SMARTER risk management

Regulatory Compliance in Community Bank:

An Exercise in Risk Management

By:

Kelly Lutinski, National Director

KellyLutinski@smarterriskmanagement.com

www.smarterriskmanagement.com

Executive Takeaways

- Compliance is an important component of the Enterprise Risk Management (ERM) function.
- The regulators have required the board of directors and executive management to have much greater involvement in compliance management.
- Compliance should be a formal program with:
  - Active support from the board and executive management,
  - Defined roles and responsibilities, and
  - A compliance dashboard to formalize and track ownership and compliance risks across the organization.
- Compliance is a business unit function that requires active support from the organization's compliance function.
- The compliance function is not a part of Internal Audit working for the board of directors but is intended to assist bank management in maintaining compliant activities throughout the organization.

A Brief History of Compliance

The role of regulatory compliance in financial institutions has changed dramatically over the last thirty years. Remember back in the 1980s? Regulatory compliance was viewed as an operational function that was owned deep within the confines of the organization. The success of the function was viewed by the executive management team and board as a "check the box" activity, only hearing about compliance when something failed. So when regulatory compliance issues bubbled up, there was a lot of reactive education and training required to familiarize executives about the regulation's purpose and the processes the financial institution was using to comply.

Beginning in the 1990s, bank regulators started requiring financial organizations to have formal Compliance Management Systems where board and management were expected to get much more involved in regulatory compliance. They were mandated to make compliance a high priority, recognize the scope and implications of laws and regulations that apply to their bank, have senior management help develop and maintain the compliance program, and review the effectiveness of their compliance program.

Since the end of the 20th century, board and management's involvement in regulatory compliance has only become more pronounced given the significant cost of non-compliance and the increased complexity and volume of regulations – like Gramm-Leech-Bliley (GLBA), the Patriot Act, changes to Fair Lending, UDAAP, Dodd Frank and the Consumer Financial Protection Bureau's expansive list. Banks now have Chief Compliance Officers who are tasked with overseeing all regulatory compliance and communicating with the board on a regular basis.

Given these significant changes to both content and approach, has your organization changed with the times to continue to support an effective Compliance Management System? Through discussions with many financial services executives and seeing first-hand how organizations manage compliance, we have observed that many community banks and credit unions have made a handful of minor changes to their compliance function, but have not made the meaningful changes necessary to effectively manage (as a program) the new role of regulatory compliance in the 21st Century.

The role of the compliance function in financial institutions needs to change. Whether you call it Compliance Management, a Compliance Office, or just plain old Compliance, the role and management of regulatory compliance in community banks and credit unions needs to be rewritten. The compliance function needs to be transparent in the organization in order to effectively manage the changing regulatory landscape. It must be embedded in the culture of the organization and owned by the individuals performing the work. Compliance should not be seen as an operational or audit function, but as an organizational process necessary to provide reasonable assistance and assurance so that institution's strategic objectives will be achieved. The role of compliance management is a critical component of risk management.

The Compliance Function: Protagonist or Antagonist

In some organizations, the compliance function continues to be seen as the bad guy – the antagonist who inhibits the organization from being successful because of "their" rules. Management continues to view compliance as a necessary evil and buries it in the organization where the function has no authority, or it is managed like an audit function where all findings are reported to the Audit Committee. In some organizations, compliance is staffed by individuals who had "time available" though they had only rudimentary training on regulatory compliance and banking. While these approaches may have worked in the past, there is a much more effective and opportunistic way to manage compliance that will add value to the organization.

Instead of being viewed as the antagonist, compliance should be viewed as the protagonist. (Merriam-Webster defines a protagonist as "a leader, promoter or supporter of a cause"). As the protagonist, the compliance function would have the following characteristics:

- A consistent and continuous process designed to manage compliance risks.
- Available across the entire organization as a partner and advocate to the business lines in identifying, understanding, and managing compliance risks.
- A resource to management and the business lines as they implement their strategic objectives.
- An authority on compliance risk but not the owner of compliance risk.

Using this approach, the compliance function becomes a leader and educator of compliance risk within the organization. Communication between the board, management, and the business lines becomes more transparent since compliance is seen as a partner who can help manage compliance risks in the organization and not the adversary inhibiting the organization from achieving its objectives.

