©2015 ARMA International

Designing a Records Audit: A Controls-Based Approach

Andrew Altepeter

Using a controls-based approach to auditing for IG program compliance can help ensure a focused scope, collaborative effort among appropriate stakeholders, quantifiable findings, and trackable remediation progress.

©2015 ARMA International

Giving a deposition about an organization's information governance (IG) program in connection with litigation or a regulatory investigation can be a daunting experience. Opposing counsel may ask for evidence, such as policies and procedures documentation, retention schedules, and employee training, to show that the organization has an effective IG program.

More challenging, though, is if counsel also asks for proof that all members of the organization are being trained and that they are following the policies and procedures. Producing policies, procedures, and retention schedules is a great start, but their mere existence does not prove that they are being followed; the organization must have a way to show it is doing what it says it is doing.

Auditing as Evidence

Many organizations choose to audit their internal processes as a way to show that they are living up to the mandates set in their policies. But auditing IG – something that touches every member of the organization – can be challenging, and not all audits will satisfy a court.

For example, some organizations may "audit" by asking all employees to click an electronic check box or sign a statement to attest that they are in compliance with the organization's IG policies and procedures. This process is easy to set up and easy to get a majority of employees to respond to since it takes only a few seconds to check a box or sign a form.

This approach is useful for periodically reminding everyone in the organization about their need to comply with the policies and procedures. But, this is not an audit. And in all likelihood it will not satisfy opposing counsel or a judge.

The key to an effective audit is having the right controls, scope, and stakeholders. This article provides guidance for assembling these elements and building an audit that will enable an organization to show its IG program is legally defensible.

Narrative Policy

The company shall maintain records in accordance with all retention schedules, which are to list the retention periods for all major record categories of records across the organization. Employees are responsible for maintaining their own records in accordance with these retention schedules. When the records reach the end of their required retention period, and if they are not subject to legal hold, they must be disposed of in a secure manner.

The corporate records manager is responsible for the maintenance of the retention schedule and in assisting employees in its use. When changes to the retention schedule are required, the corporate records manager must undergo a formal change management process.
The corporate records manager is responsible for developing employee training and ensuring training is taken by all employees in the organization.

Control Standards

RM1001 – The corporate records manager is responsible for the maintenance of the RIM policy, training, and retention schedule.

RM1002 – All electronic and hardcopy records must be retained in accordance with the records retention schedule.

RM1003 – The records retention schedule must be updated to reflect current legal and regulatory requirements.

RM2001 – Training must be completed by all employees when hired and every three years thereafter.

RM3001 – A legal hold mechanism must be in place to notify users that their records are subject to legal hold.

RM3002 – All records subject to legal holds must be retained until the hold is lifted.

Figure 1: Narrative vs. Controls-Based Policy

Going Beyond the Maturity Model

ARMA International's Generally Accepted Recordkeeping Principles® (Principles) includes the Principle of Accountability, which stipulates that practitioners must ensure program auditability; specifically, it dictates "Review/auditing of information governance policies and processes to monitor success and failure and to improve and update them proactively."

There are multiple ways to accomplish this. For example, ARMA created the Information Governance Maturity Model (Maturity Model), among other instruments, for organizations to use to benchmark their growth in accordance with the Principles. This is well and good; the Maturity Model is a useful tool for measuring an organization's IG profile at a high level. But, that is different from conducting a true audit.

Audits require a scientific inventory of current practices across the organization, its repositories, and its office locations. It may involve interviews, questionnaires, observation, or the collection of other evidence. This is often where practitioners become overwhelmed trying to determine where to start, what questions to ask, and what aspects to audit.

Using Control Standards

The key to a successful audit begins with a policy against which com-

©2015 ARMA International

pliance can be measured. One way to make a policy auditable is to write it in the form of *control standards,* which, simply put, are binary, concise, numbered, unambiguous, easily referenced ways of stating and measuring compliance with policy. Controls are often used in the areas of IT, information security, or finance. One well-known example of this is the Sarbanes-Oxley Act, which requires certain internal controls for publicly traded companies.

