



# ***Surviving a Records Audit***

## ***6 Steps to Prepare Your Organization***

*Although most records are created electronically, physical records continue to proliferate and demand that organizations seek software solutions that meet the requirements for effectively managing records in both media.*

**Neil Simons**

In 2007, actor George Clooney and his girlfriend were cruising through northern New Jersey when their motorcycle was hit by a car and they were briefly hospitalized at Palisades Medical Center in North Bergen, N.J. There, according to *The New York Times*, the temptation to look at the famous actor's Health Insurance Portability and Accountability Act (HIPAA)-protected medical information proved irresistible to as many as 40 hospital employees. Some even tried to sell the records to the tabloids.

This fact was later uncovered during a records management audit of HIPAA compliance routinely conducted by the hospital's records management personnel. Needless to say, it caused quite a stir, and dozens of medical personnel were suspended without pay.

More importantly, the hospital uncovered serious lapses in its records management practices and was able to quickly institute records access policy changes to prevent future federal statute violations. What's more, the medical center's records managers emerged with their reputations intact, rather than being the scapegoats. This incident serves as a good illustration of the value of internal audits.

### **Why Audit Yourself?**

Every organization should consider a policy of regular records management audits for several reasons.

First, internal records audits are essential to ensuring your organization is following its internal standards and practices – and can prove it, if required, to external auditors, regulatory agencies, and courts.

Second, they are essential for complying with your organization's regulatory or oversight bodies and to ensure your organization's records are meeting regulatory criteria and the recordkeeping is legally defensible.

Records audits also can contribute to improved business processes – not just within records management itself, but within the business units responsible for the records.

Finally, but perhaps most importantly, if you regularly audit your records management policies, practices, and systems, you'll automatically be prepared for virtually any external audit scenario.

Testing your ability to pass an external audit usually means conducting a simulated audit based on your records management policies. You can conduct mini audits with a portion of your policies or audit all your records management policies at one time.

These types of internal audits can prove invaluable if an auditor from a regulatory agency calls you and gives you a week to prepare for a full-blown sales audit. If internal records management audits are part of your standard operating procedure, there's no reason to hit the panic button. Instead, it's just a part of your normal, routine business practices. You know what to do, your staff knows what to do,

and other players, like your IT department, know what to do.

Key to any organization's preparation is gaining an intimate knowledge of the operational, legal, and regulatory issues respective to your organization or industry. As a records and information management (RIM) professional, you must either know these issues yourself – or have access to resources that do – and build them into your internal records management audit practice. Those resources can be legal and financial experts within your own organization, government regulatory organizations related to your industry, professional associations, or professional networks.

### **The Costs of Waiting**

A failure to prepare for external audits can result in serious consequences with significant costs, both in terms of disruptions to your daily operations and the penalties associated with any compliance failures. Furthermore, these consequences can apply to organizations of any size.

For example, a major bank that gets hit with a Treasury Department audit as a condition of a financial bailout better have practiced internal audits many times before, or the delays and missing records associated with its lack of preparedness could be catastrophic. Similarly, smaller banks need to take the same precautions. Organizations of any size may literally have to shut down for days when surprised by an audit they knew could be coming, but had failed to prepare for.

Conversely, other organizations are prepared to effortlessly comply with U.S. Securities and Exchange Commission audits requiring the submission of thousands of physical records in as little as a few days. The difference is these organizations have made records management audits part of their standard operating procedure.

Furthermore, the cost of poor records management is showing up in some surprising new ways. For example, there's the so-called "produce-the-note" defense, in which homeowners demand the original mortgage paperwork from lenders who are trying to foreclose on their homes, who often can't comply. According to a 2008 University of Iowa study of more than 1,700 bankruptcy cases involving home foreclosures, the original note was missing more than 40% of the time. As a result, financial institutions stand to lose billions of dollars simply because they can't produce the original records.

Situations such as these can stop foreclosures in their tracks and turn up the pressure on lenders to renegotiate the mortgage. According to a February 2009 article by the AP, some judges have thrown out such foreclosure cases entirely, costing lien holders hundreds of thousands of dollars. For many of these lenders, it's an extreme example of the risks of not considering records management a business-critical operation.