The Risk of Weak (Compliance) Governance

"Governance is not a fixed set of guidelines and procedures; rather, it is an ongoing process by which the choices and decisions of [Financial Institutions] are scrutinized, management and oversight are strengthened and streamlined, appropriate cultures are established and reinforced, and FI leaders are supported and assessed." A lack of effective corporate governance has been seen as one of the big reasons for the economic collapse as well as many of the financial institution scandals that have occurred during the first eight months of 2012.

Governance is much bigger than just compliance but in order to evaluate an organization's approach to compliance governance, financial organizations need to critically assess how the compliance function and overall compliance with regulations is regarded. While the importance of compliance might be preached at the top levels of an organization, what is more important is how the board and management support the compliance function when issues or concerns arise. The key to good governance is not talking the talk but the success in walking the walk – or as Benjamin Franklin said "well done is better than well said."

Management and the board need to promote and foster the understanding that regulatory compliance is critical to the success of the organization and it is everyone's responsibility. Compliance needs to be held in high esteem where their opinion is listened to and respected; they need to be treated as a team member in decision making and issue escalation; they are no better or worse than any other member of the team and need to be treated as such. As mentioned earlier, this is not the role they have played in many financial institutions.

Clearly Defining Roles and Responsibilities

Once the executive management team and board have started “walking the walk”, it is important to define the compliance function’s roles and responsibilities in order for everyone in the organization to have a clear understanding of who does what and who is responsible for what, as it relates to regulatory compliance.

Compliance’s role is to oversee and manage regulatory compliance within an organization. The primary responsibility for this important role is given to a Compliance Officer (or Chief Compliance Officer). The role of the compliance officer is broad. The FDIC Compliance Manual describes a compliance officer’s role to include:

- Developing compliance policies and procedures.
- Training management and employees in consumer protection laws and regulations.
- Reviewing policies and procedures for compliance with applicable laws and regulations and the institution’s stated policies and procedures
- Assessing emerging issues or potential liabilities.
- Coordinating responses to consumer complaints.
- Reporting compliance activities and audit/review findings to the board.
- Ensuring corrective actions.

This is an overwhelming job that cannot be accomplished in an office with the door closed. The link between operations, compliance and product knowledge is so embedded in the individual business lines that the ability for a compliance officer to successfully execute compliance related policies and procedures without that knowledge is unrealistic and inefficient.

In order to increase efficiencies in the organization and properly carry out regulatory compliance in financial organizations, the compliance function needs to take on a leadership and support role. The business lines should be responsible for ensuring and owning compliance with regulations within their product lines. More importantly, instead of having the business lines focus on creating controls for each regulation, they should look at a specific activity (e.g., loan origination, sending wires), identify the regulations involved in that activity, and integrate controls for each regulation into their policies and procedures. These last two sentences describe a new approach to regulatory compliance for many organizations and one that we have implemented successfully.

One of the primary reasons this approach works is that there is a very clear understanding of who is responsible for what. Without the understanding and support of management and the board (i.e., the governance piece), the responsibilities for compliance tend to fall back to the compliance function which, for reasons mentioned earlier, is an impossible job for anyone to be successful and is grossly inefficient. This new approach also focuses more on the activity being performed instead of a specific regulation which is easier for the business line to understand, implement, and comply.

The following outlines some of the responsibilities for the compliance function and the business lines. (The board and management's responsibilities are not addressed here, as they were addressed in the Governance section earlier in this document).

Compliance Responsibilities	**Compliance Function**	**Business Line**
Stays current on regulatory issues / changes and communicates when appropriate.	☑	
Researches compliance questions / issues.	☑	
Trains and educates.	☑	
Ensures new or changing requirements are incorporated into business processes including all materials (e.g., policies, procedures, documents).		☑
Takes corrective action and updates materials as necessary.		☑
Performs on-going monitoring.	☑	
Owns compliance with regulations.		☑
Responds to consumer complaints.		☑

As you can see, the responsibilities are never shared between the two as sharing creates confusion and, ultimately, lack of ownership. The compliance function is an expert in regulations and is there to work with the business lines to make sure they understand the regulations and are applying them correctly. The compliance function relies on the business line for their expertise on the products and services offered. The business lines rely on compliance for their understanding of the regulations. The importance of having strong communication between these functions cannot be underrated. The only way an organization can be successful with compliance management is to have everyone working together and understanding their roles and responsibilities. The risks associated with not getting this right are extremely high.

