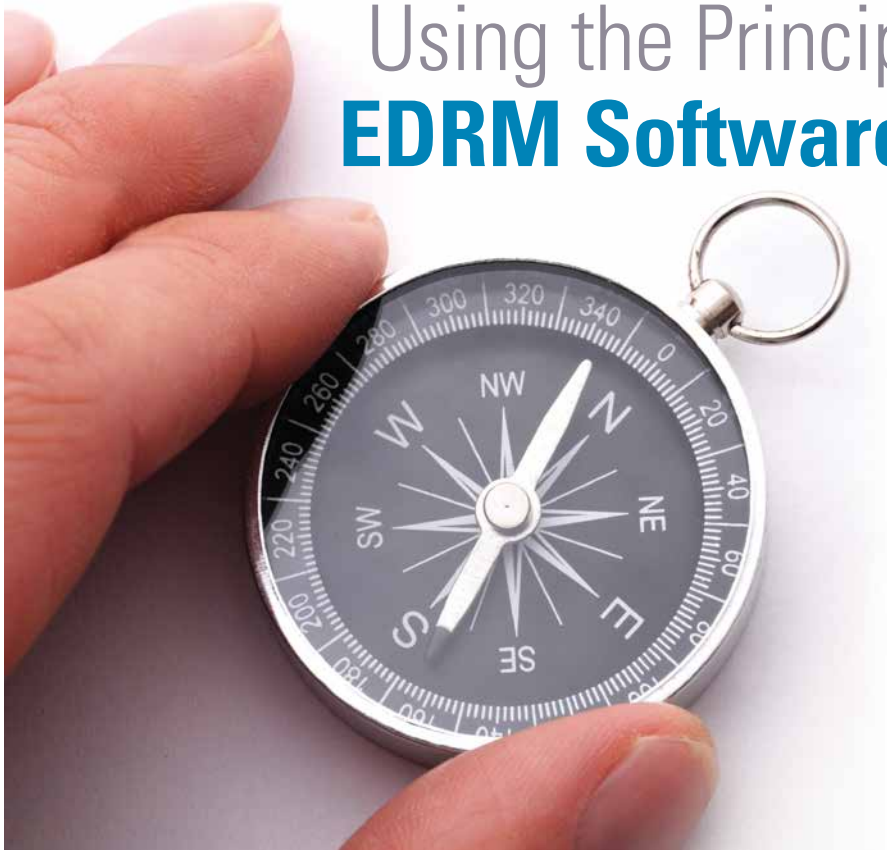
The Generally Accepted Recordkeeping Principles® provide the framework an organization can use to determine the functionality an electronic document and records management (EDRM) system must have to ensure information integrity, availability, protection, retention, and disposition. Successfully implementing an EDRM, though, is dependent on the organization's ability to provide the specific information needed for the EDRM to automate information governance policies, procedures, and processes – such as the appropriate classification scheme and properties for various types of metadata.



Using the Principles to Guide **EDRM Software Decisions**

Julie Gable, CRM, CDIA, FAI

At some point in their careers, most information governance (IG) professionals will confront the need to acquire software as a way to control their organizations' electronic records. Whether the situation calls for buying a new system or replacing an older one, nothing tests the IG program more than software acquisition and implementation.

A Decision Framework

The Generally Accepted Recordkeeping Principles® (Principles) are a framework for the kind of functionality that software should provide. Those who have never worked with software that's designed to manage electronic assets may not realize the interplay between the level of functionality desired from a product and the degree of IG program maturity required to implement it.

Generally speaking, sophisticated software capabilities require higher levels of IG maturity in certain areas, and the Information Governance Maturity Model (Maturity Model) can help in assessing readiness. Even in an organization with a level 3 (Essential) maturity, additional work may be necessary to accomplish the degree of IG automation sought.

Embarking on the software journey requires thoughtful research in several areas:

- What IG objectives will the software help meet? Or, alternatively, what IG gaps will the software help close?
- What functionality does the software offer?
- What functionality is expected?
- Is the current IG program mature enough to provide the elements for implementation success?

IG Objectives

Although improved compliance, transparency, and accountability are often the byproducts of successful document management projects, they are not in themselves the main reasons to invest in technology.

External drivers are usually regulation, vulnerability to litigation, and the need to show the outside world there is an expectation of adherence to internal policies. This is often the case following a compliance or litigation failure.

A regulatory audit that resembles a scavenger hunt, with multiple versions of requested documents clouding the proceedings, usually results in unsatisfactory findings. Inadequate response to a legal discovery request, complete with headlines and sanctions, isn't anyone's idea of good information management practices.

