CORNERSTONE
ADVISORS

EMBEDDED COMPLIANCE:

A New Approach to Containing Rising Compliance Costs and Improving Results

COMMISSIONED BY

COMPLIANCE
SYSTEMS

TABLE OF CONTENTS

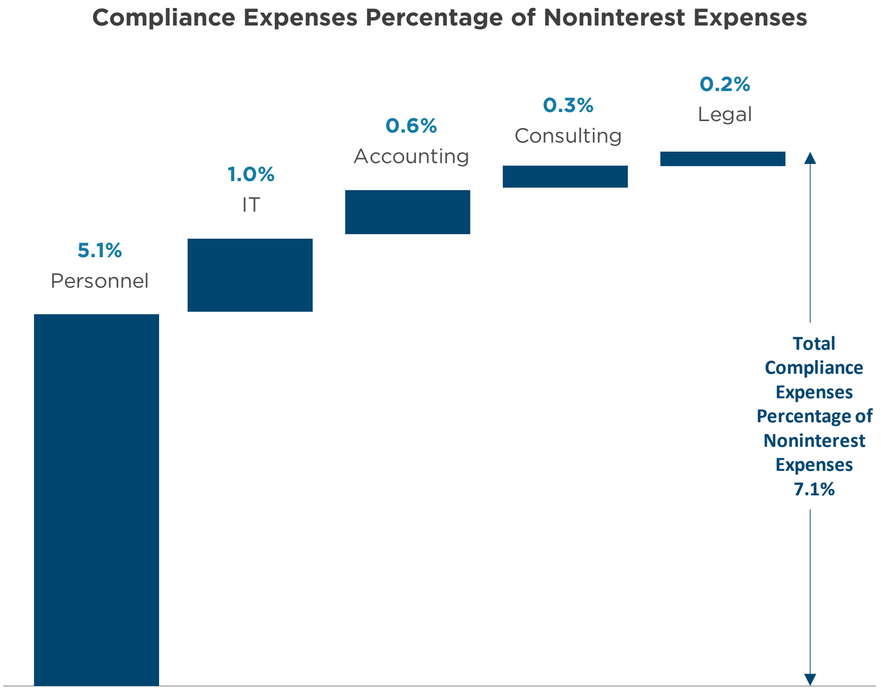
INTRODUCTION

Regulatory guidance for financial institutions (FIs) has become more burdensome in recent years, and the ever-changing and strengthening of requirements is not likely to move in the opposite direction anytime soon. According to International Banker magazine:

> *"Banks spend $270 billion per year on compliance. Some 10 percent or more of most bank operating costs can be attributed to compliance, and some estimates have regulatory costs doubling by 2022."*

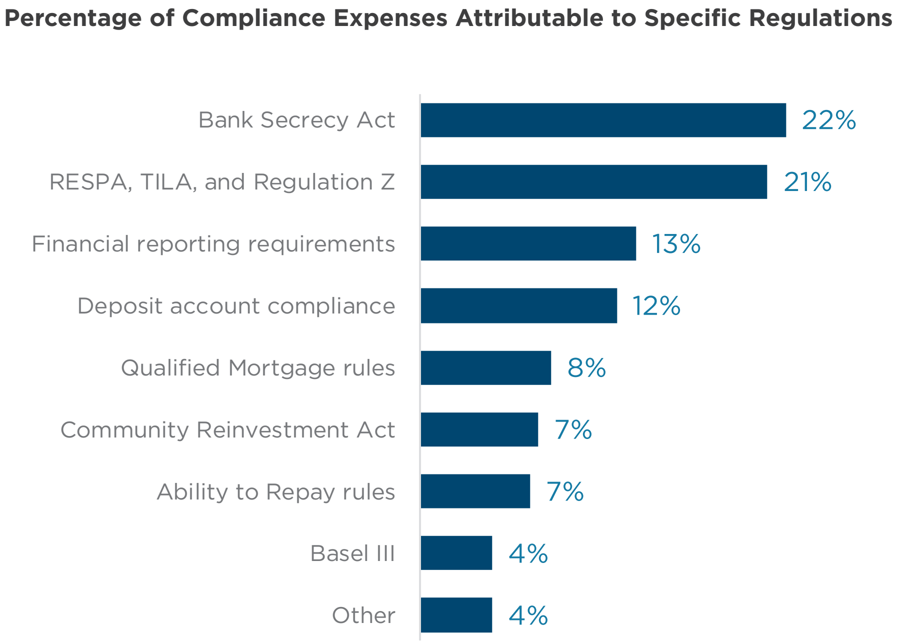
According to the Federal Bank of St. Louis, compliance expenses account for 7 percent of banks' noninterest expenses (Figure 1). In addition, the Fed estimated that the Bank Secrecy Act, RESPA, TILA and Regulation Z combine to account for 43 percent of banks' compliance costs (Figure 2). The proliferation of bank-related regulations over the past decade adds new costs—and increased complexity—to compliance management every year.

