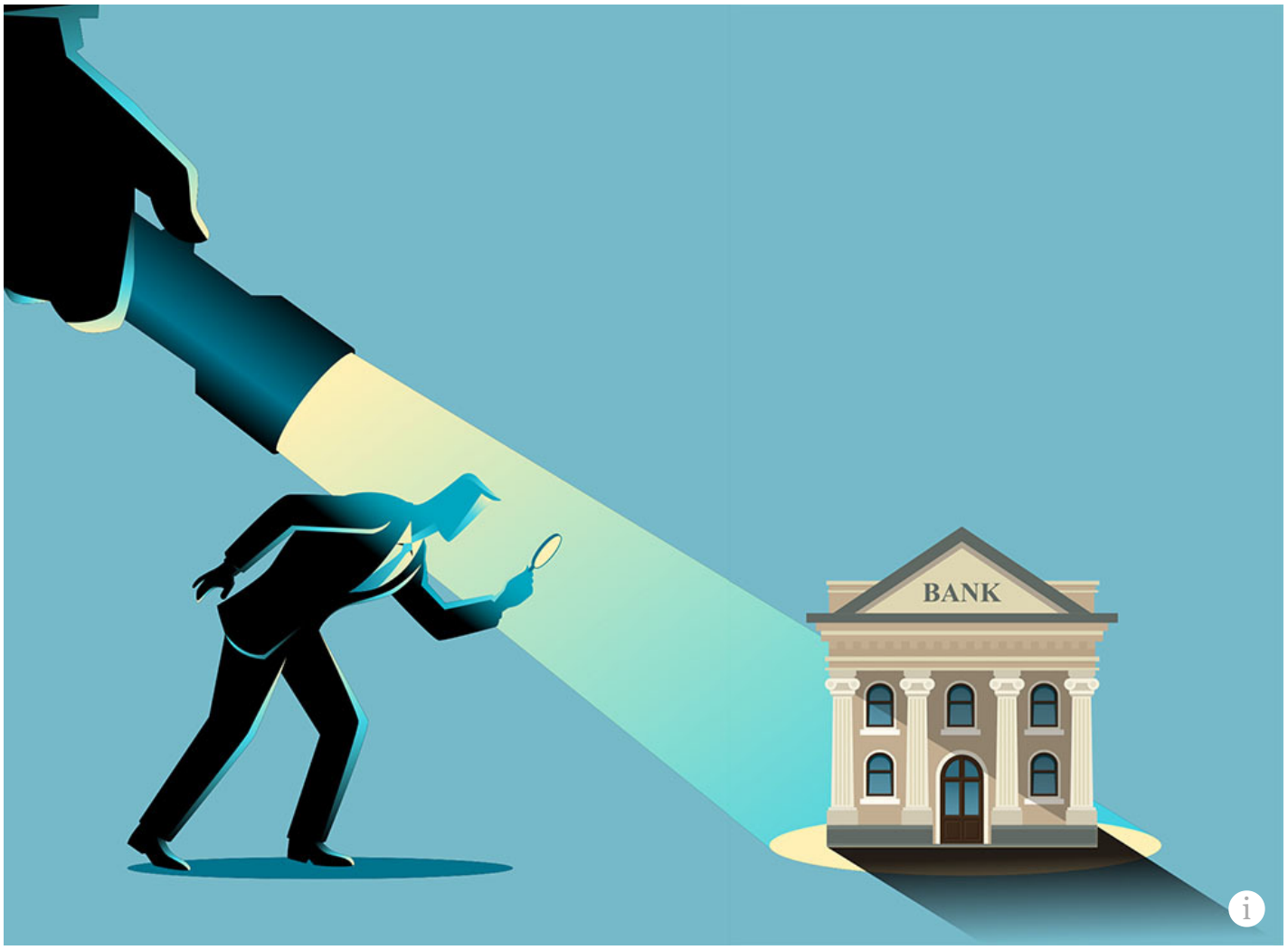
How to Audit Compliance Effectively

BY HEIDI WIER, CFSA



THE DYNAMIC NATURE of compliance has always posed additional challenges to the audit world. Differentiating between the operational role within business lines and the advisory role of the compliance department adds to this challenge. Auditors need to navigate between these complimentary components of compliance, all while handling slews of ongoing regulatory changes and emerging issues like COVID-19. Partnering with compliance, while still maintaining independence, can ease the impact of these challenges, increase audit effectiveness and add additional value to the organization.