Beyond these extremes, both internal and external forces define the reasons for acquiring software. The major internal driver is better productivity through enhanced information utility, as assets become easier to create, revise, find, and manage.

Controlled document repositories are appealing in industries such as pharmaceuticals where documentation is central to research, product development, and regulatory approval. Industries that rely on infrastructure history, such as gas, oil, and water utilities, also invest in software as a way to ensure controlled access to past work and future projects.

EDRM Functionality

Electronic document and records management (EDRM) software generally has capabilities for document creation, collaboration, workflow, version control, and redaction of information. Expect EDRM software to have enhanced search capabilities, as well as the ability to control what documents users may see and what functionality they can use.

All EDRM software has at least basic *records management functionality*, usually defined as the ability to identify records, attach a retention rule, and enforce disposition as necessary, with the option to place a hold on records needed for audit or legal matters.

Some EDRM software now marches under the banner of IG. Be aware that true IG software is an emerging field and capabilities are not yet well-defined or standardized. The IG label is loosely used to mean anything from automatic classification of existing content, to dashboard displays of where risky records reside, to something as sophisticated as a top-level architecture tier that actually superimposes governance rules on an entire enterprise's technical infrastructure.

It helps to remember that EDRM products were originally designed to help organizations know what documents they had – once called "knowledge management" – and to make them available to operations that needed them. Most EDRMs were developed long before the Principles appeared, yet the Principles can help in determining what functionality is essential, what is desirable, and what is optional. The following few paragraphs focus on specific Principles to illustrate these points.

Integrity

At its foundation, *integrity* means that records are not alterable and that events related to them are captured in an audit trail. Be aware that some products keep the audit trail log for a relatively short time and automatically overwrite prior data.

But integrity also applies to system reliability and the monitoring of components such as hardware, network infrastructure, software, and storage media. It helps to understand what facility the product has for self-monitoring.

Integrity requires particular attention when documents will be migrated from older systems into newer ones, and importing may have implications for original document

dates and electronic signatures. In highly regulated industries, the entire system may have to be validated to demonstrate that it produces the same results time after time.

Availability

Availability routinely includes full text as well as keyword search, and, in the most sophisticated systems, content analytics to assign a risk factor to unstructured data of many types. Availability can also mean the opportunity to identify documents of long-term value and ensure that these migrate forward as technology changes, perhaps to an electronic archive, so they are readable and usable well into the future.

Another desirable function may be the software's ability to identify the final or "official" version of documents. The benefit of this in some environments is that prior versions can be eliminated, an effort that can save time and money in daily backups and decrease confusion in regular audits.

Protection

At its most basic, protection is the ability to assign levels of confidentiality or privacy to documents, then to construct profiles for users that govern what documents they may see. Protection also usually encompasses functionality privileges as part of the user profile, with those users at a higher level able to perform functions restricted at lower levels. For example, a contractor may input metadata or create documents but may not be allowed to make changes to documents or to print or send them.

Beyond this, consider the product's redaction capabilities – the ability to obscure specific form sections or document passages. Also important to protection is the ability to restrict functionality for sharing items via e-mail or copying items to removable media. These restrictions can prevent the theft of intellectual property.

Retention

When it comes to retention, basic functionality is the ability to attach a retention rule to a record, calculate the retention period, and report on when records are due for disposition. Retention is often linked with classification, where all records associated with a particular category automatically receive the same retention rule.

Retention capabilities may or may not include the ability to maintain the retention schedule within the software or the ability to keep track of the legal, regulatory, fiscal, operational, and historic reasons for each retention period. It is also good to understand how changes to retention periods can be made and whether they can be retroactively effective, or start on a designated date, or a combination of both.

Disposition

Disposition usually includes the ability to identify records that have reached full retention. In the electronic world, this should include all versions and renditions. Although disposition is one of the central tenets of IG, it is a tough idea for some stakeholders to embrace. The keys are to ensure that the software has very strong hold capabilities and that adequate controls and approvals are in place before anything goes away permanently.

An important thing to look for is how the software product places a legal hold. Must this be done one record at a time? Can an entire class of records be put on hold easily? Once applied, is there an effective way to communicate holds – for example, through posting to an internal website? The software should maintain records of what has been destroyed and, of course, be able to destroy completely and irreversibly.