FIGURE 1: Compliance Expenses Percentage of Banks' Noninterest Expenses



Source: Federal Reserve Bank of St. Louis

FIGURE 2: Compliance Expenses Attributable to Specific Regulations



Source: Federal Reserve Bank of St. Louis

With the increased speed at which consumers desire digital delivery of financial products and services, FIs struggle to meet these requirements.

It is common to see FIs try to handle their compliance efforts—which are often manual-intensive—by adding new tracking and reporting systems and additional layers of auditing. Usually this involves adding headcount, a tactic that is often supported by regulatory agencies. In addition, many FIs centralize as much as possible in order to maintain some level of controls. We hear line managers say:

> *"We really struggle to manage it all. We should be implementing more controls but just can't seem to find the time."*

These actions are survival tactics. FIs end up in a perpetual cycle of cleaning up the data after-the-fact. These methods don't get at solving the root cause of the problem and usually result in adding costs in the hope of satisfying regulatory requirements.

A NEW APPROACH: EMBEDDED COMPLIANCE

How can FIs deal with the intersection of tighter regulatory guidelines (higher quality) and increased speed of delivering digitally, while reducing costs and staying competitive?

One approach is embedding compliance into digital delivery processes. Embedding compliance can help FIs grow their business while simultaneously moving the measures of quality, delivery (speed) and cost in the proper directions. There are examples in digital banking where FIs are using software applications that have artificial intelligence tools to help identify compliance problems.

It sounds simple, yet identifying a problem is the result of first defining what the requirement or standard is. Once that is set, FIs can identify gaps, or problems, in processes that don't meet standards. Using artificial intelligence software could surely help, provided the gaps that appear are fully understood. Therein lies the rub, and that's just in the problem-finding part.

Next comes the most important part—developing ideas to solve the problem, testing them (and learning from those tests), and then implementing what was learned as improved controls (countermeasures). This problem-solving process is fundamental to an embedded compliance approach.

When it comes to compliance, do FIs have a good grasp on what their regulatory requirements are? A senior leader in charge of a community bank's lending operations said this:

> *"Our internal silos have worsened as we've grown. The teams don't understand each other's requirements. We have organizational dysfunction, for sure, and in the end the loudest voice tends to prevail."*

Similarly, a director in charge of deposit and loan operations had this to say:

> *"Internally, we all seem to have different interpretations of the regulations and a lack of understanding of what is required."*

If the requirements are not clearly understood, and there is not an established definition of what is acceptable versus not acceptable, then FIs don't have much of a chance of getting compliance right. This is surely not a problem that artificial intelligence can help with—FIs will need actual intelligence to solve the problem.

How do FIs move forward with embedded compliance? Through 1) Organizational structure, and 2) Process design.

ORGANIZATIONALLY EMBEDDING COMPLIANCE

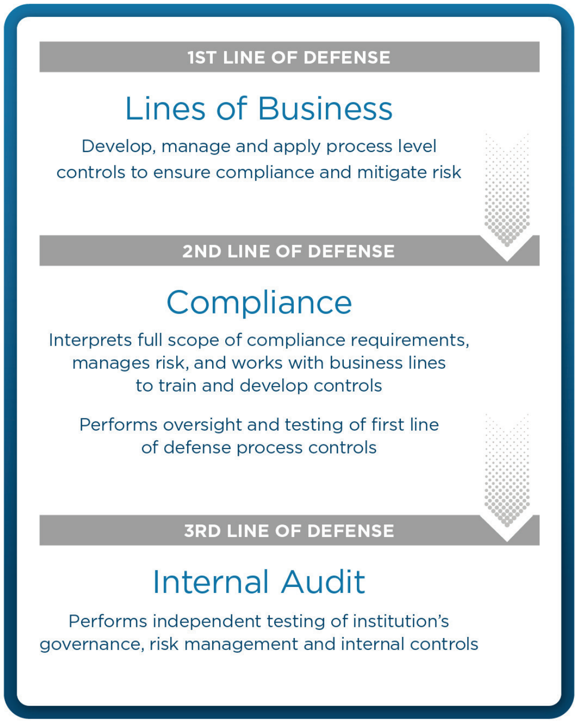
Components of an organizational approach to embedded compliance include a focus on the following areas:

- High-level governance and organizational structure
- Regulatory communication protocols
- Risk assessment methodology
- Policies, procedures and controls
- Training
- Monitoring and testing
- Reporting

When it comes to the organizational structure for a compliance and risk management program, a common approach is to follow a "three lines of defense" structure (Figure 3).

FIGURE 3: Three Lines of Compliance Defense

Three Lines of Compliance Defense



1ST LINE OF DEFENSE

Lines of Business

Develop, manage and apply process level controls to ensure compliance and mitigate risk

2ND LINE OF DEFENSE

Compliance

Interprets full scope of compliance requirements, manages risk, and works with business lines to train and develop controls

Performs oversight and testing of first line of defense process controls

3RD LINE OF DEFENSE

Internal Audit

Performs independent testing of institution's governance, risk management and internal controls

Source: Cornerstone Advisors

Much of what we see occurring in FIs today, however, is the result of focusing primarily at the second and third levels (compliance advisory and audit) and not enough on active—that is, embedded—participation at the first line of defense. This results in perpetually treating symptoms rather than developing, educating and supporting problem solving to address the root cause of regulatory gaps and risks.

Embedding compliance organizationally involves clearly identifying subject matter experts for each of the regulations in scope. These experts are typically found within the second line of defense. This is not a small undertaking, and smaller FIs will need to rely more on external resources to ensure complete coverage.

Next, clear assignment of the second line subject matter experts to the first line of defense (business line units) where the regulations come into play must occur. This assignment works best when coupled with a physical embedded presence as a part of the work team. The interactions between regulations and ever-changing daily situations require a continuous monitoring and involvement in problem solving.

SETTING UP SMALL IMPROVEMENT TEAMS

To facilitate problem solving and achieve embedded compliance organizationally, it's crucial to involve key line of business stakeholders and form small improvement teams.

This concept of forming small improvement teams has existed for many years in industries outside of financial services and is the key ingredient in an embedded compliance approach that achieves the highest level of quality.

In manufacturing, for example, quality control (QC) teams, or QC Circles, are a well-established approach to embedding quality into the organization. For whatever reason, this approach is rarely seen in FIs today. The teams are best kept to two to five people and are ideally composed of the following functions:

- People who do the work every day (core)
- Line of business leads/supervisors/managers (core)
- IT support/system administrators (support – multiple teams depending on size of FI)
- Compliance subject matter experts (support – typically multiple teams)
- Problem-solving guides (support – ideally this skill is embedded into the line leaders)

