. Before litigation, an organization maintains information to comply with laws or regulations and to meet its business needs.
We can define these as “records.” This is where records management begins in the classic sense. An organization can – and should – create, implement, and evaluate records retention policies pursuant to which records are kept and, when appropriate, destroyed.

When litigation begins or is reasonably foreseeable, a duty arises to preserve “relevant information,” which goes beyond what the organization treats as “records” to encompass all media on which relevant information may be recorded, from the most formal report to the board of directors to the most informal and transitory text message. If the information is relevant to the subject matter of the dispute, broadly defined, it becomes subject to a litigation hold. This hold is imposed by law and requires an organization to preserve information that it might otherwise routinely destroy.

Again, what is “relevant” is generally broadly defined, at least before adversary parties agree on narrowing the scope of what must be preserved or a party seeks judicial intervention to narrow scope. As we will see, failure to comply with a litigation hold can, under certain circumstances, have severe consequences. Simply put, the loss of information subject to a hold is called spoliation.

After information is preserved, it must be reviewed, the information may be subject to disclosure and discovery by other parties, and, at some point, the information may need to be admitted into evidence. The ERDM recognizes the spectrum, as does the “Flow of Litigation” chart on page 4.

Note, again, the theme of a spectrum: The litigation hold may be “triggered” at different times for different parties, but the hold runs throughout the course of a given litigation and across various events that may occur before litigation is commenced and even after litigation is concluded.

Any response to actual or threatened litigation begins with a records retention policy, assuming it exists. Once there is a trigger, an organization imposes a preliminary hold, begins to preserve, and identifies sources (or repositories) of information that must be preserved. Note that there are two constants that run through litigation:

1. Preservation of information subject to the hold
2. An ongoing review and refinement of the hold, as well as the periodic reissuance of litigation hold notices

Preservation, of course, is not to be seen in isolation. Once information is preserved, the information must be reviewed to determine if it is in fact relevant and, if so, whether the information may be withheld from disclosure to other parties by reason of, for example, confidentiality or privilege.

After this review, and perhaps subject to a protective order under Rule 26(c) of the Federal Rules of Civil Procedure (FRCP) or a nonwaiver agreement or order under Rule 502(d) or (e) of the Federal Rules of Evidence, the information should be disclosed in discovery and, perhaps, introduced into evidence.

The "Flow of Litigation" chart offers a concise overview of the various stages of a civil action in U.S. courts. Remember, this is just an overview and that events – and costs – may vary on an action-by-action basis.

Note also that there should come a point when the duty to preserve ceases and an organization’s records retention policies again control the destruction of information.

What can go wrong when an organization finds itself in litigation? One leading judicial decision that offers a variety of errors that can occur at the earliest stage, that of the establishment and implementation of a legal hold, is Pension Committee of the University of Montreal Pension Plan v. Banc of America v Securities LLC, 685 F. Supp. 2d 456 (S.D.N.Y. 2010). This lengthy decision, authored by United States District Judge Shira A. Scheindlin, gives numerous examples of actions by a number of plaintiffs that led to the loss of relevant information, including:

• The failure to issue a written litigation hold
• The failure to stop the routine deletion of information after a hold was issued
• The failure to secure information from “key players” (employees having information subject to the duty to preserve)
• The failure of management to supervise when delegating search efforts to others.

When litigation begins or is reasonably foreseeable, a duty arises to preserve “relevant information,” which goes beyond what the organization treats as “records” to encompass all media on which relevant information may be recorded...

Scheindlin analyzed each failure within a framework of whether the failure was the result of gross negligence, negligence, or willful misconduct and imposed appropriate sanctions, including spoliation sanctions, which alter the ordinary burden of proof in litigation and allow juries to presume missing facts or make adverse inferences.

Decisions that cite to and follow Pension Committee include Crown Castle USA Inc. v. Fred A. Nunn Corp., 2010 WL 4027780 (W.D.N.Y. Oct. 14, 2010), in which a duty to preserve had been triggered when employees discussed possible insurance claims and an in-house attorney labeled communications as being subject to attorney-client privilege or work product protection.

For a decision that questions the need for a written hold notice in every instance (suggested by Pension Committee to be a grossly negligent act), see Orbit One Communications, Inc. v. Numelex Corp., 2010 WL 4615547 (S.D.N.Y. Oct. 26, 2010). The point here is that reading Pension Committee and other judicial decisions can lead to the development of best practices that benefit, rather than harm, organizations.


The reader should also think of sanctions for spoliation in the context of a trilogy...
of the scienter (or state of mind) of the spoliator, relevance of the information destroyed or lost, and prejudice to the party that was deprived of the information.

Mere negligence, without a demonstration that the missing information was relevant or harmed the ability of the requesting party to conduct the litigation, will seldom result in more than a slap on the wrist.

The more egregious the conduct, however, the more likely the court will allow a jury to presume that the missing evidence was relevant and that its loss prejudiced the requesting party.

But in most circumstances, all three elements – a culpable state of mind, relevance of the missing information, and prejudice to the requesting party – must be proven for a severe sanction, such as default judgment or dismissal of the action, to be imposed.

