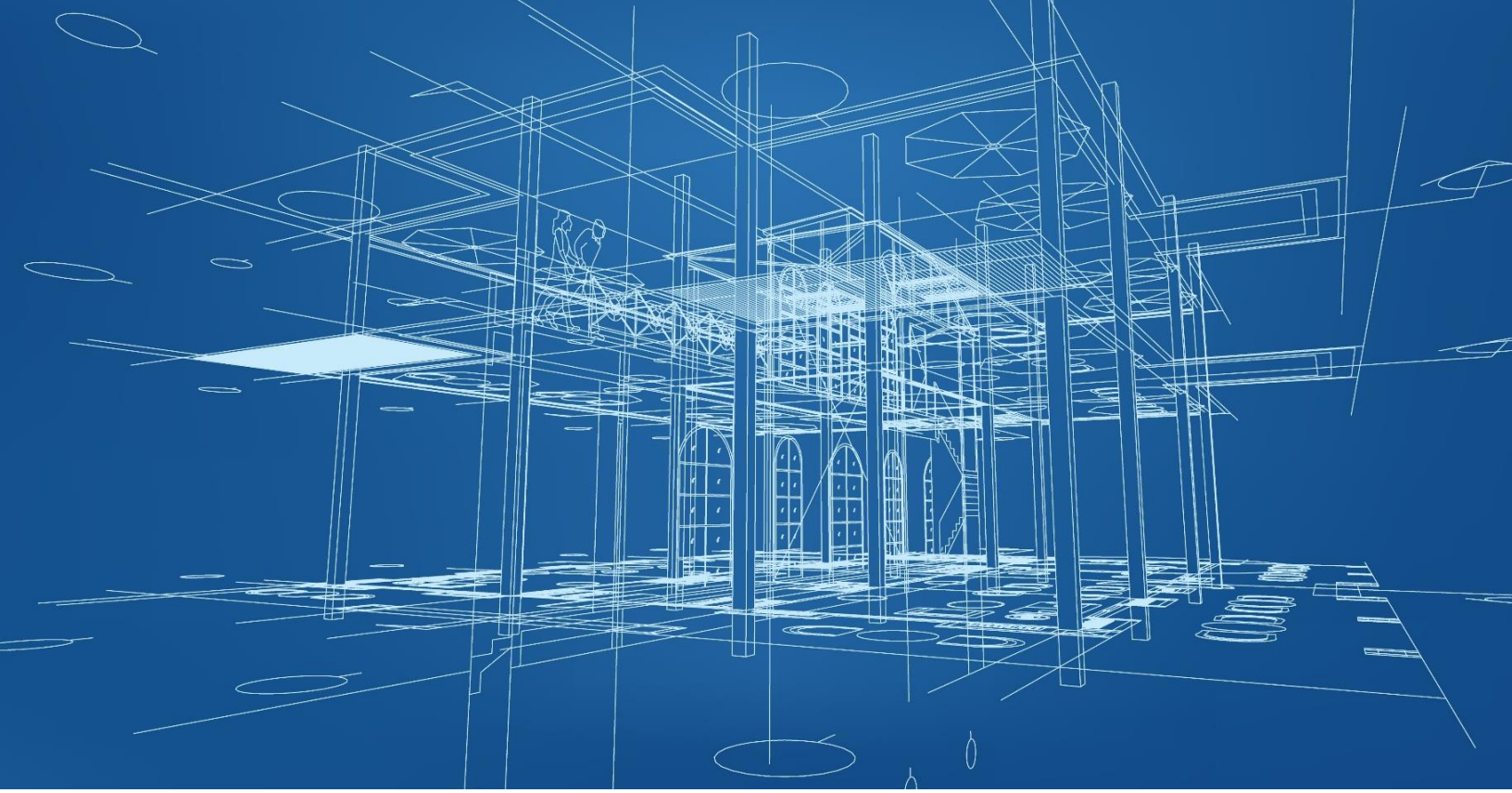
CrossCheckCompliance

Building Your Defenses: Compliance Management for First-Line Operations

Contents



Introduction

At some point in your career as a bank compliance professional, you have probably heard comments like "compliance is the compliance officer's job." However, as more focus has been placed on the bank's compliance program and regulatory burden has increased over time, a common question is *"who owns the compliance risk?"* Is it the business line? The compliance department? Bank leadership? As regulators expect a more proactive approach to compliance with consumer protection regulations, the answer to "Who owns the compliance risk?" is "Everyone" because risk is created throughout the bank. Even a fully resourced compliance department may not have the capacity to monitor all regulations and all products and services on a regular basis. This can lead to significant periods of time before a control weakness is identified, which may create substantial risk for the bank. Because of this, many banks have moved to a three lines of defense (3LOD) model even if they are not yet required to because of their asset size.