ProSight™

The ProSight Compliance Risk Management Framework

BAI & RMA:
Together we're ProSight

ProSightFA.org

About ProSight Financial Association

ProSight Financial Association empowers financial services leaders to strengthen and advance our industry. Formed through the merger of BAI and RMA, trusted organizations with rich histories and deep expertise in risk, compliance, and retail and commercial banking, we are here to support you during times of great change, guide you towards new opportunities for growth, and help you act with confidence. As ProSight, we've enhanced our ability to support you at a time when the industry is challenged to meet changing customer needs, adopt new technologies, and manage more complex risk and compliance issues. Our work creates positive ripple effects throughout financial services organizations and our industry—and ultimately helps consumers, businesses and communities thrive. Learn more at ProSightFA.org.

Acknowledgments

The ProSight Compliance Risk Management Framework is published by ProSight Financial Association.

ProSight would like to recognize the work and guidance of RMA's Compliance Committee, chaired by PNC Chief Compliance Officer Michael Abriatis, in the creation of this framework. The ProSight Compliance Risk Management Framework has been approved by RMA's Operational Risk Council. The members of the Compliance Committee and Operational Risk Council are named below:
Candice Aaron, Charles Schwab, Dallas, TX; Roy D'Sa, Huntington Bank, Columbus, OH; Ryan Dirks, Fifth Third Bank, Cincinnati, OH; Lisa Hershey, DTCC, New York, NY; Ed Noonan, Truist, Charlotte, NC; Kelly O'Brien, M&T Bank, Eden, NY; Joel Ramos, Busey, Urbana, IL; Kevin Reese, Zions Bancorp, Farmington, UT; Carolynn Rosse, Raymond James, St Petersburg, FL; Prakash Samaga, Forbright Bank, Potomac, MD; Bill Walsh, First Citizens Bank & Trust Co, Raleigh, NC; Sean Walther, Huntington Bank, Columbus, OH.

Please direct inquiries to Katie Williams at rmaxchange@rmahq.org.

Design by Christopher Santoro.

March 2025

Table of Contents

Introduction

Financial service institutions have grown in size, scope, and complexity in recent years both organically and through the increasing use of third parties. As institutions have grown more complex, so have the requirements to comply with applicable law, regulation, and guidance on a federal and state level, as well as institutions' own governance policies. In short, institutions face considerable risk management challenges with respect to compliance risk management. The ProSight Compliance Risk Management Framework was designed to advance sound risk management and compliance principles for institutions of varying size, complexity, and reporting lines.

Compliance risk can result in regulatory fines and penalties; limits on growth; lawsuits and legal losses; and significant reputational risk. Accordingly, an institution should design, implement, and enhance its compliance risk management programs and oversight to align with its risk appetite.

'Compliance Risk' Defined

Compliance risk is the risk of legal or regulatory sanctions, financial loss, or damage to reputation resulting from failure to comply with applicable laws, regulations, rules, other regulatory requirements, or codes of conduct and other standards of self-regulatory organizations applicable to the institution.[1]

Purpose and Structure of the ProSight Compliance Risk Management Framework

The purpose of this framework document is to establish the overall parameters of a Compliance Risk Management Framework. The circular structure of the Compliance Risk Management Framework pictured in the figure on page 5 is highly intentional and can be applied regardless of the size of the institution or how an institution categorizes its risks. The individual components (such as "Policies & Procedures" or "Governance & Reporting") are not meant to be sequential, but, instead, are intended to represent a dynamic flow in both directions. Additionally, "Culture" is depicted as the foundation of the Compliance Risk Management Framework because an institution cannot foster an intentional and rigorous compliance risk management program without the "right" culture. By using the ProSight Compliance Risk Management Framework, an institution will be able to provide a clear connection to its risk appetite, Enterprise Risk Management (ERM) Framework, Operational Risk Framework, and risk reporting and analytics.

