BUILDING AN EFFECTIVE COMPLIANCE SCORECARD

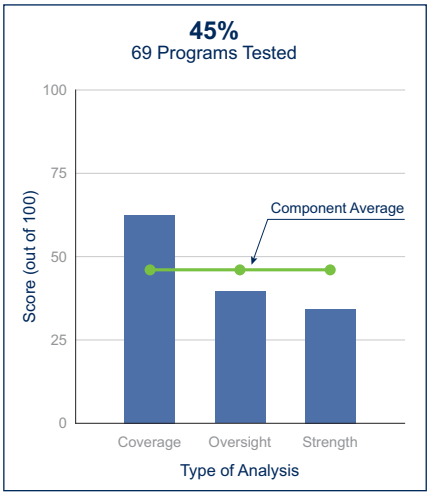
FOR YOUR FINANCIAL INSTITUION

Continuity

white paper

Do you have an effective way to monitor the state of your compliance programs?

Sample Compliance Scorecard



Scoring a financial institution's composite and component scores across all compliance programs.

Introduction

Community banks and credit unions across the U.S. are facing a compliance crisis. Throughout the last two years, nearly 10 percent of financial institutions have been under enforcement action. The Bank Secrecy Act, safety and soundness, consumer protections, mortgage lending and vendor management are just a few of the regulatory focal points that have turned compliance on its end over the last decade.

As the risk of non-compliance looms large, CEOs and compliance officers aren't the only ones frustrated by a steady increase in regulatory updates and overwhelming page volumes. Examiners have long acknowledged that financial institutions need a comprehensive and consistent way to process, enforce and monitor compliance across the organization – yet few institutions have taken these measures. They are losing patience and that has added a new dynamic to the compliance landscape.

Examiners, perhaps most of all, understand that the current way by which most community financial institutions manage compliance is not tenable in the long run. The complexity and cost of compliance has never been greater. Every quarter for the last two years, an additional 1.5 to 2.3 full-time equivalents have been required to handle the additional workload required to comply with each quarter's regulatory changes. During this time, the incremental cost of compliance per quarter has been between $35,000 and $40,000. As these trends continue, it has become cost-prohibitive for community financial institutions to simply hire their way out of the problem.

The solution requires a fundamental shift in the way financial institutions view the underlying problem. Compliance is not an all or nothing game. In fact, it's impossible for most financial institutions to be 100 percent compliant all of the time. Examiners understand this. However, they expect banks and credit unions to be *mostly* compliant, while providing an accurate picture of areas of risk. This requires an effective way to monitor the state of their compliance programs, identify the areas where they need improvement and apply resources accordingly. And, like all aspects of banking, this understanding and process must be well-documented.

One measure used to monitor, identify and document compliance risk mitigation is a regulatory compliance scorecard. This tool can be used to find and eliminate blind spots in an institution's compliance programs, as well as demonstrate to examiners that the financial institution is aware of

Continuity

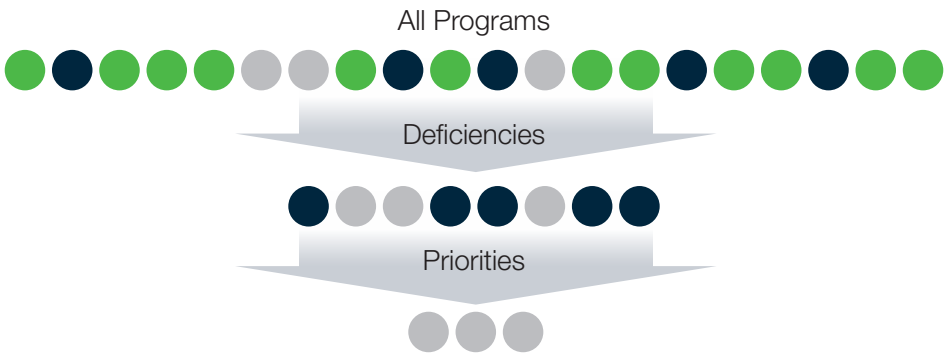
high-risk areas and has an action plan for abatement. Finally, it can be used to navigate course correction.

So, how can community banks and credit unions use a compliance scorecard to meet examiner expectations and minimize risk in their compliance programs?