According to a March 15, 2009, *Accounting Today* article "Small Business to Face Closer Audit Scrutiny" by Ken

Rankin, small businesses have been targeted for more rigorous scrutiny by federal tax enforcement officials and the nation's auditing standard setters. The reason? Many regulatory and legal agencies believe hard economic times will tempt many smaller companies to engage in financial chicanery. In its January 2009 document "An Audit of Internal Control Over Financial Reporting That Is Integrated With an Audit of Financial Statements: Guidance for Auditors of Smaller Public Companies," the Public Company Accounting Oversight Board was pretty explicit about the matter when it called for auditors to take a more hard-line approach to smaller companies, concluding: "The extensive involvement of senior management in day-to-day activities and fewer levels of management can provide additional opportunities for management to override controls in smaller, less-complex companies."

The financial and legal implications of poor records management are greater than ever. As mentioned, it can greatly affect the company and, in some cases, even the RIM professionals and other executives. As RIM professionals, if you are not prepared to meet every audit scenario, you can be held liable internally or legally. That could mean losing your job and the possibility of being sued by your former employer.

An investment in a proper records management function is a cost of doing business. You need the systems and technologies, the policies and procedures, and the personnel and facilities to meet the records management requirements. If those requirements include successfully meeting legal and regulatory compliance, your records management function will also need a regular policy of records management audits and assessments, which in turn require time and training.

All of this comes at a price – a price you often must justify to management and gain their commitment to address. In this situation, it's important for RIM professionals to make the case in

clear and unambiguous terms by identifying the:

- Legal and operational implications of poor performance
- Business disruptions resulting from being unprepared for an audit scenario
- Potential costs of being non-compliant

If management fails to associate records management with compliance, quality, and risk management – and balks at making that investment – don't slink back to your office, never to broach the subject again. If future audits unearth compliance issues or lead to excessive business disruptions, you could end up shouldering much of the blame. The bottom line: Make your case in writing – and make sure the information gets to the senior managers who will be held accountable.