1 Compliance and the compliance function in banks, Basel Committee on Banking Supervision, April 2005, www.bis.org

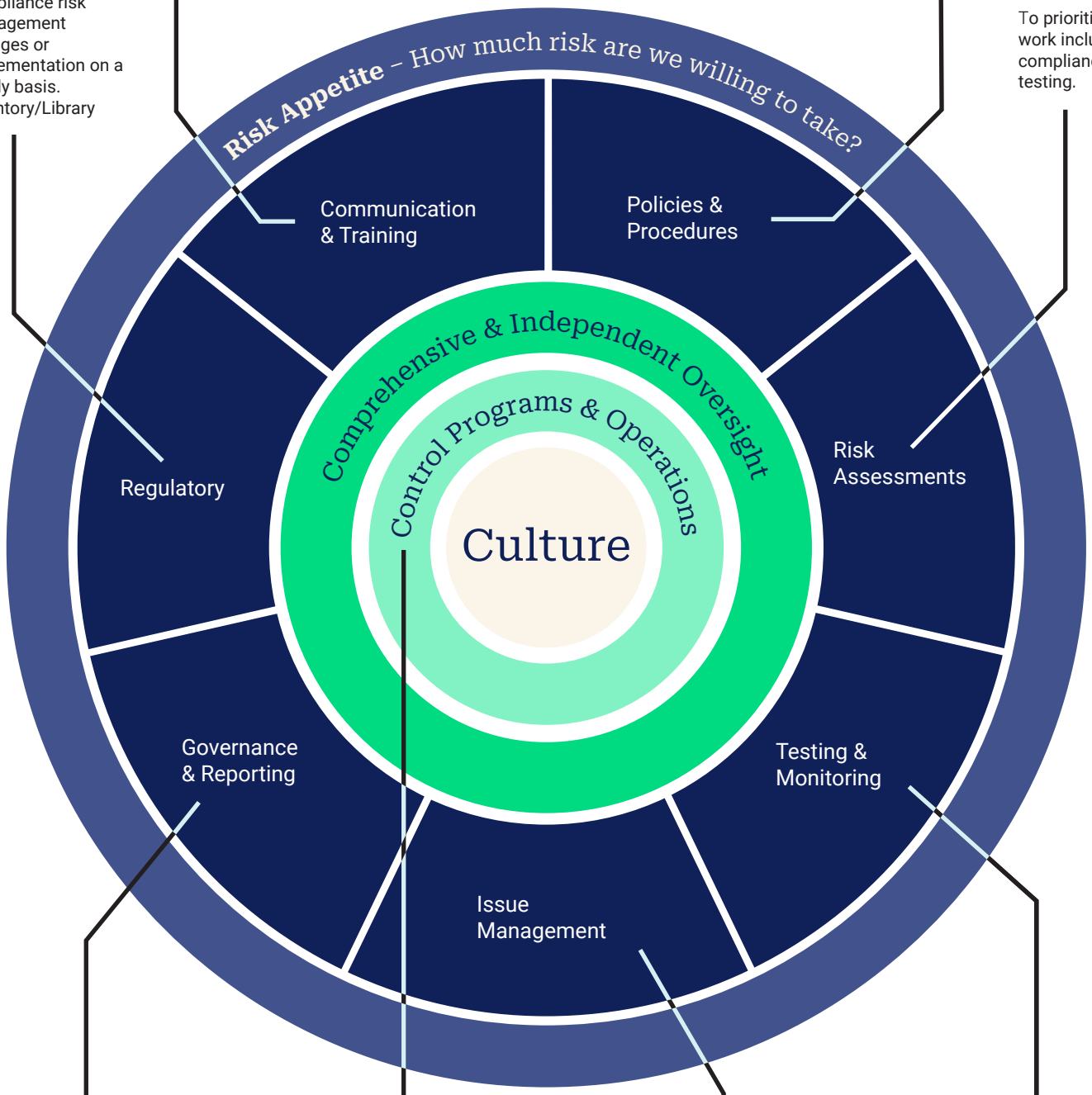
ProSight Compliance Risk Framework

- Regulatory Change: Monitor applicable legal and regulatory environment to ensure that compliance risk management changes or implementation on a timely basis.
- Inventory/Library

Ensure that applicable stakeholders (e.g. staff, board) understand applicable regulatory requirements and emerging risks.