[1] Under the 3LOD model, the first line (1LOD) comprises the frontline and back-office operational groups that sell and service the bank's products. The 1LOD is responsible for developing and maintaining an effective compliance management system (CMS) for the business line. An established 1LOD CMS is better able to proactively identify, monitor, and control risk more effectively on a real-time basis because first-line staff have firsthand knowledge of the products, personnel, systems, and potential risks in their departments. Whether you are in the process of building out a 1LOD, or just starting to make the case for one to management, this white paper provides the construction materials you need.

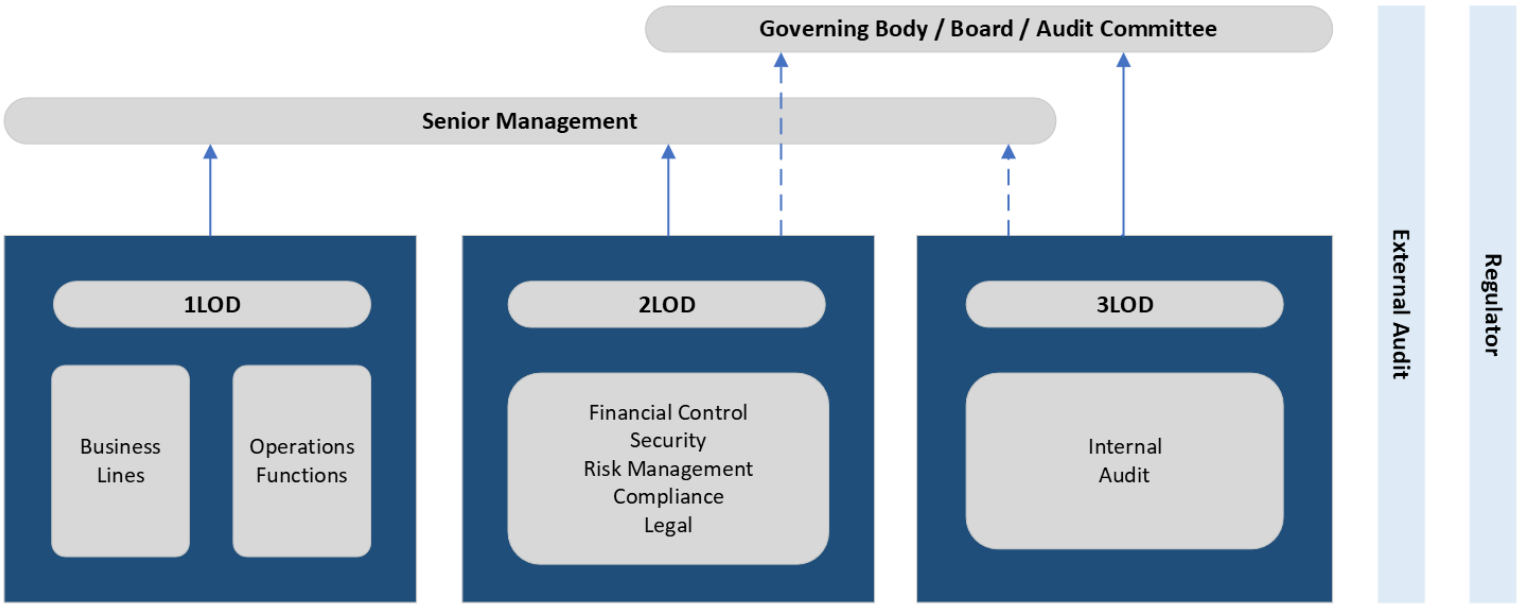
TRACEY LEVANDOSKI, CRCM

Managing Director – Regulatory Compliance, Internal Audit & Fair Lending

[1] The regulatory agencies have established heightened standards for designing and implementing a 3LOD risk governance framework, which includes compliance risk, covering banks with assets of $50 billion or more.