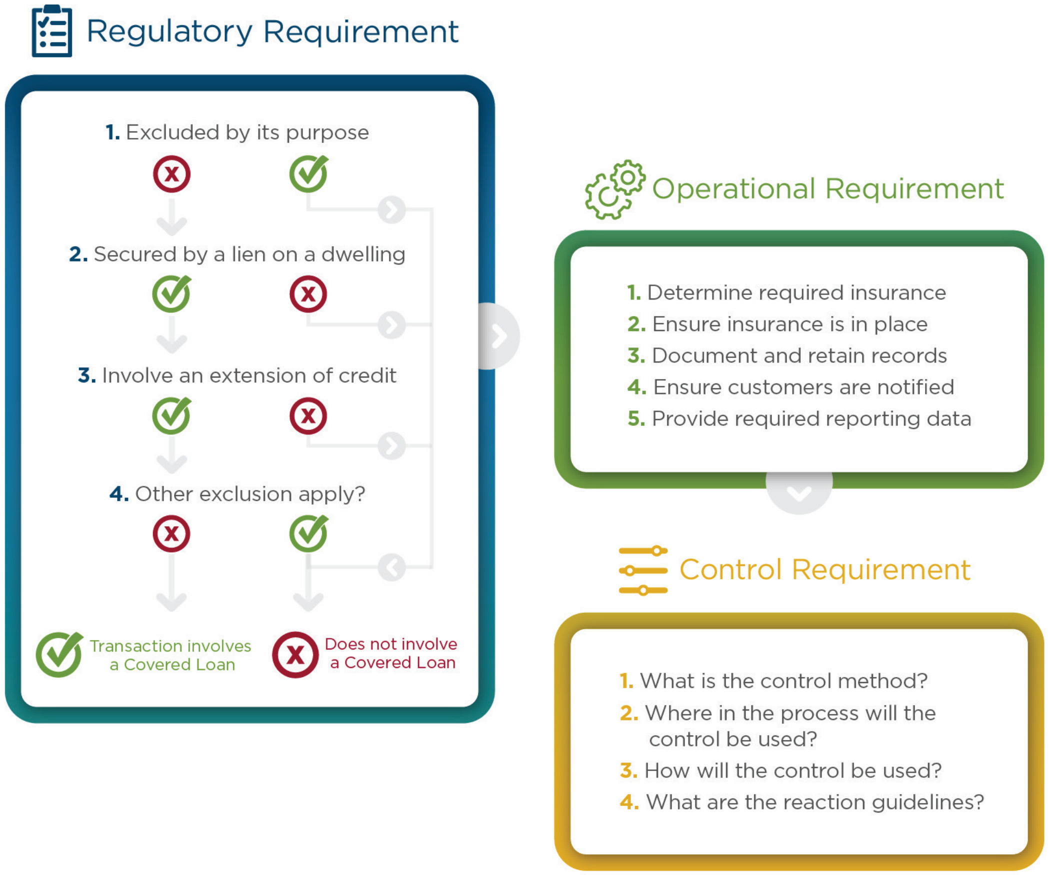
Once the QC team has been established and the key operational requirements have been identified, specific controls must be developed, embedded into the process and documented using a control plan. Full team involvement is critical so that everyone fully understands the background and requirements and has ownership for the controls.

EMBEDDING COMPLIANCE INTO OPERATIONAL PROCESSES

An organizational approach is necessary but not solely sufficient to achieve embedded compliance. Embedding compliance into the process design involves three key steps (Figure 4).

- Clearly defining the FI's position and interpretation of the regulations
- Translating the regulations into clear operational requirements
- Developing control plans that embed the operational requirements into the processes

FIGURE 4: Translating Regulatory Requirements into Operational and Control Requirements



Regulatory Requirement

1. Excluded by its purpose ☒ ✓
2. Secured by a lien on a dwelling ✓ ☒
3. Involve an extension of credit ✓ ☒
4. Other exclusion apply? ☒ ✓

✓ Transaction involves a Covered Loan

☒ Does not involve a Covered Loan

Operational Requirement

1. Determine required insurance
2. Ensure insurance is in place
3. Document and retain records
4. Ensure customers are notified
5. Provide required reporting data

Control Requirement

1. What is the control method?
2. Where in the process will the control be used?
3. How will the control be used?
4. What are the reaction guidelines?

Source: Cornerstone Advisors

How each regulation is defined will be informed by the FI's risk tolerance, which should be well documented and communicated. It is common to see FIs take the safest approach, and compliance with laws, rules and regulations is often viewed as a zero-tolerance activity. The customer experience isn't always given full consideration. Compliance leadership must be willing to challenge and cultivate creative ideas to ensure that the control methods achieve the desired risk outcome yet don't create a poor customer experience.

Once the regulation is clearly defined, specific operational requirements must be developed. The operational requirements must be reviewed to identify and rank what matters most. The time spent on each compliance demand must be prioritized according to the FI's highest sensitivities, biggest risks and impact in noncompliance.

The third step is where embedding occurs. Embedding compliance into processes is enabled by 1) the use of control plans, 2) the creation of strong controls and 3) automation of the controls.

EMBEDDING COMPLIANCE THROUGH THE USE OF CONTROL PLANS

Developing a control plan involves thinking through how each of the key operational requirements is going to be successfully achieved. During this development, the possible ways the requirements could fail to be met must be understood. Each opportunity for failure needs to have a countermeasure, or control, that will prevent the failure from occurring. The critical components of a robust control plan include the following:

- What is the operational requirement that must be met?
- What is the control method(s)? Is it preventative or detective? Is it manual or automated?
- What is the sample size and frequency of the control? (100 percent is preferred)
- What are the reaction guidelines and improvement activities?

The control plan provides the front-line team member with the information required to properly control the process and produce quality products and services. It should also include instructions regarding actions taken if a non-conformance is detected.

