Deloitte.

Training plan

The elements of "getting to strong" in focus

Produced by the Center for Regulatory Strategies

What does it take to get to strong?

There are four specific elements banks should consider to build risk management programs that would be considered "strong" in the eyes of regulators. While the elements themselves have not changed over time, their reach and the depth in which they could be applied are different today.

Below, we offer a detailed look at how banks might put each of these elements to work.

Governance

Throughout the industry, there is a concerted effort to raise the game when it comes to risk management. The status quo is not good enough. As a result, the new utopian state appears to be one that defines risk management programs as being rated nothing less than "strong." While there is little in the way of formal guidance as to exactly what strong looks like, there is a high degree of confidence that it's not where the industry is today. Included in the strength equation is the adequacy of the risk governance effort. The inability to achieve the highest designation in risk governance will likely diminish any hope of gaining a strong overall rating. Consequently, it's important that banks get the governance component right.

Creating an effective governance program begins at the top with bank leaders. The level of emphasis the board of directors or senior management place on governance—what is known as the "tone at the top"—is often the most important factor in determining the success or failure of an organization's efforts. A strong "tone at the top" can help shape an organization's culture to focus on proactively managing risk.

The following are specific steps a banking organization could take to assist their governance program in "getting to strong:"

Set the "tone at the top"

It is crucial for the board of directors and senior management to relay and disseminate consistent messaging across their organization.

"Tone at the top" can help shape attitude and culture, and is extremely important for leaders when creating accountability for risk across an organization. Individuals at all levels should not only understand what is expected of them, but also know the consequences if they engage in unacceptable risk-taking. For leaders, setting the "tone at the top" can be a challenge as they also may need to deftly build an ethical environment in which individuals are allowed to take informed, intelligent risks without stifling innovation. Effective organizations aren't defined just by the smart risks they take, but also how they manage them. Setting a strong "tone at the top" is likely to help create and support strong risk management principles throughout an organization.

Define and implement a strong risk culture

Whether written as a mission statement, spoken, or merely understood, corporate culture can be described as how an organization thinks, feels, and acts. When implemented effectively, culture is the foundation for everything the board and management do to properly govern an organization. Building a genuine culture of "doing the right thing" reinforces the responsibilities and accountability of those within an organization and helps hold employees to the highest level of integrity and ethical conduct. Organizations should focus on ongoing communication and training to enhance and maintain the risk culture.

A key component to sustaining a strong risk culture is to strive to ensure the bank deploys the right human talent. Hiring processes that focus on risk awareness, promotions based on a demonstrated commitment to risk management, clear standards of behavioral expectations, and appropriate structuring of incentives to induce desired outcomes may all play a key role in guiding the bank's employees.

Define roles, responsibilities, and authority

In an environment in which everyone is expected to play an active part in managing risk, it can be hard to know where one individual's or group's responsibilities end and another begins. Therefore, it's increasingly important to clearly define who is responsible for what, particularly as it relates to risk management. The board plays a key role in determining which responsibilities and authorities must be clearly defined to ensure strong governance. Boards are expected to take a more active role in risk oversight and need experienced members who not only have a deep understanding of an organization's issues, but the ability to challenge the executive team and management.

Although the board plays a specific role, it's crucial that all individuals clearly understand their respective roles and responsibilities. Clear accountability and responsibility assists all parties in being able to make better, more informed, and quicker decisions—and avoid conflicts of interest. Clearly defined roles and responsibilities may allow for greater individual impact on an organization's strategic plans. Knowing one's place in an organization may help everyone understand their part in executing long-term performance. Of course, it also may allow for associates to hold each other—and the board/executive team—accountable to strong standards and a shared vision.

Organizations may deploy a strategy of "three lines of defense" so everyone may be part of risk management ownership—from front line and business unit management to the oversight and internal audit functions. A clear definition of roles and responsibilities helps players at all levels understand their part of the process.