©2023 CrossCheck Compliance LLC. All Rights Reserved

The Three Lines of Defense (LOD) Model



Drafting the Floor Plan – Establishing the 1LOD CMS

We have already established that compliance is everyone's job. The regulatory agencies are focusing more on the design and effectiveness of the overall CMS. Having a 1LOD staffed with knowledgeable people who have a comprehensive understanding of the control environment and the risk in the products and services of the business line is essential as the bank prepares for growth. A 1LOD CMS contributes to a more effective risk management framework and allows for quicker or real-time identification of compliance issues that can be resolved before they create widespread consumer harm, which in turn helps to effectively mitigate compliance risk to the bank as a whole.

As with any significant operational change, implementing a 1LOD will include challenges such as resistance from the business lines which may not want what they perceive as added compliance responsibility. Compliance responsibility has always been with the 1LOD, those responsible for sales and servicing execution and customer service. However, the historical approach to managing compliance risk may have been reactive; waiting for issues to be identified through examinations and audits. Business line management may not see the benefit of establishing the 1LOD. These challenges can be offset with a robust compliance culture set by the tone at various levels of management and that includes both 1) clear communication of expectations and 2) support to resolve issues such as a lack of resources or resources that lack the requisite expertise.

If you are just starting to make a case to bank leadership to gain the support needed for a 1LOD, consider the benefits the function brings:

- Reinforces compliance culture within the business lines and places the responsibility for compliance where compliance risk is created.
- Provides faster, or real-time feedback on compliance issues and exemplifies a more proactive approach. For example, compliance monitoring imbedded in the first line will accelerate the identification of weak or failed controls and if promptly and properly addressed will prevent issues from occurring over long periods of time. It would also reduce the time and costs of any associated remediation. Timely identification of compliance risk provides management with more insight into the overall risk level of a department.
- Increases compliance expertise across the bank – Line staff responsible for implementing the CMS 1LOD will develop in-depth compliance knowledge. Therefore, in addition to executing day-to-day activities in a compliant manner, line expertise can benefit the compliance department's succession planning.
- Allows the Compliance Department to serve as a true second line of defense (2LOD) – By relying on 1LOD activities, 2LOD resources could focus on areas such as:

©2023 CrossCheck Compliance LLC. All Rights Reserved

- Providing a higher level of compliance risk management coordination across the bank;
- 'Checking the checker' by auditing the first line quality assurance and quality control functions to validate first line results; and
- Providing compliance guidance to the business lines.

- Demonstrates a commitment to compliance – Having an established 1LOD CMS demonstrates to examiners and auditors that the bank has a strong commitment to consumer protection and compliance which contributes to a more effective compliance program.

Laying the Foundation – Compliance Program Elements and Regulatory Applicability

Just as the bank's overall CMS program should be documented, the 1LOD's CMS should include a compliance management policy that serves as the governance document that defines the responsibilities tailored to each business line/operations function. The compliance management policy outlines the key components of the 1LOD CMS such as:

- Compliance policy statement, which should mirror the bank-wide compliance policy;
- General program scope and definitions;
- Roles and responsibilities including a high-level description of each of the business line positions involved in the CMS;
- CMS program elements including as applicable: oversight, policies and procedures, risk assessment, monitoring and corrective action, complaint response, training, vendor management, and change management;
- References to related policies, programs, procedures, and guidance;
- Applicable laws, regulations, and interagency guidance impacting the business line/operations function.

The 1LOD compliance management policy should be reviewed annually to align with the annual review and approval of the bank-wide compliance policy.

As with any area of the bank, robust procedures are the backbone of operations and support the compliance management policy. CMS procedures should:

- **Further define roles and responsibilities** – Be as detailed as necessary to capture everyone's contribution by naming each role in the department, such as department manager(s), frontline staff, any imbedded quality control functions, and other operational positions, and defining what aspects of compliance each role covers.
- **Define the monitoring objectives, frequencies, and sampling methodology** – Coordinate with the bank's overarching risk methodology for assessing risk and determining monitoring frequency. Sampling methodology should include whether statistical or judgmental sampling will be deployed and thresholds that would require increased sample sizes.
- **Outline corrective action and issue tracking** – The procedures should address the bank's approach to root cause analysis, corrective action, and issue tracking. This is another area where consistency with the 2LOD procedures would be beneficial as there may already be a centralized issue tracking system in place that monitors all corrective actions in process across the bank for appropriate and timely resolution.
- **Define reporting requirements and timelines** – Results of monitoring activities should be documented and promptly addressed. The CMS procedures should cover who should receive monitoring results and the expectations for timely reporting and content. A best practice is to develop a standard reporting template that mirrors the 2LOD reporting template to promote consistency across the bank.
- **Address change management and third-party vendor management** – The business line's change management procedures should mirror the bank's change management program and define who is responsible for change management oversight at the business line level. And do not forget that if

©2023 CrossCheck Compliance LLC. All Rights Reserved

vendor management is included in the responsibilities of the business line, that should also be addressed in the CMS procedures.