Technical Expertise for Compliance Audit

The internal auditor role is complex and requires a diverse and broad perspective about the operations of the organization, internal controls, risks, best practices, etc. However, the level of compliance expertise needed to audit the bank's compliance program should not be underestimated. An effective compliance auditor must also have a strong understanding of both the technical regulatory compliance requirements and the practical application of the requirements in the day-to-day operations of the organization.

One frustration of many compliance departments is an internal auditor who does not understand compliance and how the rules are operationalized in the business. Without a solid foundation and understanding of the requirements, auditors lose credibility with both the business line and compliance team. Even within the realm of the compliance audit, additional specialization in areas of fair lending and Bank Secrecy Act/Anti-Money Laundering (BSA/AML) is warranted.

To ensure the quality of the compliance audit and add value to compliance and business lines, audit departments should invest in building an audit team that specializes in compliance audit. Numerous training opportunities are available to develop a specialized compliance audit team including those offered by the American Bankers Association, and various industry organizations. If developing compliance expertise in-house is not practical, consider teaming with third-party vendors who specialize in compliance audit to augment the team as needed.

Compliance Risk

The first step to audit compliance effectively is understanding the compliance risk faced by your bank.

The Office of the Comptroller of the Currency (OCC) describes compliance risk as "the risk to a bank's current or projected financial condition and resilience arising from violations of laws or regulations or from non-conformance with prescribed practices, internal bank policies and procedures, or ethical standards." Compliance risk exposes the bank to fines, penalties, lawsuits, voided contracts and can lead to diminished reputation, reduced franchise value, fewer business opportunities, among other things.

Preparing a compliance risk assessment will help you understand the bank's compliance risk profile and should drive your compliance audit plan. It will also provide the documentation and support needed to explain the scope and prioritization of compliance audits.

Like any risk assessment, the compliance risk assessment for determining the audit program should identify the bank's inherent risk and evaluate the bank's internal controls to mitigate that risk. Inherent risk increases or decreases with the complexity of the regulatory requirements and the nature and volume of the services a bank provides. The higher the volume and the more creative or unique the services, the higher the inherent risk. Complicated and changing regulations such as the Truth in Lending Act (TILA) or BSA/AML requirements typically have a higher inherent risk. Inherent risk is mitigated with strong risk management and mature internal controls. Residual risk is the risk that remains once the controls have been considered, and it is used to drive the audit scope, depth, and frequency of the audit program.

In most banks, especially larger ones, the internal audit risk assessment used to determine the audit plan is done independent of the first- or second-line risk assessment. Audit should review other compliance

risk assessments for differences in outcome. While the purpose and use of the risk assessments are different, the results should be similar. Material differences should be discussed with the compliance department and potentially resolved, or at least understood. This process provides a great opportunity to partner with compliance and fin-tune your compliance audit coverage.

A comprehensive compliance risk assessment should also include an understanding of the risk appetite of the Board and management. While higher risk can lead to higher profits, that is not usually the case for compliance risk. Instead, because regulators have a low threshold for errors, and regulatory issues can be very expensive, banks tend to have a very low tolerance for compliance errors. The key is to understand what level of compliance risk that management is willing to accept, and ensure strong internal controls are in place to mitigate that risk. In addition, products and services should be designed with that risk appetite in mind. Audit can then ensure that the products, services and controls are properly designed and effective, to protect consumers and the bank from losses.

It may also be necessary to complete specialized risk assessments for more complicated areas of compliance. These areas could overlap multiple business lines such as: BSA/AML risk, fair lending risk, privacy, and Unfair, Deceptive, or Abusive Acts or Practices (UDAAP).