Using a standardized approach to support governance

Within any given bank, different parts of the organization typically face a variety of risks and are subject to a number of different compliance and regulatory requirements. As a result, it is not uncommon for a bank to harbor several wholly discrete approaches to risk management, from processes to technology and beyond. This results in vulnerability as decentralized and inconsistent approaches may cause inefficiencies and operational gaps within an organization. Banks should aim for a more streamlined, holistic approach—one that improves its ability to delegate authority, escalate issues, and control complexity. All business units and functions should perform their risk-related responsibilities in a similar manner, while at the same time, governing bodies, such as the board, audit committee, and risk committee, should gain consistent levels of visibility and transparency into the organization's risk management practices. These can be achieved through established reporting lines, organization, and committee structures with clearly defined mandates, agendas, and reporting. These approaches create mechanisms to identify risks as well as to escalate, monitor, and report issues. In addition, a risk appetite statement should be established, communicated, and understood by the entire organization. Communicating this risk appetite is critical—everyone in the bank should be able to articulate how it applies to their area of responsibility.

Over the long haul

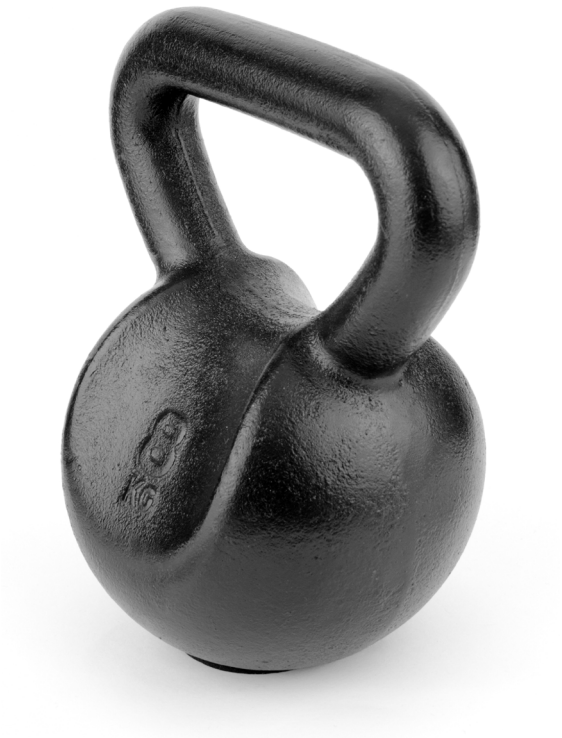
Given the speed that an organization's operating, market, and regulatory environment can change, it is important to frequently reassess the approach to governance to see what's working, what's not, and change course accordingly. An organization should continuously evaluate performance goals, incentive compensation, metrics, and employee training. It should determine that the roles and responsibilities are clearly defined, examine the risk training for effectiveness and compliance, and continue to hire and promote the appropriate human capital. An organization's approach should not be static. There are, however, some governance values that are unchanging, starting with the "tone at the top" and the culture of accountability. In the absence of clear, consistent messages from top-level leadership communicating the importance of risk management and a mandate to operate in a safe and sound manner, an organization's approach to governance will most likely be lacking.

In addition to frequent reassessments, thinking about implementing a governance maturity model may also help leaders evaluate the strength of their institution's governance program. The model can help identify warning signs of an undeveloped governance program and how to improve it, what a strong program entails, and how to streamline an organization's current program while leveraging existing practices. Key governance cornerstones assessed through the maturity model are the overall governance structure, the governance strategy and decision rights, supporting infrastructure, communication and reporting, and an organization's people and culture. Implementing and leveraging a governance maturity model is likely to help an organization determine where its approach stands in relation to where it should be to reach that strong rating.

Policies and procedures

An organization's risk appetite can set everyday expectations for its people. So how can an organization ensure the actions being taken are appropriate and uniform throughout? The answer may be found, in part, in the policies and procedures it has set in motion, and the rules implementing those expectations. Policies and procedures are the link between a bank's strategic vision and its day-to-day operations. It's not likely banks will be able to satisfy regulatory requirements for strength in risk management without a robust set of policies. Just as important, banks may be in a better position to weather the future's unexpected events because of them.

For many banking leaders, the issue of policies and procedures may be quite straightforward: Identify specific risks and regulatory requirements; develop clear policies that address them; and, execute those policies with procedures that match the operating environment of the business. That's all very important, but is not all-encompassing.