Foundational Elements of a Compliance Scorecard

At a definitive level, a compliance scorecard is a repeatable way to measure and score all compliance programs, determine deficiencies and prioritize action. Conceptually, its application looks a lot like an inverted triangle where a large number of programs are measured, high-risk areas are identified and remediation is prioritized. For example, a financial institution can use the scorecard to measure the effectiveness of each of its 50 different compliance programs. Out of 50, there may be 10 programs that have deficiencies, and out of those 10, there may be five that have significant deficiencies. The scorecard enables the financial institution to determine these deficiencies and prioritize which programs need immediate attention.

Scorecard Conceptual Overview



A compliance scorecard is a repeatable way to measure and score all compliance programs, determine deficiencies and prioritize action.

Some compliance scorecards take the form of automated tools, while others are homegrown. Regardless of whether the tool is proprietary or created by a third-party, it should provide an informational report that quantifies program strengths and weaknesses, identifies risks, and points the institution to clear, concise and actionable results. It should also establish a documented benchmark so financial institutions can see how their compliance programs and risks are progressing over time.

For a compliance scorecard to be effective, it must meet three foundational requirements to provide a documented benchmark for financial institutions to measure their compliance programs progress over time. **An effective scorecard must be:**

1. **Objective.**
   The scorecard must objectively apply measurements – a "score" to each regulatory area. It's not a gut-check; it's evidence-based.

2. **Complete.**
   All regulatory areas must be included in the scorecard to provide a comprehensive view of the state of compliance and priorities.

3. **Repeatable.**
   The scorecard must allow for a routine, consistent measurement of progress.

Continuity

What is a Regulatory Scorecard?

Scorecard Uses	Target Audiences
Exam Preparation Annual Assessment Planning Sessions Committee Meetings	Executive Leadership Board of Directors Compliance Committee Examiners

Compliance Gaps – The 10 Most Commonly Missed Programs

1. Compensation Practices
2. Complaint Resolution
3. Children's Online Privacy Protection Act (COPPA)
4. CEO Succession
5. E-SIGN and E-Disclosure
6. IT Change Control
7. Credit Card
8. Record Retention
9. Servicemembers Civil Relief Act
10. Anti-harassment

Getting Started - 3 Steps to Effective Scoring

Assuming the compliance scorecard meets the requirements and objectives previously specified, the tool can be used to score and analyze three key areas – gaps, structural effectiveness and oversight.

Gap Analysis. The purpose of this analysis is to determine if all applicable compliance programs have been established and are represented in the scoring process. The average financial institution needs anywhere from 50 to 100 compliance programs to meet today's regulatory demands – a surprising number for many community banking leaders. The actual number for each institution is dependent upon the bank's unique regulatory requirements driven from operating model, products and services.

While this initial step seems simple enough, the ramifications it has on compliance risk are great. Part of the overwhelming complexity that surrounds compliance is determining how different regulatory requirements impact the individual institution. To conduct a thorough gap analysis, compliance professionals and the executive team must ask themselves the following questions: What areas and changes are applicable to our financial institution? Which programs do we need to have in place? Which programs are we missing?

Structural Analysis. Once the right mix of compliance programs are identified, each policy and procedure needs to be scored based on its structural soundness and effectiveness. This includes determining if each document contains the right anatomy:

- **Controls** – Are there controls present to prevent, detect and correct issues? These include the dos and don'ts as well as limits and thresholds relative to the regulatory requirements pertinent to each program.

Continuity

- **Risk Assessment** – Are regular risk assessments specified for each program?
- **Training and Testing** – If required, are ongoing training and testing requirements included in the policy?
- **Audit** – Is there an ongoing audit structure in place to ensure controls are enforced?
- **Review** - Is there a formal process to update and review methodology?

When evaluating the structural soundness of each policy, community financial institutions should avoid getting hung up on word choice. Instead, the policy should be evaluated on its effectiveness in communication. Is it written in such a way that the intended audience can understand requirements and expectations? Or is it full of jargon and regulatory-speak? Is it comprehensive and specific in its intent, or is it lacking the key elements and clarity of a strong policy?