Redefining the Compliance Management Approach

Remember when you were in fifth grade and were just learning multiplication and division? The teacher always told you to show your work. There was a reason for that – it helped the teacher recognize if you truly understood what was being asked of you. It also became an artifact that could be used in discussions on the approach you took and where you might have gone wrong in your analysis. Many teachers gave extra points for showing your work.

The approach described further formalizes a major component of the compliance program – the need to understand all of the laws and regulations that apply to the organization's business operations, and how an organization should prioritize their compliance monitoring. (Other components not specifically discussed include, but are not limited to, the Compliance Policy, BSA Risk Assessment, and training). This approach is completed using a compliance dashboard and encourages the "show your work" motto and simplify what many organizations feel is a very complex and onerous process.

The approach of the compliance dashboard is as follows:

- The business lines:
  - Identify their compliance activities and the regulations associated with them,
  - Document the controls and expected results using SMARTER charts, and
  - Rate their internal department using risk attributes (e.g., changes in staff).
- The compliance officer rates the regulations applicable to the organization.
- The end result provides an intersection of high risk compliance activities that need to be monitored closely due to their attention by the regulators, the significant penalties for non-compliance and/or the changes taking place in the business line.

In order to implement the compliance dashboard, there are five different modules that must be completed. These modules are designed to be very intuitive with no need to learn a new software package. It is recommended the modules be updated at least quarterly.

Module I: Compliance Activities and Regulations

Many organizations find it difficult to understand what regulations they must comply with across an organization. Instead of focusing on individual regulations, this approach has the business line document all of the different activities they are involved in, and then identify all of the regulations the business line must comply with as they perform those activities. (Compliance is intimately involved in this activity working with the business lines to ensure they have all of the regulations identified). From this, the organization has a much better (and documented) understanding of the activities that create compliance risk for the organization. The benefit? – business lines understand and can identify activities. They have a much more difficult time understanding a specific regulation and determining what activities are impacted by that regulation.

Module I

SMARTER CHART	Risk Activity / Business Process	FILTER ON: Risk Owner	Completed SMARTER Chart	# of Regulation Impacted by Risk Activity	Right to Financial Privacy	Safeguarding Customer Information - GLBA/Outsourcing	Identity Theft	CIP/USA PATRIOT Act	BSA/AML/KYC	OFAC	SAR	Truth in Savings Act - Reg DD	Reg CC	Electronic Funds Transfer Act	Truth in Lending Act - Reg Z	Flood Insurance	Home Mortgage Disclosure Act
1	Originating Consumer Loans	Smith	Jones	2						x					x		
2	Real Estate Foreclosure Processing	Smith	Jones	4				x	x	x	x						
3	Sending Declination Notices	Smith	Jones	0													
4	Identifying HMDA Reportable Loans	Smith	Jones	1													x
5	Performing OFAC Searches for potential C&I borrowers	Smith	Jones	4				x	x	x	x						
6	Decisioning overdrafts	Smith	Jones	3			x				x			x			
7	Monitoring loans over legal lending limit	Smith	Jones	0													
8	Approving loans to executive officers, director, or principal shareholders (insider)	Smith	Jones	0													
9	Conduct backup w/holding	Johnson	Grimes	2				x	x								
10	Monitoring Reg D transaction	Johnson	Grimes	2			x					x					
11	Escheatment of Funds	Johnson	Grimes	1	x												

Module II: SMARTER ™ charts

After the business lines have identified the activities they are involved with and the specific regulations that are associated with these activities, they are responsible for documenting the controls they have in place to manage each regulation, what they are expecting as a result of the controls, as well as other items. They use a SMARTER chart to walk them through this process. (SMARTER is an acronym that is used to walk clients through the risk management thought process.) This helps business lines understand where they are exposed to higher risks and formalizes (i.e., show your work) the compliance risk management process. Out of the SMARTER chart process, there is also a requirement to develop Action Plans for those regulations that expose the organization to compliance risk outside of the organization's risk appetite.