A bank's current menu of policies and procedures should reflect its risk appetite. For example, a conservative appetite might stop an aggressive policy on leveraged lending in its tracks. Policies and procedures should include reference to the laws, rules, and regulations pertinent to the area covered. Policies governing heavily regulated areas, such as deposit gathering or mortgage servicing, could include appropriate reference to the myriad of government expectations applicable to them. Policies should likely reflect the bank's current business strategies. If the current business plan calls for introduction of new or modified products, or new geographies, related policies and procedures could be adapted accordingly. New adventures should not be embarked upon without first having some degree of rules in place.

Policy development tends to be ineffective without execution. Enforcement of policies and procedures is important. A company can have great policies, but if no one follows them, they are likely to serve little purpose. To ensure adherence and enforcement, a robust system of periodic self-testing could be put in place to ensure policies and procedures are being followed. Notable exceptions could be tracked and causative factors investigated. Frequent exceptions may indicate the policy is at fault and may be in need of revision. Worse, however, might be the possibility that corporate culture eschews a process mentality or individual employees act deliberately out-of-policy. In either case, remedial action could be taken. All of these may be avoidable with a strong execution process.

Banks may also, at times, suffer the issue of version control. Over time, multiple policies and procedures are discovered to target the same issue, and not always consistently. This might arise when the governance process over policies is weak. There can be many reasons for this, ranging from a simple failure to cancel previous versions to managers keeping a "desk copy" of an old version for handy reference or others as complex as an intranet issue that fails to delete prior versions.

Compounding the issue of version control may also be the possibility of unauthorized policies circulating throughout the bank. Often done with the best of intentions, these are "policies" issued by nonsanctioned individuals seeking to address a chronic problem or a perceived risk. Proliferation of unsanctioned policies may result in conflict with official company posture, create confusion among employees, and even create a legal threat to the bank by establishing behavioral standards against which it could be subsequently held. One of the ways to avoid such problems could be via a strong control over policy and procedure governance.

An executive team and board actively engaging in setting the standards, and making sure the effort is supported by the right governance structure, may be able to exercise firm control over its policies and procedures. For example, ownership for policies and procedures should be clearly defined throughout the organization. The owner should ensure the policies are approved by the appropriate committee or other authorized agent. All policies should be registered to prevent unauthorized issuance, centrally maintained to facilitate ease of access, and periodically reapproved to ensure they continue to reflect the organization's current posture on the topic.

Following are a few specific steps bank leaders can take to shore up their approach to policies and procedures.

Focus on oversight

Effective oversight results in stronger policies and procedures. But the issue of oversight can remain a challenge for many banks. The board of directors sets the standards for policies and procedures. From there, the interaction between a board of directors and executive managers is essential in developing, overseeing, and managing these rules. It is management's responsibility to create and implement policies and procedures based on the board's risk management expectations and standards. Of course, the process doesn't stop there. Committees have to review and approve these policies and procedures, which then should be clearly communicated to the relevant lines of business.

Banks should consider using a host of mechanisms to verify that the policies and procedures are sufficient, in line with expectations, and applied appropriately to the specific business units. There could also be other mechanisms in place to inform the board when these policies and procedures are working properly and when they're not. This way an organization is actively monitoring and updating policies and procedures as changes to market conditions, strategies, activities, and practices occur.

Cultivate operational excellence

Once a policy or procedure is approved, it should be communicated to those affected by it. Taking the extra time to ensure clear understanding of expectations can help those who need to implement it. Depending on the policy or procedure's complexity, formal training may also be necessary. Taking the time, up front, to set the expectations and explain the rationale behind them will likely result in better adherence in the future.

Strong testing and controls capabilities on the back end help confirm that the policies and procedures are actually being followed. Like other internal controls, policies and procedures could be tested on a consistent basis to demonstrate compliance. Such testing is likely to help identify emerging issues, which may be driven by lack of understanding, lack of conformance, or policies that simply aren't working as they were expected.

Over the long haul

It's important for banks to implement and communicate clear, well-written policies and procedures tied to their risk appetite. Policies shape how decisions are made within the bank, providing needed guidance to help achieve strategies and goals. Procedures define how things get done. Sound policies and procedures help employees understand their roles and responsibilities within predefined limits—providing them with the ability to execute specific tasks reliably, consistently, and accurately. It's important that banks review the appropriateness of their policies and procedures on a regular basis. Many banks subject their policies to an annual review, or more frequently when industry or regulatory changes necessitate it.

