The Principles and External Audits

Julie Gable, CRM, CDIA, FAI

External audits depend on documentation, and that can make them stressful, time-consuming, and psychologically draining for records and information management (RIM) professionals who have to produce the documentation quickly. Learn how to prepare and respond to an audit and how basing your RIM program on the Generally Accepted Recordkeeping Principles® can reduce the strain and deliver good results even when under intense scrutiny.

Third-party audits are a fact of life for organizations large and small. Some audits are limited in scope. A U.S. Department of Labor audit, for example, reviews employee job classifications and wage rates. Tax audits, on the other hand, encompass all income and all expenses and are generally broad in scope. Even non-profits are subject to audits by grant-makers who want to ensure that their funds are well spent.

Regardless of type, third-party audits have several aspects in common. The auditors must form an opinion of how, and how well, an organization conforms to the laws or standards that govern it. Auditors rely on direct observations, overall impressions, and first-hand inspections during onsite visits that can last from days to weeks. While on the premises, auditors test an organization's compliance or non-compliance by gathering evidence in the form of records and documentation. In the process, every principle of good recordkeeping will come under scrutiny.

Even though the outcome of an external audit is a judgement on company-wide compliance, the audit processes themselves are often the ultimate test of an information governance (IG) program. As the examples will show, this is particularly true for audits conducted in regulated industries. (See sidebar "SEC, FDA Regulatory Audits.")

Timing Is Everything

Though regulatory audits may be purely routine, they may be triggered by newspaper headlines, litigation, consumer complaints, or wrongdoing by other organizations in the same sector.

Audits may also be a surprise. At best, the U.S. Securities and Exchange Commission (SEC) gives a two-week notice for an impending visit. The U.S. Food and Drug Administration (FDA) may give no notice at all and simply appear at the reception desk. Like pop quizzes, external audits, even expected ones, are measures of what has been done to date.

An IG program based on the Generally Accepted Recordkeeping Principles® (Principles) and the Information Governance Maturity Model (IGMM) goes a long way to show that the organization takes its information management responsibilities seriously. Used well, these comprehensive tools guide in developing and sustaining an IG program that delivers reliably during even the pickiest inspections.

Work guided by the Principles also provides a number of spillover benefits that become very handy during the audit process. Finally, understanding the Principles can also uncover potential problems, which are best handled before an audit occurs.

IG Bedrock Principles

The Principles of Compliance, Accountability, and Transparency are the bedrock of the IG program and the backdrop against which audit scenarios unfold. In industries where information is a crucial part of the company's end product – financials and pharmaceuticals, for example – what affects IG affects the overall entity, as shown below.

Compliance

IG compliance requires the organization to review all applicable laws, regulations, codes of conduct, and ethics that apply to it. An organization makes and maintains records to prove that it does business in accord with these, and its policies reflect how it interprets them in their operations.

These internal policies impose a duty of compliance on the organization and its personnel, and auditors will test this. A common audit finding is that the company is compliant with the applicable regulations but out of compliance with its own policies, including its IG policies.

Transparency

Transparency means documentation of procedures and processes, something that auditors always want to see. This may be an investment manager's hard-copy compliance manual, or it may be the drug company's controlled set of standard operating procedures.

Either way, it's critical to have orderly documentation for policies and processes, to be able to show that the documentation is reviewed and updated periodically, and to be able to prove that the version presented is, in fact, the latest one. In FDA parlance, "If it's not documented, it's rumor."

SEC, FDA Regulatory Audits

Audits are particularly stringent in industry sectors where regulators have a duty to protect the public. In financial services and pharmaceuticals, for example, the stakes are high, and poor audit results can have severe business consequences. Investment advisors may lose their licenses; drug makers may be prevented from operating manufacturing plants.

With regulatory audits, size does not matter. In 2012, the Securities and Exchange Commission (SEC) began its "Presence Exam" initiative among newly registered investment advisers, many of whom are either independent small businesses or autonomous groups under the aegis of a major corporation.