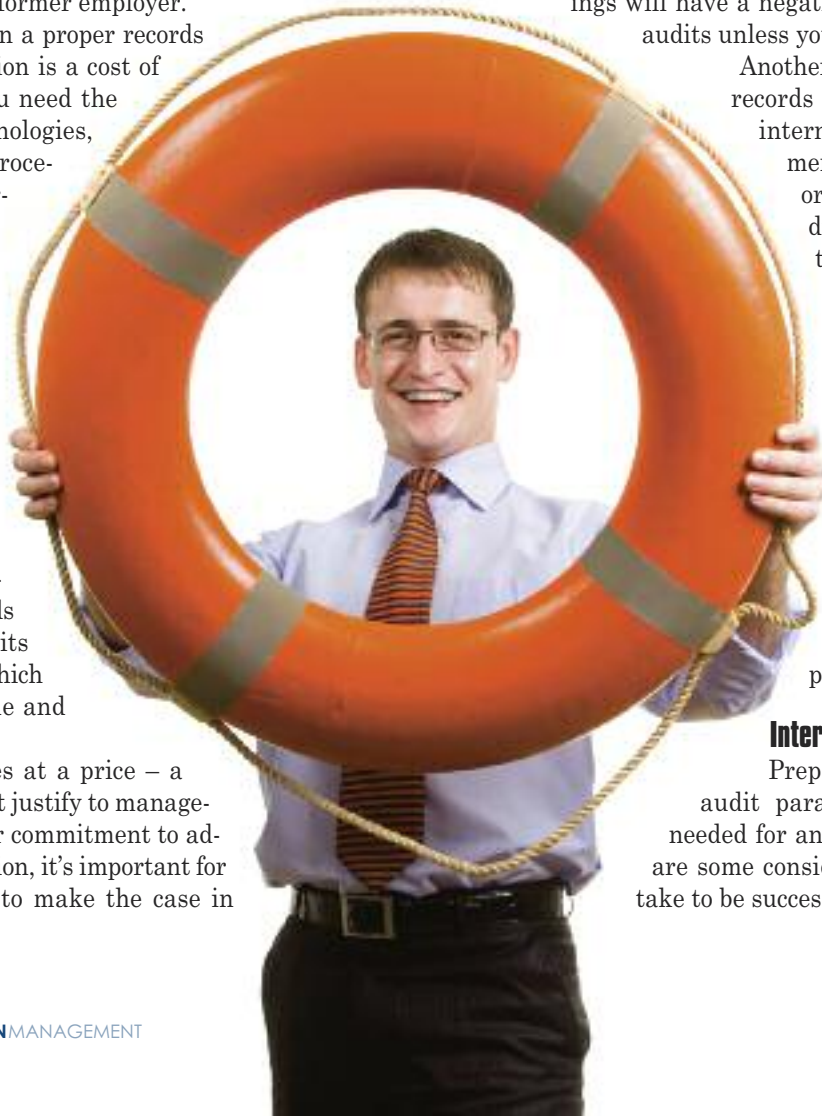
### Defining Internal Audit Intent

The purpose of an internal records management audit is to demonstrate that your policies, practices, systems, and training are sufficient to meet any audit scenario. For the audit, you're not interested in the content of the records themselves, but in how the records management program itself works. If shortcomings are revealed during internal records management audits, these shortcomings will have a negative impact on external audits unless you address them.

Another possible outcome of a records management audit is internal process improvement. You may find policy or practice shortcomings during an internal audit that have nothing to do with records management, but that may be very revealing about the organization operationally. This discovery benefit can be used as another data point to justify the importance of regularly auditing and assessing records management policies and practices.

### Internal Audit Checklist

Preparing for an internal audit parallels the preparation needed for an external audit. Below are some considerations and steps to take to be successful in both.



## **1 Understand all the requirements for every type of potential audit your organization faces.**

This includes the agencies that have the power to audit your company. Know the terms of those audits and the output the company will be required to produce. The most effective way to do this is to define the audit requirements, define the output, and work your way backward through all your policies and practices to make sure you can easily comply with all the various requirements of the audits.

## **2 Develop and maintain clear and well-documented records management policies.**

Policies should include:

- Retention and disposition policies
- Records access and security policies
- Frequency: Be clear about when and how often you conduct internal evaluations and audits. This should be based on the specific requirements of the various audits your organization is subject to and the dynamic nature of the records you manage. Test your policies and audit your practices until meeting these requirements becomes second nature.
- Training requirements: These can be very industry-specific. If you're a healthcare provider, for example, have you trained employees with access to records on HIPAA requirements?

## **3 Get management buy-off on those policies.**

This buy-off must be based on management's understanding and agreement that:

- Records management is a core requirement of the business, like human resources, sales, or any other key function.
- Management has the organizational and legal requirement to take direct responsibility for meeting all records reporting and compliance requirements.
- Management understands, at the highest levels, the costs and penalties for being unable to comply with audit requests. If an organization consciously decides to blow off an audit requirement, management must understand the risks and the associated costs.

## **4 Audit your records management practices.**

Audits should ensure you have the policies and procedures, systems and technologies, and facilities in place to meet all operational, legal, and regulatory obligations.

The key results of an audit should answer questions, such as:

- Are records complete? Often records management audits reveal that personnel responsible for creating records are not conforming to your records management policies – for example, a sales rep who is

keeping contracts at her desk instead of checking them into a file room.

- Did your internal audits identify security breaches in your records management policies? If so, determine a plan for addressing those breaches.

## **5 Document the results.**

Can you provide documentation to an external auditor that shows retention, disposition, security, and other records practices, and documents your internal compliance policies and the extent to which you are compliant with the terms of the audit?

It's also important to document your audit process itself, including roles and responsibilities, as part of your larger records management practices documentation. In large organizations with internal audit groups and smaller companies that lack such groups, documentation clarifies who is responsible for conducting audits, what types of documents and records they are required to produce, and the formats in which they should be produced and reported.

## **6 Audit your systems, technologies, and facilities, as well as your practices.**

The key question to ask here is, "Do your records management systems and technologies support your basic internal and external compliance requirements?" For example:

- Do they provide ways to track and audit retention management?
- Do they automate and enforce records destruction policies?
- Do they enforce security requirements, such as access control and tracking with recording and audit for physical and electronic records, and security for modification and deletion rights with tracking?

They can do more than required, or course, but they can't do less.

### **Sailing Through the Audit**

There's no such thing as a perfect audit, whether it's an audit of a records management program or other business processes. That's why a records management audit will clearly indicate opportunities for improvements, which may make a difference during an external audit. There is one standard of success in an internal records audit: Did you satisfy management's and your expectations of performance?

With an external records audit, there's only one standard of success as well – did you satisfy the obligations of your organization to the auditing agency? If you as a RIM professional can clearly answer "yes," then your organization is ready to survive an audit. **ENR**

*Neil Simons can be contacted at [neil.simons@smead.com](mailto:neil.simons@smead.com). See his bio on page 54.*