Internal controls

Internal controls have continuously been the focus of change and enhancement in the financial services industry. However, this is particularly true over the past 30 years. From the 1991 FDIC Improvement Act[1] and the subsequent 2002 Sarbanes-Oxley Act,[2] banks worked purposefully to improve internal controls, likely resulting in improvements in their ability to detect and prevent inappropriate or unapproved risk taking. Today, banks once again may be seeking to take their internal control framework up a notch. The reason? A desire to achieve the coveted regulatory rating of "strong" for their risk management programs.

Mapping business flows

Business flows—the routes that everything from loans to deposit accounts to investments follow throughout the organization—lie at the heart of this focus. Why is that? In order to understand where controls should apply, banks need to have a solid understanding of how business moves through the company. The challenge is that there are so many business flows in any given company, trying to map them all may be akin to boiling the ocean. Intimidated by the size of the task, some organizations may seek a shortcut by trying instead to best-guess where controls may be needed. The risk of such an approach is likely to be that critical processes could be overlooked, providing an open door for bad things to happen.

An alternative approach may be more appropriate—creating a hierarchy of process flows. Combining the deep knowledge of the business managers with the expertise of risk management personnel, a number of banks are identifying the most important flows to be mapped immediately. Processes falling into lower tiers are addressed over a longer period of time. Using such an approach is likely to make the entire effort more manageable.

Banks engaged in the effort of mapping business flows may sometimes find that processes are well understood and controlled within a given business unit. However, when the same business transfers from one unit to another, the clarity can fog over. The job is not done when a business unit maps the flow within its own confines. It's done when management can clearly follow the course of the business from when it enters the organization to when it exits—oftentimes across multiple business units and from front to back offices. This necessitates coordinated effort among business and functional unit leaders to ensure no one drops the ball along the way.

Mapping controls

Once the process flows are understood, the second stage of the effort begins—mapping applicable controls against them. For our purposes, the term "controls" is used in a broad sense. It includes elements such as Sarbanes-Oxley and other operating controls, as well as the checks and balances needed to implement compliance requirements, the organization's own policies and procedures, and regulatory safety and soundness expectations. Once there is clarity of how business moves through the company, it is much easier to understand where the broad array of controls need to be put into place. Thus, we move from "business process mapping" to "control mapping."

Control mapping allows organizations to create matrices that analyze where a defensive action might need to apply. For example, identifying all front or back office business units engaged in payment of funds could provide clarity regarding where dual-control requirements may be needed. Similarly, identifying all areas of the organization that engage in new account opening enhances the ability to impose "know your customer" requirements more effectively.

Spreading a list of all business units on a vertical axis against a list of control requirements on the horizontal axis provides the ability to "heat map" areas that are in need of most urgent attention. This may often necessitate parsing controls into their many component parts, creating numerous maps along the way. One only has to visualize a complex requirement such as anti-money laundering and its many nuances to understand the size of the effort that may be necessary.

[1] Federal Deposit Insurance Corporation Improvement Act of 1991, 12 U.S.C. 1811 (1991), http://www.fdic.gov/regulations/laws/rules/8000-2400.html.
[2] Securities Act of 1933, P.L. 112-106 (approved April 5, 2012), http://www.sec.gov/about/laws/sa33.pdf.

Testing controls

The final step in this process ensures that the implementation is effective. Controls are of little use if no one is adhering to them or if there is no procedure in place to address them when they are breached. Thus, once the controls have been mapped and implemented, banks should routinely test their efficacy. Critical controls should be tested with high frequency; others can be checked over an appropriate period of time. When testing detects a malfunctioning control, causative factors should be investigated. Root cause analyses should be performed, corrective actions taken, and accountability assigned. Closer monitoring should be implemented until the organization is confident the repaired control is once again functioning as it should be.