Compliance Management System

The CFPB indicates a CMS is how an institution:

- Establishes its compliance responsibilities;
- Communicates those responsibilities to employees;
- Ensures that responsibilities for meeting legal requirements and internal policies and procedures are met; and
- Takes corrective action and updates tools, systems, and materials as necessary.

Assessing compliance risk by regulation or product should be determined on a case-by-case basis depending on the nature of the business. For example, risk relating to the Equal Credit Opportunity Act (ECOA) and TILA may be very different for a unique adjustable-rate mortgage loan than a standard car loan. The risk assessment for the mortgage loan should call out that higher risk. UDAAP risk will be more significant for an organization offering add-on products such as debt protection, credit monitoring, or payment protection products, and the risk assessment should specifically identify the higher risk for those products. Structuring the risk assessment by regulation and by product or service will ensure comprehensive input to the internal audit plan.

Be sure to include emerging or changing risks considering the current environment, economy, and industry trends. Certainly, the recent pandemic has changed most bank's risk profiles in many aspects of operations. Whether it's privacy-related risks with a workforce that is working from home, or servicing

issues as borrowers are recovering from job losses and interrupted wages, your risk assessment and corresponding audit plan should be updated throughout the year to reflect these trends.

Other areas of emerging risk will depend on the strategic direction of the bank. Partnering with fintech companies or thirdparty service providers, or banking marijuana related businesses, or digital currencies would all add additional risk to the bank's compliance efforts and will need to be addressed in the audit plan.

Developing and Structuring the Compliance Internal Audit Plan

Understanding your risk is the first step in establishing a comprehensive internal audit plan, and of course, that must be balanced with other constraints such as time, budget, and resources. As a result, often a multi-year audit plan is needed to provide appropriate, riskbased compliance coverage. An effective audit plan should allocate time to focus on high risk areas more frequently, at least annually, as well as audit areas that must be addressed on a particular time frame as prescribed by the regulations. For example, performing a BSA/AML audit every 12 to 18 months or a SAFE Act audit every year. Moderate and lower risk areas can be audited every other or every third year in the audit rotation, depending on the bank's risk tolerance. Be sure to allocate time in each year's audit plan to address emerging or unexpected situations that arise throughout the year. New products, new software, regulatory changes, or even a pandemic can derail an audit plan that is too time constrained.

It is also valuable to understand the compliance department's testing schedule and potentially structure the audit to reduce duplication of efforts in lower to moderate risk areas. This will add additional value to the organization and increase audit effectiveness. The trend in larger organizations is to structure compliance audits by product rather than by regulation whenever possible. Although it may be best to review some regulations on an enterprise basis, such as privacy or BSA/AML, aligning your audit plan operationally puts guard rails around the audit and helps to ensure:

- Management accountability for the process;
- Weaknesses are identified; and the
- Required remediation plan.

This is also the way compliance departments generally structure their compliance monitoring, and the Consumer Financial Protection Bureau (CFPB) and prudential regulators structure their examinations. For example, consider trying to tackle a TILA audit. For larger more complex organizations, that could be a nearly impossible task due to the numerous topics, products, and business lines it spans. TILA impacts almost all loan types and has requirements related to loan originator compensation, advertising, billing error resolution, periodic statements, etc. Rather than trying to do a TILA audit, it is often more effective to complete an audit by operational area of the organization. For example, mortgage lending, loan servicing, credit card operations, or marketing. The granularity of the audit will depend on the complexity and structure of the organization and the products offered.

Keep in mind too that once you dive into a loan file to test it for TILA, it is more efficient to continue to test the same loan file for the other regulations that apply, such as Real Estate Settlement Procedures Act (RESPA), ECOA requirements, flood determination requirements, appraisal notices, electronic signature requirements, etc. So rather than completing a TILA audit, it will be more effective to complete an audit of mortgage loan compliance, and separate audits for compliance with loan originator compensation requirements and advertising requirements.