Audits for these companies can include employees' use of social media; client communications via e-mail and texts; and brochures and advertising, including websites. Auditors check to see whether required records about trades, powers of attorney, custody, investment supervision, proxy voting, and personal trading are kept.

Auditors typically want to see client lists by account type and asset value, accounts opened or closed within a given period, pricing and quotation services, purchases and sales journals, chronological trade lists, and so on. They also want to see the company's own compliance manual to evaluate how well it adheres to its own policies.

The Federal Food, Drug and Cosmetic Act mandates the U.S. Food and Drug Administration (FDA) to inspect domestic drug companies at least once every two years. Inspections done prior to marketing approval for new drugs are particularly comprehensive, covering such topics as management controls, development processes, corrective and preventive actions, and production and process controls. Inspectors may test compliance with standards for good laboratory, clinical, and manufacturing practices.

The supporting materials for all of these are records. Standard operating procedures spell out what must be done, and records made and collected at each phase show what was actually done. FDA inspectors may enter, observe, collect samples, interview employees, and review any records – with limited exceptions – related to the regulated product.

How Audits Work

- Depending on its type, the audit may come with or without advance notice.
- Up to five inspectors usually arrive together.
- Most organizations assign the auditors to a conference room, making sure there is no writing on the whiteboard, flipchart easel, or other surfaces for the auditors to see.
- One or more people from the company – a compliance manager in financial services, for example, or a quality assurance manager in pharmaceuticals – will be assigned as the liaison for the auditors.
- Auditors request records through the company liaison. The liaison will contact the appropriate internal persons with the request. Each of these may, in turn, have to contact others to find the requested information. Runners may actually ferry documents among sites.
- All retrieved information goes to the liaison, who, in turn, gives it to the auditors. The liaison also keeps a copy of anything provided to the auditors, as well as a log of all requests made. At the end of each day, the liaison prepares a summary of what was requested and the topics discussed.
- If a requested record or document can't be found, auditors will almost certainly want to dig deeper to understand why. The auditors may want to understand company systems and processes in more detail to determine where the inability to provide the document is a procedural failure or indicates a more serious breach. They may also want to examine retention and disposition policies and procedures.
- Auditors can also conduct interviews as a way to compare actual practice with the company's documented policies and procedures. Interviewees should answer exactly what is asked and only what is asked. This can be particularly difficult with information management questions because an explanation of the system or method may be necessary to put the answer in context.

Accountability

Accountability says responsibility for records should be delegated to individuals and that defined roles and a chain of command should be established. For IG managers in large, multi-site companies, it can be particularly helpful in audit scenarios to know who their counterparts are at other sites and what records they manage.

In very small companies, there may be no chain of command; each department may take care of its own records, which is a dangerous practice when it comes to finding the "official" copy of a requested document. (See sidebar "How Audits Work.")

Explicit and Tacit Principles

Compliance, transparency, and accountability are explicit values that produce tangibles easily evaluated during an audit. The Principles of Availability, Integrity, Protection, Retention, and Disposition are tacit – that is, their presence or absence is implied in the handling of an auditor's every information request. The following are audit considerations for these "tacit" Principles.

Availability

Even though information may be well organized, the company may not have standard organization methods at each of its sites. Consequently, a simple request for a particular document may require multiple phone calls to people who know how to find this document in their own disparate systems.

Furthermore, there may be multiple copies of requested documents, and they may not all be the same version, so it will take time to ferret out which one should go to the auditor. The more time that elapses, the greater the impression that records are not readily available.

Integrity

A key point in some audits is that electronic systems that produce records actually produce the same results every time. This can apply even to Excel macros, with the need to prove, usually through validation records, that the macro is documented and has been tested thoroughly.

Audit trails, and records of how often audit trails are checked, also play a part in ensuring that records are unalterable. Record dates, in particular, should not change from system to system as they move through the chain of custody. Where third-party archiving services are used, as for customer communications in financial services, it is wise to have a letter from the third party stating how integrity of information is maintained.