The duty to preserve can also have a wide sweep. For example, a party may be deemed to have “possession, custody, or control” under Rule 34(a) of the FRCP over information held by another entity by reason of contract. Thus, the party may be required to take steps to preserve and produce that information.1 See, for example, Goodman v. Praxair Servs., 632 F. Supp. 2d 494 (D. Md. 2009) and Innis Arden Golf Club v. Pitney Bowes, Inc., 629 F. Supp. 2d 175 (D. Colo. 2009), two judicial decisions that reached different conclusions over a party’s “control” of a consultant under the facts presented.

As Pension Committee and numerous other decisions illustrate, preservation has its pitfalls. This white paper now returns to the Model and suggests how those pitfalls may be avoided or, at the least, minimized in an organization’s management of whatever “records” may be defined to be.

Applying the Model to Litigation and Investigations

The Model speaks of Generally Accepted Recordkeeping Principles® and, in each, establishes levels that an organization may aspire to and reach.2 (See page 7 for a full

---

1 Organizations that use web-based services to create or store information (e-mail, for example) must consider the legal risks this presents in terms of their ability to locate, segregate, maintain integrity of, and access that information. For guidance, see Guideline for Outsourcing Records Storage to the Cloud. Overland Park, Kansas: ARMA International, 2010.
description of the principles.) The principles are:
- Accountability
- Transparency
- Integrity
- Protection
- Compliance
- Availability
- Retention
- Disposition

Within each principle are the levels. These are:
- Level 1 (Sub-Standard)
- Level 2 (In Development)
- Level 3 (Essential)
- Level 4 (Proactive)
- Level 5 (Transformational)

This white paper will use, as an example, the first principle and “fit” the possible levels of that principle into the investigations and litigation frameworks described above.

The Principle of Compliance

The Principle of Compliance states that, “[t]he recordkeeping program shall be constructed to comply with applicable laws and other binding authorities, as well as the organization’s policies.”

Level 1 – Sub-Standard

Level 1 is where, among other things, there is “no clear definition of the records the organization is obligated to keep” and “no central oversight and no consistently defensible position.” Plainly, this level is a recipe for disaster for any organization that must respond to an investigation or litigation.

The organization at level 1 does not know what its records are, must respond to inquiries and demands on an ad hoc basis, and cannot demonstrate any rational means to respond. Under the teaching of Pension Committee, this organization would likely be found to be grossly negligent should it fail to preserve (or produce) information.

Level 2 – In Development

At level 2, the organization has “identified the rules and regulations that govern its business and introduced some compliance policies … but “[p]olicies are not complete and there is no apparent or well-defined accountability for compliance.” Moreover, although the organization has some “hold process,” that process is “not well-integrated with the organization’s information management and discovery processes.”

As with level 1, level 2 is not a place for an organization to be when faced with an investigation or litigation. The organization has tried, but it is not yet in compliance with legal or business requirements. Likewise, although the organization recognizes the duty to preserve, the organization’s preservation process is not thorough. Although every organization must be at level 2 at some point in its corporate existence, the organization appears ripe for a finding of, at the least, negligence, should it lose information.

Level 3 – Essential

Level 3 finds the organization on safer grounds. Here, again among other things, the organization has “identified all relevant compliance laws and regulations.” The organization has “systematically carried out” its creation and “capture” of records. The organization has a “strong code of business conduct” and has integrated its litigation hold process into “information management and discovery processes for the ‘most critical’ systems.”

At level 3, an organization is likely to meet its preservation obligations and, just as importantly, be able to demonstrate to a regulator or court what it did to preserve, what it did or did not preserve before a hold went into effect, and what it can or cannot produce.

Perhaps more importantly from a risk management viewpoint, an organization that has attained level 3 has a strong argument that it is entitled to the protection of FRCP 37(e) (and its equivalent in many states), which would shield it from a sanction imposed under the rules for the unintentional loss of relevant ESI due to the routine operation of its electronic information system, such as the loss of data attributable to an auto-delete function or the recycling of backup media.

Level 4 – Proactive

Level 4 should bring an organization even more comfort. Among other things,

... why an organization might elect to reach level 5:
“The organization suffers few or no adverse consequences based on information governance and compliance failures.”

systems have been implemented to “capture and protect records.” Metadata is available to “demonstrate and measure compliance.” There are regular audits and training of employees. Lack of compliance is “remedied through implementation of defined corrective actions.”

All these features are available to an organization when it must demonstrate to a court and regulator what it can and cannot do, and militate in favor of the court or regulator finding that the organization acted in good faith and complied with its obligations in a reasonable and demonstrable manner.

Level 5 – Transformational

At level 5, “[t]he importance of compliance and the role of records and information…are clearly recognized at the senior management and board levels.” Moreover, among other things, “[t]he roles and processes for information management and discovery are integrated.” This feature plainly describes why an organization might elect to reach level 5: “The organization suffers few or no adverse consequences based on information governance and compliance failures.”

The reader should look at each of the other principles and fit each level into the frameworks of government investigations and litigation, as did this white paper with the Principle of Compliance.