To set forth accountability and direct staff to discharge compliance responsibilities.

To prioritize work including compliance testing.



In a timely manner, ensure board and senior management are informed of any material issues or trends, individually or in the aggregate, that may result in a breach of risk limits or put the bank at undue risk.

- Financial Crimes: BSA/AML, sanctions, SAR filings and investigations
- Fair Responsible Lending: UDAAP, CRA, FLA, HMDA
- Conduct: Compliance and ethics
- Licensed Employees: FINRA and SCCA regulation
- Fiduciary type responsibilities

Ensure appropriate and timely identification, reporting, resolution, and escalation of compliance risk issues.

Business unit or financial area oversight.

Problem Statement

It can be challenging for financial institutions to consistently apply compliance risk principles in a manner that adds value to the businesses and avoids being a mere "check the box" exercise. Without consistency, it is difficult for compliance risk managers to ensure appropriate and timely identification, escalation, resolution, and reporting of compliance risk issues. Given a dynamic environment where customers' needs and preferences related to products, services, and delivery channels evolve, it is critical that institutions maintain appropriate compliance risk management frameworks capable of growing and transforming as their risk profiles change.[2] In describing each element of an effective framework, this paper aims to help ProSight member institutions do exactly that.

2 See Semiannual Risk Perspective – Fall 2024; Office of the Comptroller of the Currency. OCC Semiannual Risk Perspective Fall 2024

1. Culture

Having the right risk management governance, culture, and internal control environment involves controlling what can be controlled. Financial institutions have always been expected to know the risks they face and to manage them appropriately. Articulation of risk appetite, policies and procedures, governance, internal controls, risk measurement, data infrastructure, reporting, and all other risk management activities are mission critical but of diminished value if the institution does not have the right culture.

Culture is at the heart of any institution's compliance risk management program. Without it, the other essential elements are not nearly as effective. However, as institutions grow more diverse to meet customers' evolving needs, they necessarily grow larger and increasingly complicated. As a result, it becomes harder for institutions to remain steadfast in applying the values that foster good corporate culture.

Culture Drivers

There are seven key drivers of good culture:

- Tone from the top.
- Cascading values to the rest of the institution.
- Translating values into business practices.
- Empowerment and accountability.
- Effective communication and challenge.
- Recruitment, training, and rewards.
- Governance and control.[3]

3 Australia Securities and Investment Commission, The importance of culture to improving conduct within the financial industry - speech - 27 May 2015

The board and management can facilitate ethical conduct and compliance with applicable laws, rules, and standards, as well as internal policies, by promoting and modeling a strong institutional culture. A strong culture reinforces the ethos that the institution will conduct its activities in accordance with applicable laws, regulations, standards, and policies, and encourages employees to conduct their activities in accordance with both the "letter and the spirit of the law."

Objectives

A strong culture accomplishes two key objectives. First, it helps an institution make well-informed decisions. For example, a culture that rewards candor, transparency, and debate makes behaviors that cloud good decision-making—such as a "herd mentality," "confirmation bias," and "groupthink"—less likely, and illustrates that risk management is part of everyone's responsibilities and accountabilities. In addition, a strong risk management culture helps the institution identify rogue individuals and/or groups. It is said that 99.9% of people show up to work every day intending to do the right thing. Sometimes these people make bad decisions not because they want to, but because of flawed thinking. However, there are times when individuals or groups (the other 0.1%) are more interested in their own personal gains than in doing what is right. In such cases, a strong risk management culture tends to ensure that individuals conform to the culture or are eventually asked to leave. The reward is an environment in which people become the institution's collective strength as they work toward a common goal rather than individual interests.