- **Address complaint management** – Complaint management at the business line level should be clearly defined in relation to any centralized complaint management process including who is responsible for tracking, root cause analysis, corrective action, and reporting, as applicable.

Before building the individual elements outlined in the compliance program policy and procedures, the bank's compliance officer may need to assist the business line in determining which regulations are applicable to its operations, identifying the controls already in place and potential control gaps. For this part of the foundation, the 1LOD CMS should include the development of a regulatory applicability matrix (RAM) and a control assessment tool (CAT).

As its title implies, the RAM lists regulations that apply to the business line's operations and all the products and services it offers. (See Figure 1 for an example.)

After the applicable regulations are identified in the RAM, the next step is to complete the CAT. (See Figure 2 for an example.) The CAT serves to further segment the applicable regulations into the individual requirements that apply to the business line's products, services, and operations. Controls can then be identified for each requirement along with any control gaps or weaknesses. Taking the time to be as detailed as possible with the CAT is critical as it lays the foundation for the compliance risk assessment and the monitoring/testing program. To illustrate, let us consider the consumer closed-end mortgage origination business line and Regulation Z requirements applicable to issuance of the Loan Estimate (LE). While Regulation Z covers a lot of territory (open-end credit, student loans, credit cards, reverse mortgages, consumer loans not secured by real estate, etc.), you will want to narrow the scope for the mortgage business line. The regulatory requirement could be a statement as simple as 'All information on the LE must be accurate based on the best information reasonably available at the time the LE is issued.' Or you might even want to further break that down into the individual elements of the LE depending on how and where you obtain the information to complete it.

Regardless of how you decide to structure the regulatory requirements on the CAT, the next step is to help the business line identify the controls in place for each requirement and assess their effectiveness. Continuing with the LE example, the control might be that all LEs are reviewed by the quality assurance specialist (which is a role that should be identified in the compliance program policy and procedures) before they are issued to the applicants.

Figure 1.

REGULATORY APPLICABILITY MATRIX (RAM) EXAMPLE

Regulation/Law	Citation	Consumer Lending Department				
		Consumer Loans	Home Equity Loans	Credit Cards	Direct Auto Loans	Indirect Auto Loans
Regulation B	12CFR1002	X	X	X	X	X
Regulation …	12CFRXXXX		X		X	

Figure 2.

CONTROL ASSESSMENT TOOL (CAT) EXAMPLE

Product	Regulation Citation	Requirement	Control in Place	Control Gap/ Weakness

©2023 CrossCheck Compliance LLC. All Rights Reserved

TIP: Do not forget to formalize and document the existing framework. The business lines likely already have quality assurance and quality control reviews in place such as second reviews of deposit hold notices and adverse action notices, data integrity reviews for data collected and reported as required by the Home Mortgage Disclosure Act (HMDA) or the Community Reinvestment Act (CRA), flood insurance monitoring, loan disclosure reviews before closing packages are issued, etc. First line staff may engage in these activities as a normal part of their duties and not consider them as compliance functions; be sure to capture them in the CAT.

In some cases, this exercise will also assist the business line in identifying any control gaps or weaknesses that need to be addressed. For instance, if the only control for the LE example is that loan processors are trained annually on accurate completion of the LE, that might be a weakness in the control environment depending on the expertise of your processors and whether you experience turnover in the position. The identification of such weaknesses, or gaps where no control exists at all, should be addressed in the business line's compliance risk assessment, and serve as an opportunity for improvement in your 1LOD CMS.

Completing Construction – Risk Assessment, Compliance Monitoring, and Training

After the foundation of the 1LOD CMS has been established with the policy, procedures, RAM, and CAT, the next building block is the compliance risk assessment. While compliance officers can create risk assessments with their eyes closed, this is most likely unfamiliar territory for business line personnel, and special attention and assistance may be warranted here. There are numerous methodologies and risk rating systems available for consideration; however, the bank's established risk assessment methodology should be the basis for the 1LOD CMS, and the methodology should be defined in the 1LOD policy and procedures. Controls and control gaps/weaknesses identified in the CAT should play a significant role in establishing the business line's compliance risk assessment, which in turn should be considered in the bank-wide compliance risk assessment.