Oversight Analysis. Examiners are placing more focus on compliance program oversight – from the board level all the way down to the individual program owner. It's important for financial institutions to make sure every compliance program has the proper oversight responsibility from the right person within the organization. Analysis of program oversight should explore the following questions:

- Does the program have a clear owner? If so, is this owner the best person/role for the job?
- Is the ownership documented? Is it easy to understand? Be on the lookout for contradicting information. For example, ownership may be assigned to a BSA officer in one part of the program policy, then referenced as the compliance officer in another part.
- Is the owner specified currently employed? This is a big one, especially if the owner is specified as a person instead of a role. For this reason, consider assigning ownership to specific roles versus named employees.
- Has the program been reviewed in the last year to make sure it's policies and procedures are current and relevant? Clear, consistently maintained documentation is a sign of strong oversight; if a policy hasn't been reviewed in a while, it's a sign of poor oversight.

Tips for Effective Evaluation:

- Don't get hung up on word choice
- Evaluate policies in terms of effectiveness in communication
- Consider intended audience
- Ask intended audience for assistance if needed

Continuity

Ready, Set, Prioritize

After conducting gap, structural and oversight analysis on each program, it's time to prioritize the findings of the scorecarding exercise. First and foremost, financial institutions should focus on the results of the gap analysis. Is the institution missing any compliance programs? If so, this is the first area of focus and action. For programs that lack structural soundness or proper oversight, the following questions should be asked:

- **When is the next expected exam date for this program?** If you have an exam coming up in the near future, deficiencies in this area need to be addressed sooner rather than later.
- **How did the program rate at the last exam?** If the program was rated poorly, then this should be a red flag for high priority.
- **Any historical issues with a particular program?** Those programs that have been closely scrutinized within your institution, or institutions of similar size and scope, are more likely to receive additional scrutiny in the future. Consider this when prioritizing.
- **What regulatory areas are experiencing the most volatility and enforcement action right now?** Recent enforcement actions and regulatory updates are clear indicators of where examiners will be applying more focus in the future, and should factor into which problem areas should be addressed first.

Once priorities are set, it's time to establish an action plan. It's important to use a formal approach for consistency and ongoing monitoring. Every action plan should convey the following:

- **Clearly stated objectives** – what are you trying to accomplish?
- **Indication of priorities** – where does this action fall on the priority list?
- **Clearly communicated action items** – what needs to be done?
- **Ownership** – which one person or role owns the actions?
- **Start dates** – when an action needs to be begin.
- **Deadlines** – when an action needs to be completed.
- **Resource needs** – what financial and human resources are required to meet the objectives?

Action plans can be a part of an automated compliance management system, or can be a standalone action plan. Regardless, it needs to be detailed and used as an ongoing mechanism to track completion percentages, deadlines and status updates.

Continuous Compliance Improvement for Community Institutions

Compliance risk is unavoidable in today's regulatory environment – especially for community financial institutions that have limited financial and human resources to devote to the issue. Rather than view compliance with an all or nothing mindset, community banks and credit unions need to focus on understanding where compliance risks lie, and how they can measure, monitor and mitigate those risks in a prioritized, realistic way. A compliance scorecard accomplishes these goals. It identifies gaps in compliance program coverage, structural and oversight deficiencies, and provides an effective tool for prioritizing and monitoring risk mitigation activities.

It's important to note that scorecarding isn't a one-time event; it's a process. Whether it's performed manually, using a homegrown tool, or automatically through a third-party system, it should provide a repeatable measure – one that ensures continuous compliance improvement across all areas of the business.

About Continuity's Compliance Scorecard

View a recorded Webinar to learn about how the Continuity Scorecard works.

click to view online

Continuity

www.continuity.net

ICBA Preferred Service Provider®

ABOUT CONTINUITY

The Continuity Compliance Management System (CMS) is uniquely engineered to reduce regulatory impact (time, cost and risk) for community banks and credit unions. This single, unified system automates the entire regulatory lifecycle — managing regulatory updates, policies, procedures, risks, vendors, audits, business continuity and exam preparation along with compliance strategy and planning. Built by bankers and former examiners, the system's advanced software has been coupled with expert personalized service to help financial institutions quickly adapt to regulatory change, streamline the workload and ensure compliance. Continuity is the exclusive ICBA Preferred Service Provider for a Compliance Management System. For more information visit **www.continuity.net**.