BOARD OVERSIGHT + COMPLIANCE:

What Do Examiners Expect

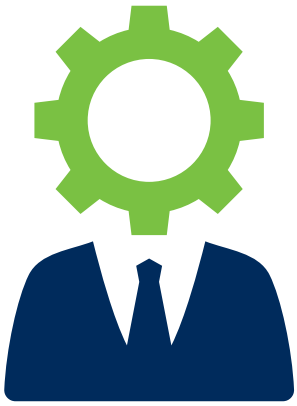
?

Continuity CONTROL

white paper 2

Board Oversight + Compliance: What Do Examiners Expect?

How does the board of directors enable compliance within your institution? It's a question that financial institutions are being asked more often by regulators and examiners, and one that's stumping many CEOs of community banks and credit unions.



Until recently, the board's role in regulatory compliance has been ill defined. Most boards, like many executives and compliance personnel, have viewed compliance as a checklist of activities executed in the lower levels of the organizational hierarchy. As a result, board oversight has been inconsistent and – in many cases – ineffective. CEOs also have lacked clarity around the board's role, leaving them unable to provide the direction required to ensure the right outcomes.

But, as the scope and risk associated with compliance have expanded, so has the board's role within this realm. Rather than inspect or ratify performance after the fact, the board of directors is now expected to be an active participant and enable real-time action on regulatory matters. The board's role is twofold – to be a "roof" that minimizes the institution's exposure to risk, as well as to provide the foundational underpinning upon which the compliance strategy is built. Most importantly, the board is tasked with setting the tone from the top and establishing a culture of compliance that permeates all facets of the institution.

It's important to note that strong board oversight is a team sport. In a **Compliance 2.0 world**, the regulatory burden is shared across the community financial institution with a series of checks and balances. Understanding the board's role in compliance and what constitutes effective oversight is just as much the responsibility of the CEO and compliance officer as it is the obligation of each director. Outside board members rely on the internal management team to keep them apprised of changes to the external threat-scape and to the bank's operating environment. Getting the right info to the directors at the right time is crucial to the exercise of their fiduciary duties.

Continuity CONTROL

Noses In, Fingers Out

As community banks evaluate their board oversight strategies, a common question emerges. Exactly how involved should the board be in compliance operations across the institution, and how much is too much? The answer can be summed up in a common saying used in the world of executive management: “noses in, fingers out.”

The board has a responsibility to be curious. It’s their job to repeatedly ask “why?” and “how?” in regards to what compliance activities are being performed and how they’re being executed, monitored, measured and assessed.

While curiosity should be unbridled, involvement in the day-to-day operations of compliance is discouraged and impractical. It’s impossible for the board to be involved in the execution of compliance activities and maintain the distance and independence required to review those same activities. Furthermore, the daily operations surrounding compliance have become too complex and intricate. It’s unreasonable to expect the board to have the required experience and expertise.

Remember:

Noses in: be curious.

Fingers out: don’t overly influence daily compliance operations!

Continuity CONTROL

white paper 4

Common Board Blunder: **Forgetting about third parties.**

More community banks and credit unions are outsourcing business activities to outside vendors. These vendors have a role in maintaining compliance, as evidenced by new vendor management requirements set forth by various regulatory agencies. Make sure your vendors are just as clear on compliance expectations and responsibilities as your internal staff.

What Are the Compliance Responsibilities of the Board?

The first step in redefining the board's role in compliance is to take a look at the collective job description. In the past, the description could have been summed up as simply making sure the institution had a compliance management program. Again, it was a checkbox approach. Today, the responsibilities are much more comprehensive and include the following:

- **Demonstrates clear compliance expectations to internal staff and third parties.** Compliance expectations need to be summarized and clearly stated in written form in a way that can be easily understood and communicated across the organization. The board must make sure these expectations are shared with third parties as well, including service providers, vendors, examiners and auditors. For some institutions, especially those with a vast network of vendors and third-party service providers, this may require a system that automatically notifies the bank's ecosystem on changes to compliance expectations and responsibilities.

- **Adopts clear policy statements.** Gone are the days when a couple of paragraphs stating the institution's intent for compliance suffice. Today's boards must take a more thorough and formulaic approach to policy statement documentation. At a minimum, these statements should cover why the policy exists, which management official is tasked with program oversight, the minimum standards to which the program will be held, and what controls are in place to make sure the policy is followed and periodically updated.