Potential challenges for business line personnel tasked with creating and maintaining the 1LOD risk assessment include:

- Understanding the difference between inherent and residual risk – An analogy to a car crash may be useful to help make the distinction. Think of the inherent risk as the risk of significant bodily harm if there are no safety features built into the car. The residual risk is what remains after the safety features (or internal controls) have been installed, i.e., anti-lock brakes, airbags, seat belts, etc.
- Identifying control weaknesses – Business line staff may be hesitant to point out their own weaknesses. Ease their concerns by assuring them that: a) they are in the best position to know where gaps exist, and b) the main purpose of a risk assessment is to

identify weaknesses so they can be addressed with appropriate corrective measures.

After the risk assessment is completed, use it to drive the business line's monitoring and reporting program. Monitoring frequencies should be based on the risk assessment results; depending on the area being tested, a high-risk rating could require monthly testing. Moderate risk areas may be tested quarterly or semi-annually, and low risk areas may be tested annually or less often. Again, assigned testing frequencies should complement the overall corporate methodology. Create a testing calendar to keep everything and everyone on track.

After you have decided what areas you will test, and when, the next consideration is how to test. Using standardized monitoring tools is a best practice, and there are software programs available for this purpose. However, you will want to ensure they are specifically tailored to the business line's operations. Another useful resource is the regulators' exam procedures, but again, they need to be tailored to the business line's products and services as identified in the RAM.

The next consideration for the 1LOD CMS is how to report testing results. Standardized reporting formats should be developed that mirror the 2LOD's format. Some items to consider for inclusion in the reporting template are:

- Scope of the review including the area and period covered;
- Overview of the procedures used to complete the testing;
- Number of transactions tested;
- Number of errors or exceptions and the details of those exceptions;
- Root cause analysis. It is best to treat the true cause of an issue rather than the symptoms;
- Results of the prior testing for the area including review of any required corrective action to validate that it was implemented effectively. There is nothing worse than repeat findings;
- Recommendations for corrective action along with the person responsible for implementation and a due date for completion.

To follow up on corrective action, all issues identified should be tracked through resolution on an issue tracking log or system. An important control is periodic reporting of any open items so that outstanding issues do not become stale and eventually forgotten. Repeat issues are cause for concern as they may indicate the root cause was wrong and therefore the implemented solution was inadequate, implementation was not effective, or reinforcement was lax.

The final building block of the 1LOD CMS is the compliance training program. First line personnel should receive training that is specific to job responsibilities and supplements the more general compliance training required as part of the bank-wide curriculum. Depending on the circumstances, training may be a necessary corrective action resulting from monitoring and testing activities or to close gaps identified in the CAT and risk assessment. Training should also be completed proactively as part of an effective change management program. First line compliance staff may also want to consider providing customized compliance training tailored to the job responsibilities of new employees as they are brought on board. As compliance officers know, if it is not documented, it did not happen. Just as bank compliance staff maintain training logs and details of the training course content, business line compliance staff should do the same, ideally in a similar format that can be easily integrated into the bank-wide training record.

TIP: Do not forget to maintain records of informal training sessions such as 'huddles.' These sessions are just as important as formal training events, and the information conveyed may be better retained by business line staff – sometimes less is more.

Handing over the Keys and Moving In

It may be a lot of work to gain 'buy-in' from business line staff as the 1LOD CMS concept is introduced, but a successfully implemented 1LOD CMS will significantly improve the bank's overall compliance program over time. With the right tone at the top and the assistance and reassurance of the 2LOD, more reliance can be placed on the 1LOD's compliance activities as the CMS matures. The ultimate results include a better informed, more compliant first line, a second line that serves as more of an advisory role, and positive compliance examination and internal audit outcomes.

©2023 CrossCheck Compliance LLC. All Rights Reserved

ABOUT THE AUTHOR

Tracey Levandoski, CRCM, is a managing director at CrossCheck Compliance LLC, and a regulatory compliance and risk management professional with over 30 years of experience in the financial services industry. Having worked as both a prudential regulator and in banking institutions, Tracey has demonstrated expertise in compliance, including extensive knowledge of lending and deposit regulations with a recent concentration on fintech lending. She is also experienced in financial institution accounting and operations. Tracey can be reached at tlevandoski@crosscheckcompliance.com.

©2023 CrossCheck Compliance LLC. All Rights Reserved