Empower the front line

No one knows a bank's business processes better than business managers—those who are on the front line of a banking organization and its biggest risk takers. By empowering them with the responsibility to self-assess and implement internal controls, this first line of defense can better gauge whether these controls are operating as intended. The idea is to make risk management pervasive throughout an organization and at every level. With frontline employees given such authority and accountability, the bank's second line of defense—the risk management unit—can provide efficient and effective oversight.

Smooth the path to escalation

While frontline managers should have the power to identify and fix problems, they should also escalate and report such problems to senior management and the board of directors. Today, banks should consider having the right mechanisms in place to help managers raise and report such concerns to the right parties in a timely manner. Many banks are formalizing their escalation processes so that employees know what to do when something goes wrong. The enhanced escalation protocol applies not only to breaches of internal controls, but also to other inevitable mishaps that occur. For example, if an information system is hacked, a robbery occurs, or an adverse media report on the bank is about to be released, employees have an established venue to notify proper authorities. This allows the right people to get involved on a timely basis to minimize damage and ensure an appropriate response.

Over the long haul

Internal controls require constant attention to keep up with business and regulatory developments. Here are some tips for sustaining a strong approach to internal controls over the long term:

- Make the effort to understand how business flows through the company. Commit them to writing and ensure they are kept up-to-date as the company changes
- Think of controls in a broad sense—in today's world, financial and operational controls are just the start. Think also of the mandates necessary to assure conformance with policies and procedures, regulatory compliance, and safety and soundness expectations
- Relentlessly test the strength of the control system
- Implement a formal escalation protocol so that employees know what to do when something goes wrong

In the end, internal controls have to be linked to *action*. When controls determine that a process is veering off course, is the organization prepared to act—or is it simply identifying a problem to check a box? A truly sustainable approach to internal controls targets underlying problems, not just symptoms.

Process and control mapping, testing, and reporting can be a laborious effort, but rewards can be plentiful. Those who can detect weaknesses in the system earlier are likely to have a much greater chance of preventing or mitigating problems before they have a chance to inflict major damage. If the importance of controls and their management is emphasized as part of the organization's culture, the effort tends to become easier over time.

Measuring, monitoring, and reporting

The ability to measure, monitor, and report risk (MM&R) is critical to the effective management of a bank. It assists organizations to understand the risks being taken, mitigate them to the extent possible, price them appropriately, and detect adverse developments on a timely basis. It is the netting that holds the risk governance process together. Not surprising, then, that significant effort is being expended by the financial services industry to raise the game on MM&R. With a strong MM&R process, prospects of achieving a strong overall risk management program are likely to be considerably increased.

MM&R can be a challenge for banks, particularly those that already have robust acquisition strategies. Such merger and acquisition (M&A) activities can result in multiple changes to systems and technologies, leaving the new company with a sometimes-random collection of technology that can be redundant, poorly integrated, and outdated. In addition, MM&R can sometimes get lost in the shuffle as banks tend to focus primarily on front-end operations. As banks continue to incorporate risk into their strategy, they should consider increasing expenditures to update data systems. Regardless of the cause, many organizations appear to be working harder to gather the right information, verify its accuracy, and generate it in a timely manner using incompatible, disparate systems.

Address the data challenge

Many banks are being pressed by many sources to provide more data. Regulatory stress tests require organizations to deliver enormous amounts of information in ways most systems have not been configured to accommodate. Enhanced Securities and Exchange Commission and FRY-93 reporting pose different data demands. New expectations on counterparty limits, data aggregation, consumer complaints, and systemic risk reporting add to the burden of fragile information infrastructure. All this, before an organization takes into consideration its own internal desires regarding risk measurement and reporting.

Not surprising, then, that many banks have major initiatives underway to create a more robust information framework. At larger banks, gap analyses are being conducted to determine where inefficiencies or faults exist and action plans are being developed to address them.

Other efforts focus on:

- Creating data warehouses in which cleansed, consistent information is housed
- Creating data marts to provide parochial information to end users
- Enhancing data aggregation capabilities that span geographies and legal entities.

Formal governance processes are being put into place to ensure data content has common nomenclature, integrity, and consistency. Generally, a data czar is appointed to oversee governance and to represent the collective interests of all involved. Once the data framework is in place, the ability to monitor, measure, and report is likely to become much easier.