- **Appoints an effective compliance officer.** The compliance officer is a key pillar in a sound compliance management system (CMS). It's the root cause from which other successes and failures might stem, and it's up to the board to ensure a knowledgeable, experienced and capable person fulfills the role. Even more so, this person must be effective. Is he/she capable of keeping up with the changing regulatory environment? Does he/she provide the board with the right kinds of reporting and data that will enable the board to perform its job well?

Continuity CONTROL

- **Allocates appropriate resources.** The board may not be involved in day-to-day compliance operations, but they are absolutely required to allocate the right resources to carry out compliance obligations – whether it's people, funding, time or technologies. Examiners have become particularly interested in how boards are equipping banks with the resources to standardize and streamline activities. This has exposed a need for more compliance automation tools, which accomplish these goals and demonstrate effective oversight.

- **Ensures periodic reporting by the compliance officer.** The board is responsible for staying apprised of what compliance activities are happening at the institution. They should know if compliance obligations are being met and, if not, what needs to be done to achieve compliance. They need to understand what regulatory changes and compliance concerns are on the horizon and when and if they need to be mitigated. These discussions need to be prompted by consistent and regular reporting from the compliance officer. Some community financial institutions may require monthly reporting while others may do it quarterly. Regardless, the reporting needs to happen in a way that's formalized and predictable.

- **Ensures compliance audits.** The board is responsible for the selection and provision of audit services, whether through an internal audit program or a third party. This includes being an active participant in due diligence and vetting, ensuring the independence of the audit function, and thoroughly reviewing all audit reports and findings to ensure they cover criteria specified in the scope of work.

Common Board Blunder: **Building an army without an arsenal.**

There has been a notable increase in the number of enforcement actions stemming from boards' failures to allocate the right compliance resources. Even with the brightest compliance officer at the helm, an institution's state of compliance is only as good as the resources available to him or her. This includes people, time, budget and, specifically, tools and technologies that automate, standardize, simplify and provide visibility into compliance across the organization.

Continuity CONTROL

Examiner Expectations – What Are They?

The first step in maintaining proper board oversight of compliance is performing the duties listed above. The next step is performing them in such a way that meets examiners' expectations – a mystifying area for both the board and CEO of most community financial institutions. So, what will they be looking for?

No more rubber-stamping compliance programs. How many times has your institution's board approved a compliance program they didn't fully understand? Or, taken the word of the compliance officer that risks are being mitigated? For many community banks and credit unions, these are common occurrences. However, this type of "rubber-stamping" approach is no longer acceptable. Examiners want to see evidence of discussion and thoughtful consideration within board minutes that demonstrate:

- Approval of the **compliance management system** and programs
- Approval of significant policies (ones that require board approval)
- Consideration of staffing, compensation and budgetary needs of the CMS
- Evaluation of CMS effectiveness, including annual independent reviews (audits) and discussion thereof
- Review of assessments and risk monitoring

Remember – If it isn't documented, it didn't happen.

It's time to say goodbye to the rushed board meeting – especially when it comes to agenda items involving compliance. Take the time to have a thorough discussion and DOCUMENT it. Recent enforcement actions provide guidance:

1. Minutes should clearly reflect the discussion of and decisions made with respect to compliance.
2. Review and discussion of compliance reports should be a customary part of each monthly meeting.
3. Policy reviews and substantive discussion should be recorded.
4. Keep a chronology or chart of significant compliance-related board actions.

Continuity CONTROL

Ongoing compliance training for all board members. If boards are expected to stop rubber-stamping compliance initiatives, they must be more knowledgeable about the regulatory landscape as it relates to their institution. This is a challenge for many community banks and credit unions as their board members come from all backgrounds. By no means do examiners expect them to be compliance experts, but they do expect them to have the appropriate knowledge and skill set to carry out their fiduciary duties. The good news is board-level training is widely available, from online training and manuals published by different regulatory agencies to field workshops and seminars.

