**Practical Considerations for Implementing a Record Retention Policy**

Information is everywhere and the amount of data and information that is created every minute multiplies as the years go by.[[1]](#footnote-1) Because of this vast proliferation of data and information, banks and employees tend to retain this information longer than is required by any statute or regulation for several reasons. One, data is data—it is not stored on a desk or in file cabinets and therefore keeping it in perpetuity on a computer does not prevent an employee from seeing his computer, unlike paper on a desk. As the saying goes, “out of sight, out of mind.” Second, many employees have no idea of the costs and risks associated with storing data and information that no longer needs to be retained by any statute, regulation, or legal hold and no longer provides any value to the bank. Finally, data is everywhere. It is no longer just on an employee’s workstation or a bank server. It is on their smartphone, in the cloud, or on their tablet or iPad. So what can banks do to manage the information that comes through their servers and stays there or on the myriad of devices and servers available to employees?

One answer is implementing a record retention policy. While there is no “one-size-fits-all” record retention policy for any organization, including banks, there are some considerations that banks can apply when implementing a record retention policy and schedule. First, banks and their employees must understand what a record is and what it is not. Not every piece of information is a record. For example, in the world of emails, personal, transitory, or informational emails are not likely records that need to be retained for any specific period of time.

Second, banks should consider the “buckets” of information that need to be retained. For example, certain records must be retained for a specific period of time by federal or state statute or regulation and others must be retained because of legal hold orders related to anticipated or current litigation. Those records must be retained for the period of time required by either statute or regulation or, in the case of a legal hold, until the litigation is closed and the legal hold lifted. A quick reference guide to statutory and regulatory record retention requirements applicable to banks is available from the Virginia Bankers Association.

Next, banks should consider which records without a regulated retention period have business value and how long those records have value. Retaining information simply because it may be useful in the future does not necessarily mean the information retains value.[[2]](#footnote-2) For example, records related to active projects have value for only a certain amount of time after the project ends and therefore, should not be kept indefinitely. Banks should perform a cost-benefit analysis with respect to each category of data they maintain that is not subject to a statutory, regulatory, or legal retention requirement to determine the benefits of retaining the information versus the costs and risks associated with its disposal.[[3]](#footnote-3) The cost-benefit analysis should consider applicable claims limitation periods. For example, in Virginia the general statute of limitations period for written contracts is five years, but it may be increased or decreased by statutes governing specific types of contracts or the terms of a contract. It is often appropriate to retain written contracts for the period the contract is effective, plus the applicable claims limitation period.

Banks should also consider where their records are stored, as they are no longer just in paper in an organized file cabinet. Banks should evaluate where their employees can store information —from their email mailbox to the desktop of their computer workstation to certain shared server files to even their personal tablet. Banks need to understand where their records are to effectively implement a record retention policy. Without an idea of the sources and forms of their records (paper, email, instant message), it is difficult to monitor compliance with any retention policy.

A record retention policy is an important component of an organization’s broader information and record management policy. Related matters that may be addressed in the broader policy include how documents are organized and indexed for efficient retrieval when needed, and how to protect and secure documents from unauthorized access or destruction.

Employees must be aware of the retention policy and follow it to effectively manage information. Information management cannot exist in a vacuum. Accordingly, the stakeholders in the retention policy, including leaders in record management, legal, information technology, bank operations, and finance/accounting, need to not only understand the retention policy but be its champions, including practicing what the retention policy preaches. Additionally, these stakeholders need to assist in informing and training bank employees on what the policy is and how they can comply with it. The more information that is provided to employees on what must be retained and what can be discarded, the more effective the retention policy can be.

For more information about record retention policy considerations contact Mel Tull, VBA General Counsel, at mtull@vabankers.org or (804) 819-4710. To purchase a copy of the VBA’s *Bank Record Retention Quick Notes*, contact Amy Binns at abinns@vabankers.org or (804) 819-4726.

*This article has been prepared for informational purposes only and is not legal advice.*

1. *See* Data Never Sleeps Infographic 3.0, https://web-assets.domo.com/blog/wp-content/uploads/2015/08/15\_domo\_data-never-sleeps-3\_final1.png. [↑](#footnote-ref-1)
2. *See* *The Sedona Conference Commentary on Information Governance*, 15 The Sedona Conference Journal 125, 148 (2014) https://thesedonaconference.org/download-pub/411. [↑](#footnote-ref-2)
3. *See* *id*. [↑](#footnote-ref-3)