Determine quantitative measures

Many banks are utilizing revitalized technology to strengthen their risk monitoring capabilities. Not the least of these would include implementation and enforcement of the risk appetite. The appetite is the board's statement of comfort regarding how much risk the bank can take. It is up to management to determine the critical metrics and reporting requirements that ensure the business undertaken conforms to the appetite. To help do so, banks are utilizing wide nets of key risk indicators (KRIs) and key performance indicators (KPIs) to monitor all manner of risks. Sarbanes-Oxley controls, operational controls, policies and procedures, compliance requirements, and safety and soundness mandates all lend themselves to quantitative monitoring. Similarly, functional risk categories such as credit, market, operational, liquidity, and capital adequacy can be continuously monitored via KRIs and KPIs.

Modeling provides the opportunity to measure risks. Whether via stress testing, economic capital, value-at-risk, earnings-at-risk, probabilities of default and loss given default, or a panoply of other models, management may obtain valuable indicators as to where risk may be headed. If done properly, management may gain the opportunity to peer into the future via its models. If the risks appear uncomfortable, this measurement and modeling may provide sufficient lead time to act in a meaningful manner.

[3] "Consolidated Financial Statements for Holding Companies—FR Y-9C," Board of Governors of the Federal Reserve System, http://federalreserve.gov/apps/reportforms/reportdetail.aspx?sOoYJ+5BzDal8cbqnRxZRg==.

Powered by improving data quality and modeling capabilities, stress testing has leapt to the fore as an important risk management tool. Stress testing may enable banks to take today's balance sheet and/or business forecasts and "see what the future holds" under a variety of scenarios. Whether it is measuring capital or liquidity adequacy, stress testing helps an organization to forecast differing potential outcomes. If the stressed results are undesirable, management may be able to do something about it while a market still exists to do so. Those who view stress testing as a regulatory exercise may be missing the opportunity to work proactively and guide their business thoughtfully in the future.

Consider qualitative measures, too

In addition to quantitative measurement and monitoring of risk, the industry is deploying a variety of qualitative measures. Risk committees at both the board and management levels not only look at quantitative data, but increasingly spend time trying to "peer around the corner" to anticipate threats that may not have manifested themselves numerically. These "what-if" exercises challenge participants to think about the consequences of potential internal and external threats should they come to fruition. Often the dialogue is primed by analyzing the top threats to the company, which are gathered via a robust, organization-wide, self-assessment process.

Self-assessment programs are gaining significant traction as a vehicle to monitor and measure risks. The framework of the assessment is typically developed by the risk organization. Risk management also aggregates the end results and summarizes them for executive management and the board. Content, however, is generally provided by those closest to the risks—the risk takers/owners. Utilizing frontline personnel to generate the self-assessments fosters greater risk awareness and ownership among them. Some banks even require the business manager to certify the assessment. In so doing, the manager states the assessment is a fair representation of the risks within his/her area of responsibility, and opines as to the strength and efficacy of controls in place to manage them.

Efficient communication of risk information can be critical to effectively managing the organization. To do their jobs, senior management and directors need management information systems (MIS) that are concise, timely, understandable, and actionable. It is incumbent, then, on those who produce such information to ensure it comports with such objectives. A 300-page report to the board's risk committee, prepared in the spirit of keeping the members informed, probably achieves the opposite effect. "Too much information is no information at all" is how a former chair of a risk committee described it. Many organizations are now reassessing the nature and content of their risk MIS both from the size and scope perspective.

Over the long haul

Effective monitoring, measuring, and reporting of risk is front and center in the quest to attain strong risk management. System enhancements are often required and smart processes, such as metric monitoring and self-assessments, should be in place. Risk models, including stress testing, can and should be utilized to forecast threats, with action plans put in place when the modeled outcome appears undesirable. Both quantitative and qualitative efforts can be utilized to achieve a holistic view of a bank's risk profile. Risk MIS needs to be user-friendly and actionable. Achieving the utopian state with regard to monitoring, measuring, and reporting of risk is not easy, but the rewards can be great.

It all starts with a plan

There's a good chance that many of the actions, ideas, and strategies identified here are already in place in your organization. How are they linked? Are different parts of the bank at different stages of maturity when it comes to these elements? Where are the gaps between what the organization is doing today, and what it *should* be doing? Without good answers to questions like these, your organization may never achieve a "strong" rating from regulators.