In short, a strong culture bolstered by an effective compliance risk management framework helps to ensure that an institution operates with integrity and provides fair treatment to its customers.

2. Control Programs and Operations

Role of Business Units

Business units are responsible for managing the daily activity of the institution and for ensuring implementation of the Compliance Risk Management Framework. This responsibility includes ensuring the framework is adopted by the business units in accordance with framework guidelines and that the internal control environment has a sufficient level of controls to assure that errors and omissions are identified and corrected as part of the ordinary course of business.

Control Environment

Every institution conducts its business in a volatile and changing operating environment. There is risk inherent in every business activity and process. The internal control environment is one of the most important tools for the management of risks, because internal controls can help reduce the level of inherent risk. This resulting level of risk—residual risk—is the level of risk acceptable to management. An institution's control environment will include both preventative and detective controls that are subject to testing by second line risk management and compliance.

3. Comprehensive and Independent Oversight

Compliance Risk Management

Compliance risk management establishes the framework at a strategic level by providing guidance, developing and maintaining tools, consolidating and reporting compliance risk exposures, and measuring activity to ensure that it remains within the risk appetite of the institution.

The compliance function will generally be more effective when there is a strong working relationship between compliance and the business lines. However, the corporate compliance function—like second line risk management—must be independent of the business lines. Inherent conflicts of interest can be avoided or mitigated by ensuring that the business line is accountable for managing compliance risk while the independent second line/corporate compliance function provides the framework and tools for doing so. Independence ensures objectivity and helps to avoid inherent conflicts of interest that would otherwise impede or weaken the effective implementation of an institution's compliance risk management program. However, independence should not preclude compliance staff from working closely with the management and staff of the various business lines.

4. Policies and Procedures

Policies

Policies communicate and reflect the institution's risk appetite to all stakeholders. Policies describe what the institution is willing to do and not willing to do. An institution's risk appetite statement is operationalized through policies that describe what the institution should do, as well as procedures that set forth how the policies will be implemented and executed.

An institution's policies set the tone of the control environment by establishing the fundamental set of rules that govern how business will be conducted. Policies set the boundaries for risk management and make clear that it is management's responsibility to see that risk, including compliance risk, is managed within the boundaries set.

Policies can exist across the organizational structure. Board policies (also known as bank policies or corporate policies) communicate the institution's risk appetite to staff and provide institution-wide guidance and risk expectations. While board policies may largely impact only one part of the institution, they nevertheless apply to everyone.

Examples of board policies include the:

- Corporate risk management policy.
- Credit policy.
- Liquidity policy.
- Information security policy.

Generally, board policies are ratified by the board (or a designated committee of the board) at prescribed intervals, with an annual review being most common.

Management or operating policies are typically more operational or technical in nature and generally apply only to a specific operating area of the institution. Examples of operating policies include policies related to technology systems, technical compliance requirements, or other department-specific policies. Operating policies are usually owned and updated by a specific department and are typically ratified by the institution's risk committee or other designated governing body.

Generally, policies should be brief and include the following attributes:

- Overview of the policy, which states what the policy is intended to accomplish.
- Authority, which identifies the role or function that is accountable for implementing the policy.
- Implementation, which states how the policy will be implemented.
- Exceptions, which note how deviations from the policy should be handled.

Procedures are highly specific and describe in detail how the policy will be executed. Effective procedures should be written at a level and in a manner that allows them to be audited or tested.

Generally, policies are approved by the board of directors or its designated committee; they are expressions of the board-approved risk appetite statement.

Procedures

Procedures are commonly used control tools and are approved by the appropriate management group that is responsible and accountable for their execution. How an institution approaches development and implementation of procedures should be consistent with the institution's size, scale, complexity, and ability to maintain them.

Operating procedures document the manner in which a process is accomplished at the most granular level. Granularity in this context is defined as the level of detail the institution wants to capture. For some institutions, this may be step-by-step instructions detailing the mechanics of a process. For others, it may be a more general description of how a process is accomplished.