Control standards should avoid ambiguity. Avoiding such qualifiers as "effectively," "timely," and "properly" will clarify the requirements and expectations, which will make the auditing process more straightforward. Often, policies are written in a narrative form instead, as shown in the left-hand box in Figure 1; it uses sentences and paragraphs to explain the roles and responsibilities of the organization's members. There is nothing inherently wrong with this approach, except it lacks the advantage of being auditable. Compare it to the right-hand box in Figure 1, which would be easier to audit.

Whether the organization is replacing a narrative-form policy with control standards or supplementing it with controls, the important thing is to have controls that can be referenced in an audit. There are several advantages to the controls-based approach, as discussed below.

Allows Prioritization, Focus

Policy requirements are not necessarily equally important. Numbered controls allow an organization to choose which ones are the most important or have the highest risks and prioritize them to be addressed first in an audit.

Numbered controls also can be gathered into intelligible groups, such as those dealing specifically with offsite storage of physical records, or electronic records, or legal holds, and so on. Some controls may fall into multiple groups. These control groupings allow an organization to focus an audit on a specific topic and keep the scope appropriately defined.

Compliance Matrix

	The Principles	ISO 15489	HIPAA	PCIDSS	Sarbanes-Oxley	COBIT
RM1001	X	X				
RM1002	X	X			X	
RM1003	X		X		X	
RM2001	X	X				X
RM3001	X	X		X		
RM3002	X	X	X		X	
RM3003	X	X				X

Figure 2: Compliance Matrix

Makes Results Quantifiable

Numbered controls also enable an organization to calculate risk based on the number of controls that are being met and to report that risk in a quantifiable way in the audit findings.

Maps to Other Standards

Control standards can be built from and mapped to other standards, such as ARMA's Principles, ISO 15489:2001 – *Information and documentation – Records Management – Part I – General*, the Health Insurance Portability and Accountability Act, the Payment Card Industry Data Security Standard, the Sarbanes-Oxley Act, and so on.

Mapping can be shown in a compliance matrix as illustrated in Figure 2; this is useful when responding to management or customer requests regarding the organization's compliance with specific standards.

Scoping the Audit

The beauty of IG control standards is that they allow the audit's scope to be defined precisely. The policy is no longer an "all or nothing" requirement in an audit. It can be defined based on any number of factors.

For example, if an organization has acquired another company in the past year and had a resulting large influx of employees, it may be wise for it to focus an audit on the controls related to new employee training or merger and acquisition activity. Or, if an organization's litigation profile has increased recently, perhaps an audit should focus on the controls relating to the effectiveness of the legal hold mechanism.

The bottom line is that it is unrealistic and a misuse of resources to attempt to audit an entire IG program. Control standards allow an audit's scope to be limited to the most relevant controls and the highest risks.

Identifying Stakeholders

An IG audit should be a multiteam effort. While the IG professional may be accountable for the audit outcome and remediation, there may be other resources in the organization that can be leveraged. For example, it may be unrealistic to audit all locations of a multi-national organization, but stakeholders throughout the business can act as "boots on the ground." Logical stakeholders to invite may be records champions embedded in the business, loss prevention and/or physical security, internal audit, and risk management.

Control standards allow accountability to be assigned to these stakeholders. While IG owns the policy and maintenance of the controls, responsibility may be assigned across the organization. For example, controls