Implementation of a board oversight program that surrounds and contains risk. The very purpose of a board oversight program is to reduce, mitigate and control compliance risk across the institution. To that end, the board must demonstrate to examiners an oversight program that *identifies risks* posed by the bank or credit union's business operations, *monitors and measures risk exposures* as they change over time, and *controls risks to acceptable levels* commensurate with the risk appetite determined by the board. One of the most effective ways to accomplish this is through an automated compliance management solution that effectively demonstrates a systematic and consistent approach to finding, monitoring and controlling risk across the institution.

Common Board Blunder:
Compliance training is only for compliance professionals… right?

Think your compliance team is the only one that needs training? Think again. Board members should be actively engaged in ongoing compliance training. It's essential to preserving board oversight effectiveness and reducing risk in a rapidly changing regulatory landscape.

Does My Institution Need a Compliance Committee?

Compliance committees are viewed as a best practice, but are in fact optional unless they've been mandated by enforcement action. Some community bank boards form them as an added measure to reduce risk. Others use them as an alternative to a full-time compliance officer resource. If your board is considering forming a compliance committee, take a best practices approach:

- Representation should be interdepartmental.
- Committee must be focused on action and implementation – not just discussion.
- Ensure activities are monitor-driven and results-oriented. Demand regular documentation of results.

Continuity CONTROL

white paper 8

Defining Risk Tolerance and Exposure

In community banking, risk is unavoidable – especially when it comes to compliance. It's the board's responsibility to identify risk exposure as regulatory changes occur and make sure it's within acceptable tolerance levels.

5 Q's to Determine Acceptable Level of Risk

1. HOW much risk should we accept?
2. WHY are we required to (or have decided to) accept this risk in our institution?
3. WHAT risks should we eliminate or transfer to third parties?
4. HOW do we mitigate the impact of the risk we're accepting?
5. WHO is responsible for managing it?

5 Q's to Determine Risk Exposure

1. WHY was this rule adopted? Understanding the rationale can help you determine how your institution is affected.
2. HOW does this rule affect our institution? Knowing which products and people are affected and whether system upgrades may be required is a critical first step toward implementation.
3. WHAT challenges are associated with implementation? The harder a change is to implement, the greater the risk of noncompliance.
4. HOW MUCH is the estimated cost of compliance? Will more training, new systems, new forms, etc., be required?
5. WHAT is management's plan for implementing and monitoring compliance? The better the plan, the lower the risk that key steps will be overlooked or mistakes made.

what why how much how up

Understanding of regulatory changes, enforcement actions and the institution's unique compliance burden. The compliance burden of each institution differs, as do the impacts that regulatory changes have on the organization. Examiners expect the board of directors to have a firm grasp of how changes in the regulatory landscape – including updates, new rules and enforcement actions – are impacting the state of compliance within the institution. This, of course, is easier said than done. According to Continuity Control's **Banking Compliance Index™**, the average page count for regulatory changes issued each quarter can be anywhere from 2,000 to more than 5,000. In the first half of 2014 alone, there were 141 regulatory updates.

Meanwhile, enforcement actions are on the rise, with 335 issued in the first half of 2014. Themes common to the actions included:

- Citing "unsafe or unsound banking practices" committed in the area of consumer protection and compliance.
- Requiring disclosure of the enforcement action to all shareholders.
- Shortening timeframe for resolution of the compliance issue to 90 days or less, with periodic progress reports to the regulator.
- Requiring formation of a compliance committee and/or hiring of an independent outside consultant.