Regardless of the level of granularity, an institution should maintain standards established to drive a clearly defined level of consistency across the institution's documentation.

Process Flows

Process flows—supported by supervisory and operating procedures—capture the essential elements of how a process progresses from a clearly defined starting point (where hand-offs between departments occur). In addition, process flows specify which systems are critical in performing a crucial step, and, importantly, identify control points along the way.

Process flows are essential to an internal control environment, given the need to communicate to external parties how the institution's critical functions are executed.

The most important factors in the execution of policies and procedures are: (a) regular, clear, and effective communication to the appropriate stakeholders; and (b) incorporation of policies and procedures into day-to-day processes and technology.

5. Risk Assessments

Once the processes and controls are in place and operational, the next step is to establish a framework for assessing the effectiveness of the risk-mitigating controls. The first line of defense owns these processes and is accountable for their management and ensuring they operate within an acceptable risk tolerance. The role of the second line of defense is to ensure that the first line is living up to this expectation.

The compliance risk management program is instrumental in establishing how these assessments are conducted. Regardless of structure, it is essential to the internal control environment to have a mechanism for assessing the risk to the institution, based on a range of plausible scenarios and the strength of the institution's controls in managing that risk.

Risk assessment is the identification, measurement, and analysis of risks, both internal and external, controllable and uncontrollable, at individual business levels and for the bank as a whole. Management must assess all risks facing the bank because uncontrolled risk-taking can prevent the bank from reaching its objectives or jeopardize its operations. Effective risk assessments help determine what the risks are, what controls are needed, and how they should be managed.[4]

4 Comptroller's Handbook – Internal Controls, p. 6, Office of the Comptroller of the Currency pub-ch-internal-control.pdf

Process Risk and Product Risk Assessments

Process risk assessments are used to demonstrate that management is aware of its control environment and that it can proactively address control gaps. Process flows must have a combination of preventive and detective controls to ensure that, as business is transacted, a potential error is identified and corrected as part of the normal course of business; however, this does not assume that every sub-process has a control. Process risk assessments are a means through which management can measure its own system of internal controls. Product risk assessments, as used with the framework document, is a term applied to new products and/or services, new business initiatives, or existing products.

Target Risk Assessments

Target risk assessments are ad hoc analyses that result from observed or perceived deficiencies within the control environment. Target risk assessments are used to identify and measure the significance and likelihood of a control breach and possible regulatory, financial, or reputation impact that could occur within a function or specific process. The target risk assessment allows the business to gauge the effectiveness of the controls relative to the risks and to plan which type of controls should be implemented to mitigate the risks.

Control Failure Analysis

Despite maintaining a robust control environment and rigorous testing, control failures can occur. Control failure analysis is performed to explore the root causes of a failure and to make systemic changes to the control environment based on the analysis and findings.

6. Testing and Monitoring

While testing and monitoring are often used synonymously because they both help to identify weaknesses in controls, it is nonetheless important to differentiate the two concepts to drive maximum value for the institution. Monitoring, on one hand, is the regular and systematic review of key risk indicators (KRIs) as an early warning sign that there may be compliance violations. On the other hand, testing of compliance controls helps to determine whether the material assumptions, data sets, and procedures used in measuring and monitoring compliance risk are working as intended.

The frequency and scope of compliance testing should be based on the assessment of the specific compliance risks associated with a particular business activity, while key compliance risks should be monitored—either on an automated or manual basis—as part of daily activities.

7. Issue Management

Having good controls in place is an important first step in managing compliance risk to an acceptable level—but control design is only the beginning. In order for a system of controls to work effectively, it must be combined with systems for monitoring activities and identifying when activities take place that either violate a control or indicate a potential risk despite the presence of a control.

When evaluating issues that do arise, it is important to focus on understanding the actual or likely impact of the event, its root causes, what needs to be done to recover from the event, and what can be done to prevent the same or similar issue from arising again. Unfortunately, too much time can be spent determining which person/function is at fault, but this is informative only within the context of corrective actions. In fact, if someone does cause an error or problem, then this person should be given the first chance to suggest ways to improve the process so that the incident can be avoided in the future.