An efficient audit plan will align compliance testing with operational areas of the organization whenever possible. In addition to testing the products (e.g. loans), and the business line processes for compliance, audit should also incorporate the role of the compliance department in the process as it relates to the Compliance Management System (CMS). For example, does compliance management have any additional concerns that should be addressed in the audit plan, what monitoring has compliance completed, what issues were identified, and how were they remediated. Did the audit results confirm that remediation efforts were successful, or were other issues identified that were not noted by compliance. Collaborating with the compliance department can help to identify the root cause of compliance issues and provide practical and effective recommendations for improvement.

The trend in larger organizations is to structure compliance audits by product rather than by regulation whenever possible.

The Impact of Compliance Culture and Responsible Conduct

Regulators are increasing their focus on a bank's compliance culture, and compliance auditors should do the same. In addition to a bank's CMS and the technical regulatory requirements, a compliance internal audit plan should include an assessment of the bank's compliance culture. Recent trends in the banking and compliance industries have proven that compliance policies and procedures are not enough to assure compliance. Enforcement actions and penalties for violations are still too prevalent and remind us that there is still a lot of room for improvement. One way that organizations are trying to improve compliance and reduce the number of compliance issues faced by the organization is by fostering a culture of compliance across every aspect of the organization. Compliance culture is a combination of tone from the top, social and bank norms, training, communications, internal controls, and alignment of incentives with compliance values. Leveraging experiences from internal compliance staff, compliance reporting results, and remediation efforts will provide the auditor with additional insight into a bank's overall compliance culture.

The CFPB recently issued a bulletin (CFPB Bulletin 2020-01) addressing responsible business conduct and building a culture of compliance in order to minimize the likelihood of violations and prevent consumer harm. The bulletin focuses on certain factors including self-testing for the prevention or early detection of violations, prompt self-reporting of violations, full remediation of any issues, as well as cooperating with the CFPB, which is further described as the quality of an entity's interaction with the CFPB after it becomes aware of a violation.

Whether completed as a separate audit, or as part of each compliance audit, some items to consider when auditing the compliance culture include evaluating the following:

- Management's response to self-identified issues or issues identified in audits or examinations. Findings should be addressed promptly, include expanded testing if needed to: identify the full extent of the issue, provide reimbursements to consumers if needed, and implement operational changes to policies, procedures, and practices to address the root cause of the issue and prevent recurrence.
- Employee compensation, incentive plans, and key performance indicators (KPIs) for reasonableness and alignment with compliance directives and bank core values.
- Communication of core values and strategies from all levels of leadership.
- Restrictions and monitoring of exceptions to policy or management overrides of control.
- Ethics and Code of Conduct training provided reiterating the bank's standards.
- Risk escalation protocols or the existence of whistleblower hotlines and how concerns are addressed by management.
- Established procedures and committee review and approval of new products and services, as well as marketing materials and sales methods.

An organization's compliance culture is often fluid and intangible, and compliance auditors should continue to strive to assess the compliance culture and alert management to potential issues or concerns.

Auditing compliance is challenging in today's changing environment. Successful audits are dependent upon the auditor's understanding of the technical regulatory requirements and how they are operationalized throughout the business lines. While maintaining the independence of the third line of defense, auditors should collaborate with compliance to fully understand the bank's compliance risk and develop and execute an audit plan to best address that risk. By maintaining open communications and working with the compliance department, auditors will be better positioned to protect the bank's organizational value and provide meaningful recommendations and insight.

ABOUT THE AUTHOR

HEIDI WIER, CFSA, is a managing director at CrossCheck Compliance LLC, a nationwide consulting firm providing regulatory compliance, internal audit, fair lending, loan review, and litigation support services to the financial services industry. Heidi has over twenty-five years of experience in the financial and professional services industries consulting with banks, mortgage companies, and fintechs of all sizes on their internal audit and compliance needs. Prior to joining CrossCheck, Heidi was the Director of Internal Audit and Financial Institutions for an international professional services firm, and held positions in internal audit, mortgage operations, and compliance with Banc One Corporation. Heidi can be reached at **hwier@crosscheckcompliance.com**.