The Principle of Disposition

This white paper has applied the Model to litigation and investigations and, for illustrative purposes, focused on the Principle of Compliance. The white paper is not intended to minimize the importance of any
other principle to a successful records management program. However, and
again for illustrative purposes only, there should be some reference to the Principle
of Disposition.

This principle states: “An organization
shall provide secure and appropriate dis-
position for records that are no longer re-
quired to be maintained by applicable laws
and the organization’s policies.”

At level 4, “[d]isposition procedures are
understood by all and are consistently
applied,” and, vital for the purposes of this
white paper, “[t]he process for suspending
disposition due to legal holds is defined,
understood, and used consistently across
the organization.”

The maturity reflected in level 4
should be of great benefit to any organi-
zation that finds itself entangled in a gov-
ernment investigation or litigation, either
as a party or a third-person respondent
for records that are no longer re-
quired to be maintained by applicable laws
and the organization’s policies.”

Second, the failure to dispose of
records simply increases the volume of in-
formation that an organization possesses,
along with the possible need to identify
and process information (with backup
media being the perfect example) for fu-
ture investigations or litigation. There ap-
pears to be no good reason to keep
information that an organization does not
need to keep.

Conclusion

When the reader looks at each principle
and level under the Model, its application to
litigation and investigations should spring to
mind. Sub-standard levels of performance in-
voke the specter of findings of gross negli-
genre or negligence in litigation. Likewise,
failures to adequately respond to government
investigations can have nothing other than
bad consequences.

Accordingly, this white paper suggests that
as organizations engage in cost-benefit analy-
ses to decide which level is appropriate under
each principle, only levels 3 and 4 are sufficient
to manage both compliance and business
needs. Level 5, the transformational level, is, of
course, an ideal to aspire to. Nevertheless, this
white paper acknowledges the costs inherent
in reaching level 5 and acknowledges how dif-
ficult it is to reach that ideal.

Indeed, as the reader looks at the Model
and considers Pension Committee and other
decisions, several conclusions can be drawn:
• As these decisions make clear, however a
particular organization chooses which
level and principle to meet, the cost-ben-
efit analysis must consider, among other
things, the degree to which the organiza-
tion expects to become involved in litiga-
tion or investigations and the expense of
establishing or implementing a legal hold
program.

• Any cost-benefit analysis must involve
counsel, whether in-house or retained, to
inform management of the contours of
litigation and investigations and what or-
ganizations can expect.

• Levels 1 and 2 are not where organiza-
tions want to be. Levels 3 and 4 are adequate
for the tasks of preservation and production.
Plainly, level 5 is where every organization
would like to be, depending on the resources
and leadership available.

About the Author

Ronald J. Hedges served as a United States
Magistrate Judge in the District of New Jersey
from 1986 to 2007. He is a member of the
advisory board of The Sedona Conference® and
several of its working groups, including those
addressing e-discovery and records manage-
ment. Hedges is also a member of the advisory
boards of the Corporate Counsel and Advanced
E-Discovery Institutes of Georgetown Univer-
sity Law Center, where he serves on the adjunct
faculty and teaches e-discovery and evidence.
Since 2010, he also has been a visiting research
collaborator at the Center for Information
Technology Policy at Princeton University. He is
the author of numerous publications, including
Discovery of Electronically Stored Informa-
tion: Surveying the Legal Landscape. Hedges
consults on varied topics, including e-discovery
and records management. He may be contacted
at r_hedges@live.com.

Acknowledgements

The author and ARMA International also
wish to acknowledge Kenneth J. Withers, Di-
rector, Judicial Education and Content, The
Sedona Conference®, www.thesedonacon-
ference.org, for his valuable contributions
to this paper.

3 For a discussion of how an organization might implement disposition, see Contracted Destruction for Records and Information
Records and recordkeeping are inextricably linked with any organized activity. As a key resource in the operation of any organization, records must be created, organized, secured, maintained, and used in a way that effectively supports the activity of that organization, including:

• Facilitating and sustaining day-to-day operations
• Supporting predictive activities such as budgeting and planning
• Assisting in answering questions about past decisions and activities
• Demonstrating and documenting compliance with applicable laws, regulations, and standards

These needs can be fulfilled only if recordkeeping is an objective activity, insulated from individual and organizational influence or bias, and measured against universally applicable principles. To achieve this transparency, organizations must adhere to objective records and information management standards and principles, regardless of the type of organization, type of activity, or the type, format, or media of the records themselves. Without adherence to these standards and principles, organizations will have poorly run operations, legal compliance failures, and – potentially – a mask for improper or illegal activities.

**Principle of Accountability**
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 auditability.

**Principle of Integrity**
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.

**Principle of Protection**
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.

**Principle of Compliance**
A recordkeeping program shall be constructed to comply with applicable laws and other binding authorities, as well as the organization’s policies.

**Principle of Availability**
An organization shall maintain records 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 legal, regulatory, fiscal, operational, and historical requirements.

**Principle of Disposition**
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.

**Principle of Transparency**
The processes and activities of an organization’s recordkeeping program shall be documented in an understandable manner and be available to all personnel and appropriate interested parties.