Repeat issues or findings of control weaknesses may be handled differently depending on the number of people involved. If the root cause consistently lies with one person, then this is an HR issue. However, if it is an issue of poor process design, under-developed or ineffective controls, the result of changing circumstances, or actions outside of one's control, then these must be dealt with at a process and control design level.

When dealing with issues, people must not be afraid to point out weaknesses for fear of criticism; in such an event, the institution will never achieve a mature risk management state. All employees should have the ability to challenge—without recrimination—assessments or assumptions related to any process or control.

Finally, the value of instituting a process for control failure analysis will be obvious when the inevitable happens and some unexpected event needs review. The process should include the following steps:

- Re-analyzing the base risk assessment and related internal controls: Did the event provide any different perspective on the inherent or residual risk? Is the residual risk within acceptable tolerance levels?
- Evaluating the controls: Are the related controls too weak? Too rigid?
- Reviewing policies and procedures: Are adjustments warranted to policies, processes, or even people?

Building a sustainable risk management program requires the inclusion of self-teaching mechanisms. This requires a level of honesty and transparency that does not always exist.

8. Governance and Reporting

Governance

Strong governance can help ensure that the risk appetite implicit in the institution's business model, strategy, and execution is appropriate such that expected risks are commensurate with the expected rewards. There are several indications of strong governance:

- Management has implemented a system to manage, monitor, and mitigate risk that is appropriate to the institution's business model and strategy.
- The risk management system provides timely and relevant information to the board regarding the major risks facing the institution and how they are being managed.
- An appropriate culture of risk awareness exists throughout the organization.
- There is recognition that management of risk is essential to the successful execution of the institution's strategy.

For large incidents, every institution should have some form of reporting mechanism to the governance committees for presenting and discussing issue identification and resolution. Learning does not stop at the department level. If senior management and the board are going to be part of the process of managing risk tolerance, they must be made aware of what is happening within the organization.

The emphasis in reporting should always be on, "What happened, what does it mean, and what are we doing about it?" To the extent possible, the institution should balance the need to make specific individuals accountable with developing a culture that encourages these same individuals to come forward before an issue arises or as soon as they are aware of an issue.

Reporting

Risk reporting is conducted in line with the approved and established policies and tolerances. Management reports should routinely include risk appetite measures. The nature of risk management programs is that they create an enormous quantity of information. The key is to identify which information is truly meaningful and actionable. The best risk reports create dialogue and are actionable. A prerequisite for effective governance and reporting is a culture that rewards learning, encourages transparency, demands cooperation, and discourages a "fortress" mentality. It is important to note that:

- Risk reporting is only as good as the level of honesty and transparency that is allowed.
- Information reported without context can be extremely dangerous.
- Thorough risk reporting considers macro risks and micro risks.
- An institution should evaluate the extent to which the risk reports discuss whether an operation is aligned with the institution's risk appetite.
- The report doesn't have to be the same one every month.

9. Regulatory Change

It is incumbent that institutions remain well-informed about the changing regulatory landscape to maintain effective compliance risk practices. The financial services industry operates in a complex, evolving, and highly regulated environment. Institutions should establish a process to routinely monitor applicable laws, regulations, and court decisions that may impact their operations. This would include monitoring financial services regulatory agency websites to remain informed about changing regulatory priorities, notices of proposed rulemakings, enforcement actions, and other matters that may impact an institution's operations. Institutions should be cognizant of other general sources of regulation that may impact their operations such as state privacy, accommodation, and disclosure laws.

In addition, institutions should consider compliance challenges that arise when the pace of innovation and technology outstrip existing law and regulation. Other sources of information regarding the impact of changes in applicable law and regulation include legal counsel, both internal and external, and industry associations.