The control plan is not meant to be created and then filed away. It is meant to be a living document that is continuously updated by the QC team as new situations arise that cause defects. This is why forming QC teams is so critical. The core team members "own" the control plans and are expected to sustain the improvement activities while bringing in team support resources as needed.

THE IMPORTANCE OF STRONG CONTROLS

The challenge is to develop strong controls that don't rely solely on a set of eyes, or human inspection—especially if the process is customer-facing and delivered digitally via online or mobile technologies. According to Joseph Juran, a renowned quality expert, human visual inspection is actually only 87 percent effective. At that rate, the chance of achieving the desired quality levels will most likely come with undesirable operational costs as the result of trying to "inspect in" data quality.

DIGITALLY EMBEDDING COMPLIANCE THROUGH AUTOMATED CONTROLS

As the QC teams attempt to meet regulatory and operational requirements and work through the control plan, developing automated controls that don't rely on human inspection is a must. When it comes to steps performed by humans, inadvertent errors are both possible and inevitable. The strongest controls will be those that prevent compliance failures through the use of technology and automation. The keys to developing automated controls include:

- Ensuring the QC teams have support from resources who have an expertise in the digital delivery technologies being utilized

- Choosing digital technologies that can be configured to harness the creative problem-solving ideas from the QC teams and embed the desired automated controls

- Partnering with digital technology providers that offer solutions that support the desired controls

When creating strong automated controls, some key questions to ask include:

- Can "Go/No-Go" tests be configured and performed at the entry point of the data?
- Does the required data or supporting documentation exist when it's supposed to in the process?
- Does the data meet the operational requirements?
- Can logic be applied to test it?
- What happens if the test fails?

Controls are rarely perfect the first time they are implemented. This emphasizes the critical need to partner with the right technology solution providers that will enable the QC teams to make the necessary changes to the embedded controls. It is also critical for QC teams to continuously remain engaged to monitor and incrementally improve the controls.

THE BENEFITS OF EMBEDDED COMPLIANCE

As the demand for delivering financial products and services quickly and accurately through digital channels increases, FIs need to be thinking differently to remain competitive and provide solutions that work correctly the first time.

One senior manager said it best:

> *“If the digital process breaks, no one is there to assist and save the customer experience like there is in a branch. Each digital opportunity is critical to our success, and we have to get it right. We have to engineer a self-service process that just works. For us, there is often no second chance.”*

If applied correctly, embedding compliance can significantly reduce the need for adding layers of staffing to “inspect in” data quality. Rather, compliance is embedded, or “built in,” at both the organization and process levels. Compliance results will improve, costs will be lower, and perhaps the most important benefit of all, employees will be engaged and involved in the improvement efforts.

ABOUT
CORNERSTONE ADVISORS

Cornerstone's multidisciplinary team is backed by the experience that comes from hundreds of thousands of in-the-trenches client hours. We live by the philosophy that you can't improve what you don't measure. With laser-focus measurement, financial institutions can develop more meaningful business strategies, make smarter technology decisions, and strategically re-engineer processes.

Cornerstone Advisors takes financial institutions from strategy to execution through an array of Solutions offerings, including Strategy, Performance, Technology, Mergers & Acquisitions, Payments, Risk Management, System Selection & Implementation, and Delivery Channels.

Cornerstone publishes GonzoBanker, our blog; the Cornerstone Performance Report, a series of annual benchmarking studies; and a variety of research.

CONTINUE THE CONVERSATION

www.crnrstone.com
in Cornerstone Advisors
@CstoneAdvisors
☎ 480.423.2030

ABOUT
COMPLIANCE SYSTEMS

Compliance Systems is a best-in-class provider of financial transaction technology and expertise. With more than 25 years' experience with financial transaction data analysis and documentation, Compliance Systems currently supports content configuration and compliance risk management at more than 1,500 U.S. banks and credit unions. The Compliance Systems warranty covers all 50 states and the District of Columbia, giving clients confidence that documentation meets compliance and legal needs. Compliance Systems minimizes transaction risk and reduces resource expenditures so that institutions can focus on business development.

CONTINUE THE CONVERSATION

compliancesystems.com
in ComplianceSystems
@compliancesys

Have questions about this report?

CONTACT:

Ron Shevlin
Director of Research | Cornerstone Advisors

rshevlin@crnrstone.com
480.424.5849

CORNERSTONE
ADVISORS