Software for managing electronic documents is notoriously flexible, and

IG Program Maturity

Software for managing electronic documents is notoriously flexible, and it works because it's able to incorporate the buyer's governance model. This presumes that the buyer has such a model and the model exists at a level of detail sufficient to attain the level of functionality expected. Generally, the more automation desired, the greater the level of detail required in the IG model.

For example, the level 3 maturity for the Principle of Availability notes that "Most of the time, it is easy to determine where to find the authentic and final version of any information." Translating this requirement to EDRM functionality may imply the ability to eliminate drafts once a final version of a document is produced. To actually accomplish this, the software will require defined rules and specific metadata. For example:

- Some mechanism or designation that identifies a "final" document. This could be an electronic signature or a metadata entry that denotes a finished item.
- A way to identify all the drafts associated with the final version
- A rule that specifies when all drafts associated with the final document are to be destroyed and what level of approval is needed (if any)
- A decision on whether the utility program that actually destroys the drafts starts automatically or requires manual intervention
- An audit trail entry that verifies all drafts of a

final document were successfully identified and destroyed

Such specific rules and decisions are beyond the Maturity Model's broad guidance on what should be in place for a successful IG program. While the Maturity Model tells *what* is required for good governance at the policy, procedure, organization, and training levels, the EDRM will require specifics about *how* these should be implemented at the detailed system level. This is particularly evident in the areas of metadata and classification schemes.

Essential Metadata Types

There are several types of metadata that are essential to EDRM functionality.

Descriptive metadata, such as document type, document name, creation date, and author, are required to facilitate keyword search and results filtering for retrievals.

Retention metadata, including record series code, retention rule, and a system-generated disposition or review date, are minimal requirements to enable records management functionality.

Security metadata identify each document's privacy level. It must work in conjunction with user security profiles that are set up in the EDRM system to control the level of viewing and sharing permitted to different levels of users. EDRM functionality privileges are also assigned within the user profile and contribute to integrity by controlling which users may make changes to documents, in particular, to documents that have been declared records.

Process metadata may include status fields showing where a particular document is with regard to a predetermined workflow.

Automating the capture of metadata often relies on a classification scheme, which is usually represented in the EDRM system as a folder hierarchy. Various metadata properties and rules are set up in advance at the folder level. When a document is associated with a given folder in the hierarchy, the document can inherit certain metadata.

This works well when the classification scheme is actually a file plan that consists of broad categories as is common in records retention schedules, where one category encompasses a number of related records, all with the same retention period. Documents classified this way become records and inherit retention rules automatically.

Classification schemes can take many forms, however, and may be designed to serve purposes beyond records management. Classification may be by topic, for example, according to the table of contents for a regulatory submission, with folders and subfolders for each section that needs to be included.

EDRM products designed around document creation and collaboration may allow users to set up their own classification schemes, a situation that diminishes the ability to apply controls such as protection, retention, or disposition in a consistent, standardized way. In these situations, manual metadata entry may be necessary.

A Business Opportunity

The amount of work required to successfully implement an EDRM can come as a shock even to those with a mature IG program in place. Good IG takes a village, and many decisions about EDRM specifics will require the consent of multiple, disparate stakeholders.

Luckily, the Principles make sense from every viewpoint and are hard to argue with, but the more difficult endeavor is to translate them into the detailed specifics the EDRM needs to automate the organization's IG policies, procedures, and processes.

it works because it's able to incorporate the buyer's governance model.

The upside is that the process of planning, acquiring, and implementing software can move the organization from the Maturity Model's "Essential" level 3 to a "Proactive" level 4, particularly in the Principles of Compliance, Availability, Integrity, and Protection.

New software implementation is an excellent time to match IG goals with business goals. Replacing an older system is an opportunity to close gaps between policy and practice. It can also allow for judicious pruning of material that lacks continuing value.

Note that while new rules, metadata, classification, and other changes can be applied to new items entering a new repository on the first day of production, they are not especially easy – or even possible – to retrofit onto older documents imported from older systems. Exceptions and workarounds may be needed to migrate older documents into newer systems.

In the world of EDRM software implementation, one size does not fit all; tailoring will be necessary to make the system work. The Principles provide the basics needed to define broad functionality requirements, and the IGMM will help to assess whether essential structures are in place.

Meanwhile, defining specifics about how to automate your organization's policies, procedures, and processes will require teamwork and attention to detail. Automating IG for electronic records is where the rubber meets the proverbial road, but with careful planning and with tools like the Principles and the Maturity Model, there needn't be skid marks along the way. **END**

Julie Gable, CRM, CDIA, FAI, can be contacted at juliegable@verizon.net. *See her bio on page 47.*