10. Communication and Training

Clear, consistent communication of the institution's expectations is central to implementation of the Compliance Risk Management Framework. Communication of the institution's tolerance for compliance risk should be cascaded down through the organization. The following examples of clear communication are for descriptive purposes only and not intended as suggestions:

- We will manage our company within the confines of all legal and regulatory compliance.
- We sell only products that we believe are suitable for the customer and that the customer will understand.
- We will be able to explain our suite of products in plain English, and the products will have no hidden features.
- Every employee will understand the compliance risk associated with his/her daily activity and conduct.

Importantly, the compliance function should analyze the impact of, and clearly communicate changes in, applicable law[5] that would impact: (a) the delivery or consumption of the institution's products or services; (b) customers, including former and prospective customers; and (c) processes to support the delivery of products and services to customers (including the use of customer data) whether performed by the institution or third parties.[6]

Training is an important component of the Compliance Risk Management Framework and should be designed to ensure that employees of the institution understand their obligations and how the changing regulatory environment may impact their job functions and processes. Training should be conducted on a regular and routine basis so that employees may stay abreast of changing compliance obligations and the institution can effectively demonstrate that compliance is taken seriously.

5 "Applicable Law" may be defined as any applicable domestic or foreign law, rule, regulation, order, or other action, decree, requirement, or guideline published or in force at any time which governs or regulates any person (including any party or any affiliate thereof), property, transaction, activity, event or other matter (collectively, the "Activities"), including those issued by any regulatory authority or issued by any court having jurisdiction over the Activities of the Institution.

6 See e.g., OCC Bulletin 2023-17, which describes sound risk management principles to consider when developing and implementing third-party risk management practices, commensurate with the bank's risk profile and complexity as well as the criticality of the activity supported by the third party.

11. Risk Appetite

Risk appetite may be defined as the amount of risk that an institution is willing to take or accept in pursuit of its strategic objectives and business plan. The concepts of risk appetite and risk capacity are often used interchangeably, but they have distinct differences in meaning. Risk capacity encompasses the broadest or maximum expression of risk an institution is capable of tolerating, when considering its capital and liquidity base, among other factors. Exceeding the risk capacity might lead to challenges in continued operations and could indicate that a bank is moving toward a recovery-type event.

Risk appetite for many banks is set within their risk capacity. The risk appetite sets constraints for absolute levels and different types of risk-taking in alignment with an institution's strategic objectives and business plans. Risk appetite may also consider other factors, such as the institution's risk management and control capabilities. Setting risk appetite within risk capacity helps to ensure that the institution does not jeopardize its ongoing operations while pursuing its business objectives.

An institution's risk appetite statement should be broadly communicated, cascaded within the institution, understood across the three lines of defense, and used to manage the business. A statement of risk appetite is as much about culture and a way of thinking and behaving as it is about risk policies, tolerances, reporting, and governance. A truly effective risk appetite program is embedded in day-to-day decision-making and influences the risk culture of the organization.

An institution should strike a thoughtful balance between comprehensiveness, prioritization, and volume in the metrics included in the risk appetite statement for compliance risk. The metrics may be a mixture of qualitative statements and quantitative measures:

Examples of Qualitative Statements

- The institution is committed to implementing practices and controls that will minimize financial losses from operational risks and compliance risks (e.g., people, process, technology, data, fraud, third parties, etc.).
- The institution will implement processes and controls to enable compliance with all laws and regulations.
- The institution has no appetite for business in countries on government prohibition or sanction lists.
- The institution will seek to retain our high performers, ensure robust succession planning, and maintain high levels of engagement with our staff.
- Compensation/incentives should be aligned with the institution's risk appetite and consider risks appropriately in addition to returns.
- The institution will not undertake a new business, expand our market, or offer new products or services until the compliance risks that will be incurred are thoroughly understood and the necessary talent and resources to effectively manage and mitigate those risks are obtained.

Examples of Quantitative Metrics

- Number of significant regulatory/audit findings outstanding or past due.
- Number of open compliance exceptions.
- Number of BSA/AML- related losses.
- Legal related financial losses.

ProSight™

ProSightFA.org