©2015 ARMA International

Dashboard Reporting

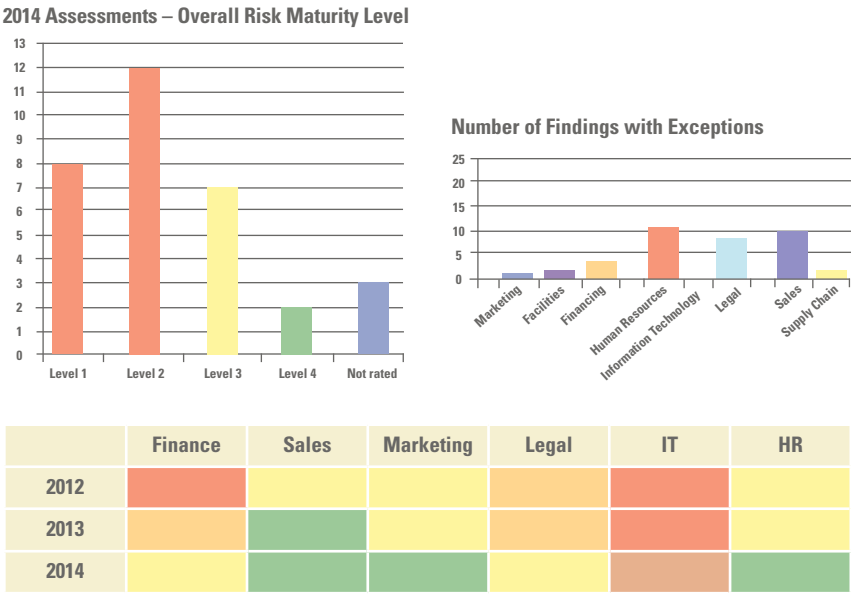

Figure 3: Dashboard Reporting

concerning paper records storage in an onsite records center may be the responsibility of facilities or physical security. Perhaps a member of the legal team is responsible for adherence to the controls of the legal hold mechanism. Internal audit may be responsible for controls requiring desk or inbox audits, and so on.

Obviously, it is very important to communicate and establish consensus on which teams are responsible for which controls. This approach allows the IG professional to focus on the organization's overall IG profile and not get caught in the weeds or be seen as simply the person responsible for pulling boxes.

Scoring Results

Score the results by audit category, but avoid becoming *too* granular. Take a risk-based approach that ranks results as 1-4 or as "critical," "high," "medium," and "low" risk. Senior management doesn't necessarily want to know all of the audit findings; it will want to know the highest risks. It is up to the IG professional to determine which audit findings are "high risk," and this will depend on the organization and the type of information it maintains. Use a dashboard like the one shown in Figure 3 to summarize the findings. A dashboard illustrates the cumulative risk across the enterprise and allows it to be tracked over time

Tracking Remediation, Exceptions

It is important to track remediation of high risk audit findings until they are corrected. A remediation plan is an important tool for this process and should be created with the business owner or functional lead.

On the remediation plan, record the organization and contact names, as well as the relevant control(s), cause of the deficiency, short-term remediation plan (to address high risks immediately), long-term remediation plan (to become in full compliance with the control), and potential impact analysis. Have the business owner agree to the plan and check the status of the finding every 90 days until it is closed.

Some findings may be impractical to remediate due to business or technical reasons. These must be documented under a formal exceptions process. Exceptions should be limited in number and valid for a finite period (typically three months to a year). Exceptions are temporary because the risk environment changes over time. It is expected that controls will be complied with as soon as possible. Exceptions should be revisited at expiration and go through an approval process if they are to be renewed. Compensating controls also must be put into place to mitigate the risk.

Finally, the risk must be accepted by someone in the organization with the appropriate level of authority – often a vice president or above. Using an exception management tool to track exceptions and map outstanding exceptions against control standards may be beneficial. When auditing again, focus on new controls or those with existing high risk findings.

Receiving the Payoff

Auditing an IG program does not have to be a daunting task when following these steps:

1. Adapt the IG policy using control standards.
2. Focus on high risk areas to limit the audit's scope.
3. Assign responsibility for specific controls to the appropriate stakeholders.
4. Communicate the findings using a dashboard to highlight high risk areas.
5. Track remediation progress and manage exceptions.

Following this plan will lead to manageable and effective audits, which will help the organization minimize its information risks, maximize its information value, and make its organization's IG practices legally defensible. **END**

Andrew Altepeter can be contacted at andrew.altepeter@gmail.com. *See his bio on page 47.*