Protection

A financial firm's client accounts will contain many fields of personally identifiable information and it is important to understand how this should be redacted in the course of an audit. In addition, requested documents may contain privileged, secret, or classified information, so it is important to know what the ground rules are for providing these. If auditors take photographs, it is advisable for the company to take the same photographs to ensure that no protected information is inadvertently captured.

Audit Survival Guide and General Advice

Orderliness counts. Don't leave records, files, or boxes strewn about; such disorder gives the appearance of disregard for good organization and protection. Auditors are forming a general impression from the moment they arrive.

Mum's the word. Make sure that all staff are aware that auditors are on premises and therefore they shouldn't discuss company business or the audit itself in elevators, hallways, cafeterias, etc. Make sure that everyone receives notice when the audit is completed. One company actually announces "Elvis has left the building" when the auditors depart.

Be flexible. An audit is an all-hands-on-deck situation. If the auditors opt to work late, staff responsible for fulfilling information requests must also work late. Make sure your staff knows where to find things and whom to call at other sites. Vacations can be disrupted by an audit.

Don't try to cover or hide deficiencies. It is better to acknowledge them and have a plan in place to correct them. Corrective action taken while the auditors are onsite can have a positive effect.

Courtesy and cooperation are the watchwords. This holds true at all times but is especially important during audits when nerves may be frayed by endless critical scrutiny. Remember that this too shall pass – hopefully in about a week.

Retention and Disposition

The Principles of Retention and Disposition may be assets or liabilities in the audit process. Retention schedules are policy documents that can legitimately justify why requested material is not available, and disposition records are proof that the organization had the requested materials at one time, but in the due course of business and in accordance with retention policy they were destroyed.

Needless to say, there should be a documented process for attaching a disposition hold to documents that are needed for audit purposes. Those organizations whose policy is to keep everything forever will find that they are expected to find anything that is requested, and those who suspend disposition of all records because of litigation may find that they are cited for being out of compliance with their own policies.

Audits and the IGMM

The higher an organization's level of maturity on the IGMM, the better its audit results will be, right? Perhaps, but even organizations operating an IG program with a maturity of 4 or 5 have no way of knowing how well that program will actually work under audit conditions.

For example, the organization may be at a level 4 for availability and have inventories of all systems, but some acquired legacy systems may not be part of the inventory. Sure enough, auditors request reports from a legacy system, sending many people scrambling to find them.

This is a real challenge in industries where there have been several mergers and acquisitions over a period of years. It is one reason why those who have a duty to preserve electronic records for long periods opt to establish electronic archives where crucial information of long-term value can be indexed, stored, protected, and available.

What is certain is that adopting the IGMM can't hurt. It provides a standards-based way to demonstrate that the company has a strategy in place to constantly improve IG elements. If nothing else, benchmarking against the IGMM gives the impression that the company takes its governance responsibilities seriously and works toward improvement goals as a matter of course, not just in response to audit findings.

Audits = Stress + Opportunity

The value of being prepared and knowing what to expect during an audit cannot be overstated. Working on an IG program guided by the Principles will automatically provide some of what is needed for audit success. Other strategies include reviewing a regulator's audit manuals to have a better idea of what will be sought and speaking to peers who have weathered the process in other companies.

Some organizations use internal audits or opt to use independent, third-party auditors to uncover deficiencies before regulatory audits occur. There are also seminars about the audit process that are tailored to those who work in regulated industries.

Even with excellent preparation, don't expect praise. Audits are stressful, time-consuming, and often done from a negative perspective. The auditors' mission is to discover faults. Remember that an art critic could find faults in the Mona Lisa. This is one reason why audits can be so psychologically draining. It helps to keep in mind the general guidelines described in the sidebar "Audit Survival Guide and General Advice."

Finally, even audit outcomes that are less than stellar can be beneficial. Audit findings must be corrected, and IG and records management, as always, tend to get much attention after a calamity occurs. Take advantage of the spotlight to get what is needed for your program. A not-so-great audit may be the kick that gives the IG program the boost it needs to move to a higher level of maturity, making for a better program – and better audits – in the future.

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