Module II

		Manifest / Materialize		Actions	Results	Testing	Expectations Met?	Review or Remediation Required?
This is the specific risk activity or business process being addressed. The activity / process should start with a verb. Example: Originate 1-4 Family Loans; Perform Outgoing Wire Transfer; Open New Deposit Account.	Describe the activity so that others who read the SMARTER chart understand what is addressed with the Risk Activity.	How would the risk materialize or manifest itself within the organization if there were absolutely no controls in place (also called the Inherent Risk)?	What regulation could be violated? Compare to the list of Regulations identified for this Risk Activity under the **Risk Activity Regulations** tab.	What actions/controls are in place to manage the risks? Document: 1. The controls that are in place. 2. If the control is automated or manual. 4. Who (title or department, not individual name) performs the action. 5. What informtion (e.g., reports, policies, procedures, other information) is used in the control? 6. Is any information transferred to another individual / department for further use?	What are the intended results / outputs from the actions? What would you expect to see happen? Document the amount of risk you are willing to take with this risk activity (e.g., Zero Risk Tolerance) and if / why you think there is risk of non-compliance with this risk activity even though we hvae controls / actions in place.	How do you as the Risk Owner make sure the controls you have in place are working? Consider: 1. What is done to verify the control is working correctly? Who does this? How often? 2. Are there reports or other information used to verify the control is working? 3. What Key Risk Indicators / Information (KRIs) would / do help to alert when the risk is increasing? The KRIs can be internal or external indicators. For example, a ratio (e.g., Loan-to-Value), or volume (# of transactions, dollar amount of acceptable losses) could be used. 4. What is done with the results? **THE GOAL IS TO BE PROACTIVE. AUDIT, COMPLIANCE AND LOAN REVIEW ARE NOT 'TESTING' CONTROLS.**	Were your expectations met? Based on your understanding, are the Actions sufficient to ensure the Results documented?	A more in-depth review is in order if the results of the review did not meet expectations, or the results indicate remediation is needed. Has an Action Plan been created to address remediation activities? The Action Plan should document what remendiation needs to take place.
Suspicious Activity Reporting	Monitoring transaction and behavioral activity across all customer accounts and reporting activity that is deemed suspicious to the FinCEN.	No SAR filings when suspicious activity occurs	BSA	Automated and manual monitoring systems to detect suspicious activity. Automated system is Patriot Officer - SAR Dector and MTM monitor. Manual reports include - monthly wire reports (incoming/outgoing), daily cash report, broken CD report, quarterly third party wire report, quarterly high risk account reviews, casa de bolsa wire review, monthly international ACH review, Patriot Officer daily OFAC review, monthly wire f/x review, monthly custody transaction review.	The Compliance Department will file SAR's within 30 days of detection of suspicious activity and 90 days thereafter, if warranted. No exceptions should occur. Zero risk tolerance.		Yes	No
		Suspicious activity undetected	BSA	Automated and manual monitoring systems to detect suspicious activity. Automated system is Patriot Officer - SAR Dector and MTM monitor. Manual reports include - monthly wire reports (incoming/outgoing), daily cash report, broken CD report, quarterly third party wire report, quarterly high risk account reviews, casa de bolsa wire review, monthly international ACH review, Patriot Officer daily OFAC review, monthly wire f/x review, monthly custody transaction review.	The Compliance Department will file SAR's within 30 days of detection of suspicious activity and 90 days thereafter, if warranted. No exceptions should occur. However, we understand that there may be some activity that goes undetected that is beyond our controls.		No	Yes
		Customer Money laundering undetected	BSA	Automated and manual monitoring systems to detect suspicious activity. Automated system is Patriot Officer - SAR Dector and MTM monitor. Manual reports include - monthly wire reports (incoming/outgoing), daily cash report, broken CD report, quarterly third party wire report, quarterly high risk account reviews, casa de bolsa wire review, monthly international ACH review, Patriot Officer daily OFAC review, monthly wire f/x review, monthly custody transaction review.	The Compliance Department will file SAR's within 30 days of detection of suspicious activity and 90 days thereafter, if warranted. No exceptions should occur. However, we understand that there may be some activity that goes undetected that is beyond our controls.		Yes	No
		Identity Theft undetected	OFAC	CIP/KYC policies and procedures. All new accounts are reviewed by compliance prior to account opening - loans and deposit accounts. Patriot Officer ID Theft scenarios (separate from MTM and SAR detector), W-8BENs forms, W-9 TIN Certification forms at account opening and updated when required.	We are comfortable with the policies, procedures and controls we have in place to adequately and reasonably identify the Bank's customers, both business and personal.		No	Yes