While some of these activities may seem daunting, the simple act of creating a plan may make all the difference. In this document, we've outlined the core components to consider in your plan. How you assemble them is your decision, based on where the organization is today and its goals for the future.

If you would like our assistance in developing such a plan, or are just looking to have a conversation, we're ready to listen.

Contacts

Deborah Parker Bailey
Managing Director
Deloitte & Touche LLP
+1 212 436 4279
dbailey@deloitte.com

Kevin Blakely
Senior Advisor
Deloitte & Touche LLP
+1 330 807 4202
kblakely@deloitte.com

Kevin Burns
Director
Deloitte & Touche LLP
+1 312 486 3609
keburns@deloitte.com

Irena Gecas-McCarthy
Principal
Deloitte & Touche LLP
+1 212 436 5316
igecasmccarthy@deloitte.com

Tom Rollauer
Executive Director
Center for Regulatory Strategies
Deloitte & Touche LLP
+1 212 436 4802
trollauer@deloitte.com

The Center wishes to thank the following additional Deloitte professionals for their contributions and support:

Governance

Henry Baltazar
Senior Manger
Deloitte & Touche LLP

Anne Leigh Blythe
Manager
Deloitte & Touche LLP

Yvette Li
Senior Consultant
Deloitte & Touche LLP

Chamrong Nguon
Senior Consultant
Deloitte & Touche LLP

Sara Oropesa
Manager
Deloitte & Touche LLP

David Rowland
Manager
Deloitte & Touche LLP

Jyoti Vazirani
Director
Deloitte & Touche LLP

Internal controls

Cheila Fernandez
Manager
Deloitte & Touche LLP

Bob Frame
Manager
Deloitte & Touche LLP

Madeline Morris
Director
Deloitte & Touche LLP

Gina Primeaux
Principal
Deloitte & Touche LLP

Jeffrey Puente
Senior Manager
Deloitte & Touche LLP

Timothy Ward
Director
Deloitte & Touche LLP

Policies and procedures

Emily Carney
Consultant
Deloitte & Touche LLP

Bob Kidd
Senior Consultant
Deloitte & Touche LLP

Jared Li
Senior Consultant
Deloitte & Touche LLP

Jeanne-marie Smith
Manager
Deloitte & Touche LLP

Ed Sullivan
Principal
Deloitte & Touche LLP

Simri Van Rooyen
Senior Consultant
Deloitte & Touche LLP

Manav Vasan
Manager
Deloitte & Touche LLP

Diane Zielinski
Consultant
Deloitte & Touche LLP

Measure, monitor, and report

Adrian Alisie
Manager
Deloitte & Touche LLP

Samantha Bonder
Senior Consultant
Deloitte & Touche LLP

Eric Bottom
Senior Manager
Deloitte & Touche LLP

Minhee Choi
Senior Consultant
Deloitte & Touche LLP

Douglas Hallett
Senior Manager
Deloitte & Touche LLP

Derek Hodgdon
Manager
Deloitte & Touche LLP

Amanda Lenok
Senior Consultant
Deloitte & Touche LLP

Other contributors

Cara Buerger
Senior Designer
Deloitte Services LP

Kristy Coviello
Senior Manager
Deloitte Services LP

Susan Jackson
Senior Manager
Deloitte & Touche LLP

Beth Leesemann
Lead Marketing Specialist
Deloitte Services LP

Seth Raskin
Marketing Manager
Deloitte Services LP

DCRS
Deloitte Center
for Regulatory Strategies

About the Deloitte Center for Regulatory Strategies
The Deloitte Center for Regulatory Strategies provides valuable insight to help organizations in the financial services, health care, life sciences, and energy industries keep abreast of emerging regulatory and compliance requirements, regulatory implementation leading practices, and other regulatory trends. Home to a team of experienced executives, former regulators, and Deloitte professionals with extensive experience solving complex regulatory issues, the Center exists to bring relevant information and specialized perspectives to our clients through a range of media including thought leadership, research, forums, webcasts, and events.

www.deloitte.com/us/centerregulatorystrategies