



# Managing Your IT Audit/Compliance Program:

## 5 Steps to Improve Effectiveness and Lower Overall Cost

By Dwij Sharma

Senior Risk and Compliance Consultant  
Compushare, Inc.

Community banks and credit unions today face increasing challenges in effectively managing risks in the IT environment. Financial institutions must make sure they have an effective risk management program that responds to changes in the technology landscape while supporting governance and compliance goals. In today's difficult environment, it is more important than ever for management teams to implement an effective audit/compliance program and aggressively manage the program to minimize overall cost. A well-designed IT audit program provides an overall assessment of the effectiveness of bank governance, risk management and compliance programs. Therefore, it is imperative that management clearly understand the value and purpose of a properly designed audit/compliance program.

The keys to an effective IT audit/compliance program are (1) keeping it simple and (2) staying proactive. First, the institution must have an effective governance framework in place. For community banks and credit unions, implementing a commercially available IT governance framework could be a daunting task. But it does not have to be if kept simple. A good governance framework is one that ensures the following:

- IT objectives are aligned with the

institution's strategic goals.

- IT processes are designed to deliver value to the internal/external client and meet compliance requirements.
- Proper controls (policies, procedures and standards) are in place to manage risks in the environment.
- Proper tools are used to measure performance.
- IT resources are managed effectively.

Once the institution has implemented these components, an IT audit program can be put in place that delivers maximum value. Being proactive requires management to play an active role in designing an effective audit program. In most cases, community financial institutions defer to an outside provider to design and deliver IT audit services. While this approach serves an important function in providing an independent assessment to regulators and the external auditor, it neither ensures IT audit is synergistically aligned with the governance program, nor does it allow the institution to derive the most value at the least possible cost.

So how can the institution successfully implement and manage an effective IT audit/compliance program? Although there are many different ways to accomplish this goal, following is a practical, proven approach that will work well for most community financial institutions.

### Step 1: Establish an IT Governance Program

Implementing an IT audit/compliance program can be accomplished much more easily if you have well defined governance processes in place. If you are uncomfortable with your bank's governance program, take the necessary steps to formalizing a program to minimize your overall cost in maintaining and monitoring compliance and risk management programs. Consider bringing an external service provider on board who can offer the expertise to carry out this task more efficiently.

### Step 2: Set Clearly Defined Objectives

Be clear about the value you expect to derive from your audit/compliance program. An effective IT audit program should:

- Provide an assessment of bank compliance with regulatory requirement.
- Provide management with an assessment of bank governance processes.
- Focus on risk management, assessing the design and effectiveness of controls to ensure risk tolerances are appropriate and functioning as designed.
- Consider other compliance programs already in place to minimize redundancy. For example, testing for Sarbanes Oxley compliance should be coordinated and integrated with the IT audit program.
- Include testing to assess the effectiveness of controls judged to be appropriate. A poorly designed test will only uncover problem symptoms instead of the root cause. Often, the same issues appear year after year because the root cause is not addressed and the problem remains unresolved.
- Undergo periodic evaluations to ensure appropriate focus on key risks, as well as to assess the impact of changes in technology, business, and regulations.

### Step 3: Partner With an Outside Firm That is Right For You

Most community financial institutions lack adequate internal resources to design, implement, and execute an IT audit program. Diverse skill-sets are required and, at times, specialized tools to conduct testing.

Given the above, how do you select the right partner to assist in your IT audit program design? Of course, there are intangible factors unique to each institution (i.e., an established personal relationship or comfort level with a firm or professionals providing the services). But there are other very important considerations to be made that will determine



COMPUSHARE

Compass  
financial direction you can count on

program success.

- *Size of the service provider.* Your choices range from large and mid-sized accounting firms to small boutique firms. The tradeoffs are significant. The larger firms, due to their higher cost structure, typically offer a cookie-cutter solution and often provide junior-level resources in order to compete with lower cost providers. On the other extreme, very small firms could be more affordable but may not have the breadth and depth of expertise needed to instill a successful program. Look for a provider whose business model and cost structure aligns well with your objectives (Step 1 above).
- *Cost.* Overall cost factors will depend not just on the cost of the service provider's resources, but also on how well the provider understands your institution's risks and whether or not their approach is synergistic with existing compliance processes. Overall cost considerations should also include your time and other resources needed from your institution. Does the provider have the experienced resources, proper tools and methodology to run its engagement smoothly?
- *Business model.* Is the service provider client-focused? A firm that has deeply discounted fees in order to earn your business will look for areas to cut corners and probably will not put your service needs first. A little due diligence upfront will save you frustration and valuable time in having to manage an ineffective service provider.

#### Step 4: Focus on Risk Assessment

Don't underestimate the value of a properly developed risk assessment. A risk assessment is an essential component in establishing a governance program. Here are some key points to consider; they will help you manage the audit/compliance program effectively and could reduce your overall costs substantially:

- It is not unusual to find a bank with several risk assessments – one to comply with GLBA, another to perform

vendor due diligence, and yet another to determine audit coverage and frequency. You should consolidate all these into one encompassing risk assessment. GLBA provides a comprehensive guidance on developing one based on the size and complexity of your institution. If properly done, it will serve many different needs.

- Share your risk assessment with the examiners/auditors to demonstrate your proactive approach in managing risk and ensuring compliance. It will help facilitate any subsequent discussions by focusing on risks in resolving issues/findings.
- Use the risk assessment as a living document. Include new risks as they emerge due to changes in business, technology, or regulations, and periodically evaluate the whole assessment for accuracy and currency. It will serve as a practical tool to evaluate risks before introducing new products or services.

#### Step 5: Look for Continuous Improvement

Often, IT audit is managed as a once a year event to get an independent assessment of the IT control environment. A properly implemented program will bring far greater value to the institution. In addition to an independent assessment, it will complement your governance, compliance and risk management programs. You should continually look for opportunities to create greater synergies among the various pieces to manage and monitor risk management and compliance processes in order to reduce total cost.

In conclusion, an aggressive and proactive approach to establishing an audit/compliance program will pay dividends in many areas. You should look for benefits, not just in terms of improving risk and compliance monitoring, but also in streamlining overall governance processes to minimize duplication, optimize use of IT resources, and implement efficient processes. In the end, it means lower total overall cost to your financial institution.