Module III: Compliance Activity Risk Rating

As a result of completing the SMARTER charts, the business lines (who is closest to the activity and understands the risks being faced) can rate the riskiness of their activities based on attributes that would change the riskiness of that activity. Examples are staff turnover, new/changes in product or service, audit findings, or technology changes. Each of these items (there are others) could have the potential of increasing or decreasing the organization's compliance risk and would be documented in the SMARTER chart.

Module III

	Risk Activity / Business Process	Changes / Additions to Products / Lines of Business	Changes in Transaction Volume	Staffing Complement	Changes in Technology	Control Documentation Effectiveness	Control Operational Effectiveness	Prior Exam/Audit Results	Current Risk	Prior Risk	Risk Direction
1	Originating Consumer Loans	1-Low/No	3-Mod/Routine	1-Low/No	3-Mod/Routine	1-Low/No	1-Low/No	1-Low/No	14	12	Increasing
2	Real Estate Foreclosure Processing	3-Mod/Routine	3-Mod/Routine	3-Mod/Routine	5-High/Complex	3-Mod/Routine	3-Mod/Routine	1-Low/No	28	27	Increasing
3	Sending Declination Notices	3-Mod/Routine	1-Low/No	3-Mod/Routine	3-Mod/Routine	3-Mod/Routine	3-Mod/Routine	1-Low/No	24	24	Stable
4	Identifying HMDA Reportable Loans	3-Mod/Routine	3-Mod/Routine	1-Low/No	3-Mod/Routine	3-Mod/Routine	5-High/Complex	1-Low/No	28	30	Decreasing
5	Performing OFAC Searches for potential C&I borrowers	3-Mod/Routine	1-Low/No	3-Mod/Routine	3-Mod/Routine	5-High/Complex	3-Mod/Routine	1-Low/No	28	35	Decreasing
6	Decisioning overdrafts	3-Mod/Routine	1-Low/No	1-Low/No	1-Low/No	1-Low/No	1-Low/No	1-Low/No	12	10	Increasing
7	limit	1-Low/No	1-Low/No	1-Low/No	1-Low/No	1-Low/No	1-Low/No	1-Low/No	10	9	Increasing
8	director, or principal shareholders (insider)	1-Low/No	1-Low/No	1-Low/No	1-Low/No	5-High/Complex	5-High/Complex	1-Low/No	26	30	Decreasing
9	Conduct backup w/holding	1-Low/No	1-Low/No	3-Mod/Routine	1-Low/No	5-High/Complex	5-High/Complex	5-High/Complex	36	35	Increasing
10	Monitoring Reg D transaction	1-Low/No	1-Low/No	1-Low/No	1-Low/No	1-Low/No	1-Low/No	1-Low/No	10	6	Increasing
11	Escheatment of Funds	1-Low/No	1-Low/No	3-Mod/Routine	1-Low/No	1-Low/No	1-Low/No	1-Low/No	12	12	Stable
12	Manage Client Return Mail	1-Low/No	1-Low/No	3-Mod/Routine	1-Low/No	1-Low/No	1-Low/No	1-Low/No	12	14	Decreasing
13	Force placement of flood insurance - Real Estate Collateral Monitoring	5-High/Complex	5-High/Complex	3-Mod/Routine	1-Low/No	5-High/Complex	1-Low/No	3-Mod/Routine	32	28	Increasing
14	Rendition	1-Low/No	3-Mod/Routine	1-Low/No	1-Low/No	3-Mod/Routine	3-Mod/Routine	1-Low/No	20	19	Increasing
15	Mortgages	1-Low/No	1-Low/No	1-Low/No	1-Low/No	1-Low/No	1-Low/No	1-Low/No	10	8	Increasing
16	Opening new Deposit accounts	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Module IV: Compliance Regulation Risk

After the list of regulations impacting the organization has been identified by the business lines (with the help of compliance), the compliance officer is responsible for assessing the impact of each regulation to the organization. The compliance officer should be influenced by changes to the regulation, the regulatory focus, and penalties for non-conformance. The focus of this exercise is to document the regulatory risk exposure from an external perspective. Internal risk should not be used in this analysis, as that is the business lines' responsibilities (Module II).