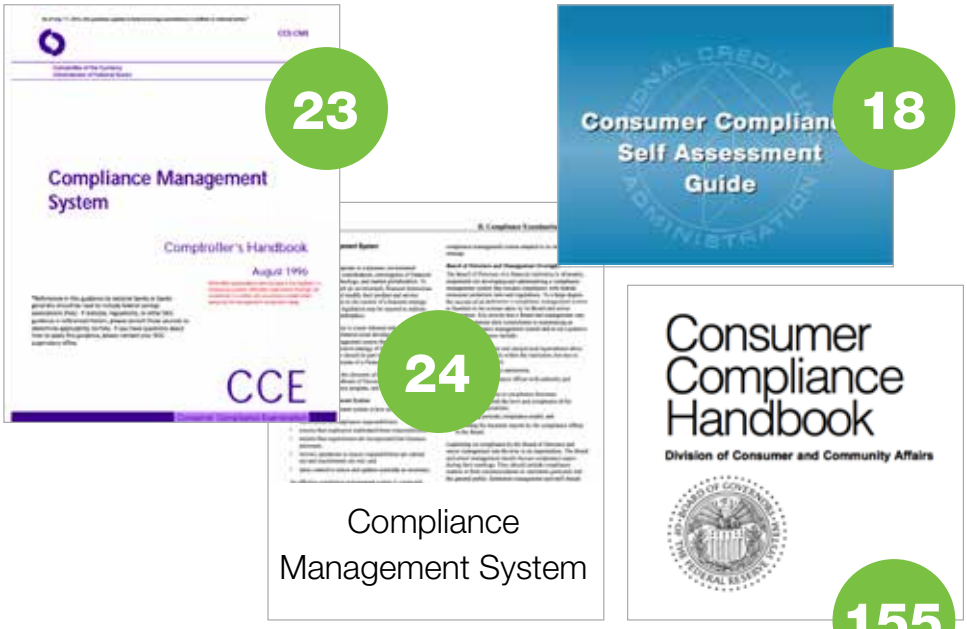
This again has illustrated a need for a more formulaic, institution-specific and automated approach to the way compliance is being managed at the board level and beyond. Being able to quickly and easily understand the impact of regulatory changes across the institution is not just a sound business practice, but demonstrates a systematic approach to compliance that examiners seek.

Common Board Blunder: **Failure to validate remediation.**

Boards of directors may not be responsible for fixing compliance issues, but they are responsible for confirming effective, lasting action has been taken and the loop has been closed. After a fix is implemented, testing must occur to prove that the fix "stuck" and was effective at correcting the identified weakness. A best practice is to allow 90 days between remediation and validation testing. As with other board actions, maintain evidence of the board's review of validation results!

Finally, it's important to note that the role of the board of directors – and their influence on the institution's compliance management system – has been elevated in various handbooks, examination manuals and self-assessment guides issued by the regulatory bodies. A quick survey of four such documents revealed that the term "board of directors" is mentioned 220 times.

Examiner Expectations



number of times "Board of Directors" is mentioned

Proper execution of corrective action after audits or examinations. The board is responsible for ensuring audits identify the root causes of weaknesses and make sound remediation recommendations. Examiners also want to see that the board has granted officers sufficient authority and resources to execute corrections, and that appropriate follow-up is being conducted to make sure actions have been effective and lasting. To meet these expectations, the board may need to prove that responsibility has been assigned and action deadlines established. The board also needs to ensure that periodic status reports are being provided while progress is underway, and that solid quality control measures have been put into place to prevent problems from recurring.

Continuity CONTROL

Conclusion

Regulatory compliance as we know it has been upended in the last decade. No facet of the banking organization has been left untouched by the sweeping changes that have occurred. The role of compliance officer has emerged as a key business enabler, and has been elevated to the highest ranks of the institution. Chief executives are no longer removed from the compliance function, but fully entrenched. The third role in the compliance management triad– the board of directors – is also undergoing a transformation, from rubber-stamping checkbox-style compliance to providing relevant oversight and guidance on the institution's risk appetites and exposures.

So, how do boards meet the numerous and formidable expectations that examiners have set before them? As non-compliance professionals, how do they ensure that compliance risk is in line with tolerance, and that the compliance management system is effective? Finally, how do CEOs ensure proper, effective board oversight?

For many, the answer is automation. From interpretation of new regulations to delegation of tasks to monitoring and reporting, automated compliance management systems deliver consistency, centralization and visibility – benefits that are just as fully realized at the board level as they are by compliance professionals.

white paper

See an online tour of Continuity Control.

Sign up for an introductory demo and see why hundreds of community financial institutions use Continuity Control to reduce the impact (time, cost and risk) of regulatory compliance. Register at **www.continuity.net/rethink**.

(re)think
Regulatory Compliance

Continuity CONTROL

www.continuity.net

ICBA Preferred Service Provider®

ABOUT CONTINUITY CONTROL

The Continuity Control 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 Control is the exclusive ICBA Preferred Service Provider for a Compliance Management System. For more information visit **www.continuity.net**.