Module IV

REGULATION	RISK RATING 0 - N/A 1 - Low / No 3 - Mod / Routine 5 - High / Complex CURRENT	PRIOR	RISK DIRECTION
Right to Financial Privacy	1	3	Decreasing
Safeguarding Customer Information - GLBA/Outsourcing	5	3	Increasing
Identity Theft	3	5	Decreasing
CIP/USA PATRIOT Act	3	5	Decreasing
BSA/AML/KYC (possible fraud activity)	5	1	Increasing
OFAC	3	5	Decreasing
SAR	5	5	Stable
Truth in Savings Act - Reg DD	1	3	Decreasing
Reg CC	3	1	Increasing
Electronic Funds Transfer Act	5	5	Stable
Truth in Lending Act	3	1	Increasing
Flood Insurance	1	5	Decreasing
Home Mortgage Disclosure Act - (HMDA) Reg C	3	5	Decreasing

Module V: Compliance Risk

The culmination of the modules is an understanding of where compliance risk exists in the organization. This module takes into account the external regulatory risk (identified by compliance) as well as the internal risks (identified by the business line). The higher the score, the more risk the organization has in that activity and the greater the need for close management of that risk. This module should also be used as an influence on compliance monitoring.

Module V

	Risk Activity / Business Process	Risk Act Risk Rtg	Right to Financial Privacy	Safeguarding Customer Information - GLBA/Outsourcing	Identity Theft	CIP/USA PATRIOT Act	OFAC	SAR	Truth in Savings Act - Reg DD	Electronic Funds Transfer Act	Flood Insurance
Compliance											
1	Originating Consumer Loans	14					17				
2	Real Estate Foreclosure Processing	28			31	31	31	33			
3	Sending Declination Notices	24									
4	Identifying HMDA Reportable Loans	28									
5	Performing OFAC Searches for potential C&I borrowers	28			31	31	31	33			
6	Decisioning overdrafts	12		17				17			13
7	Monitoring loans over legal lending limit	10									
8	Approving loans to executive officers, director, or principal	26									
9	Conduct backup w/holding	36			39	39					

Proactive Compliance Monitoring

Compliance monitoring is a "proactive approach by the institution to identify procedural or training weaknesses in an effort to preclude regulatory violations." It is not an audit. With the partnership approach to compliance management identified above, it is important to maintain the partner relationship when it comes to compliance monitoring. The compliance function is there to support the business line. Since the business lines own compliance with the regulations, it should be viewed as a benefit to the business line to have compliance assist them in ensuring compliance with higher risk activities.

The goal of compliance monitoring is to be proactive and identify regulatory violations prior to auditors or the regulators. By documenting findings (again, show your work) and correcting the issues identified, you show your commitment to complying with the regulations and can have much more fruitful discussions on your compliance processes. If auditors or the regulators identify the issue through their testing but you identified it as well through monitoring and corrected it, their reaction to the non-compliance should be much less severe due to your proactive approach.

Compliance as an Enterprise Risk Management Function

COSO defines Enterprise Risk Management as:

> “a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential [*] events that may affect the entity, and manage [*] risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”

If we add the word ‘compliance’ where there are asterisks in the definition, we have defined the compliance process described in this document.

The compliance function and the Enterprise Risk Management (ERM) function complement each other magnificently. Where compliance is focused on specific regulatory compliance risk the organization is exposed to, the ERM function focuses on organization-wide risk of which compliance is a significant part of that risk.

The same approach described to redefine the compliance management process is the approach recommended when developing an organization’s ERM process. Those compliance risks that cause significant exposure to the organization (reflected on the compliance dashboard) would be escalated to the ERM Dashboard which is used to monitor organization-wide risks.

Summary

The role of compliance management in financial institutions needs to be transparent in order to effectively manage the changing regulatory landscape. It must be embedded in the culture of the organization and owned by the individuals performing the work. Compliance should not be seen as an operational or audit function, but as an organizational process necessary to provide reasonable assurance that the institution’s strategic objectives will be achieved. In two words, the role of compliance management is risk management.