Stronger: OCC’s heightened expectations
Enhancing risk management and driving growth
In the financial services industry, the attention given to managing and controlling risk has been constant and continues to be elevated—especially since the financial crisis. Today there is a greater focus on enterprise-wide risk and compliance management, which has primarily been driven by the U.S. and European regulators. The message to institutions and their boards is that large banks are expected to establish “strong” risk management practices, as noted in the recent stream of regulatory issuances and speeches, supervisory communications, and formal enforcement actions. Regulatory expectations will likely remain high and those institutions not in compliance may be subject to adverse consequences.

The latest guidance issued by the Office of the Comptroller of the Currency (OCC) continues this trend of greater regulatory involvement. The OCC has formalized its “heightened expectations” for risk management and governance through its proposed minimum standards for the design and implementation of a Risk Governance Framework and the role of the board of directors in administering its oversight. These proposed standards apply to large national banks and are consistent with the principles embedded in the Federal Reserve’s expectations for large bank holding companies. The stakes have been raised.

With these proposed minimum standards, the OCC has established a mandatory base upon which institutions are expected to build their risk governance frameworks. However, institutions may need to go well beyond what is explicitly stated in these standards, as we are observing through our work with institutions. These serve as the starting point and can be considered as the minimum standards of expectations. Regulators will likely continue to raise the bar, and their expectations, as historical experience has shown.

Regulators expect the whole to be greater than the sum of its parts when it comes to risk management. The Federal Reserve is focused on the enterprise-wide consolidated view of the organization, while the OCC expects the bank to evaluate and manage risk separate from its parent company to “protect the national bank charter.” Both views are aligned and have the fundamental requirement of stronger risk management and governance.


Which banks are affected?

The proposed Guidelines would apply to banks (insured national banks, insured federal savings associations and insured federal branches of foreign banks) with total consolidated assets of at least $50 billion, as well as to any others that the OCC may deem appropriate. We anticipate that the expectations held by the other regulatory agencies are in alignment with the OCC guidelines. Institutions with consolidated assets between $10–50 billion may wish to review the guidelines for purposes of informing their risk management framework.

A bank may use its parent company’s risk governance framework if the framework meets the minimum standards, the risk profiles of the parent and the Bank are substantially the same, and a documented assessment demonstrates that the risk profiles are substantially the same. Risk profiles may be considered substantially the same when the bank holds 95% or more of the company’s consolidated assets, managed assets, and off-balance sheet exposures.
Institutions should develop a sweeping, holistic view of their risk-related capabilities in order to become “strong.” As a result, they should be equally prepared to manage existing risks as to detect and control emerging risks. Regulators are looking for the ability to proactively identify and address risks. These proposed minimum standards give the industry a clearer picture of what regulators mean by “strong” risk management.

It is worth noting that this is expected to be a process that evolves and unfolds over time—and one that is truly embedded in the institution. Those that plan on sprinting to meet new requirements, then waiting until the next round of guidance, may find themselves falling behind the curve. Continuous improvement is the model that institutions should look to adopt in this new world of risk management, constantly assessing their progress, addressing shortcomings, and bringing risk management practices in tighter alignment with overarching business strategy.

Sound daunting? It doesn’t have to be. For starters, many organizations have already started moving in the direction indicated by the OCC and the Federal Reserve. But even if your institution is already on the path, these standards will likely require additional effort in order to remain compliant. We have identified six possible takeaways in areas that we believe may be of special interest to boards of directors and executives responsible for leading their institutions’ governance- and risk-related initiatives. In our view, the six areas deserving special focus are:

• Risk and strategy alignment
• Board responsibilities
• Three lines of defense
• Internal audit
• Risk data and infrastructure
• Talent and culture

On the following pages, you will find our thoughts on the implications of new guidelines on each of these areas—as well as actions your institution can begin taking in order to not only comply with them, but to use them as a springboard to growth.

**Enforcement: What’s at stake**

- Due to 12 CFR, Part 30, the OCC now has wide latitude to determine whether individual institutions are required to submit a **formal compliance plan**, as part of its proposed “enforceable guidelines” for remediation efforts.
- Institutions that fail to comply could be subject to **order issuance** and **civil money penalties**.

---

**Risk Governance Framework: An Overview**

A bank should establish and implement a formal written risk governance framework (“Framework”) for managing and controlling risk-taking activities. The Framework should be designed by independent risk management and approved by the board or the board’s risk committee. It should also be reviewed at least annually or as often as needed to address changes in the bank’s risk profile or leading industry risk management practices.

The Framework should cover risks to the bank’s earnings, capital, liquidity and reputation arising from all activities, including risks associated with third-party relationships. Relevant risk categories could include: credit, interest rate, liquidity, price, operational, compliance, strategic, and reputational.

The Framework should also include the following elements:

- Board oversight
- Clearly defined roles and responsibilities
- Strategic plan and risk management integration
- Risk appetite statement
- Risk policies, processes and procedures
- Risk limits, metrics and analytics
- Risk data aggregation, monitoring and reporting
- Talent development, recruitment and retention
- Performance management and incentive compensation
- Succession planning
- Risk communication
- Risk culture
1. Risk in tight alignment with strategy

From the regulators’ perspective, managing risk requires addressing all risk in the organization and ensuring that appropriate controls are established to mitigate these risks. Regulators expect institutions to know how to manage risk in a way that dovetails with their overarching corporate strategies. Since corporate strategies are constantly changing and evolving, regulators are also seeking evidence that an institution’s risk management strategy is flexible enough to adapt and change along with the core business strategy.

The risk appetite statement has a big role to play in this environment, since it is one of the key elements in the risk management framework. In fact, this statement effectively functions as the overarching guide—and should be directly tied into the strategic plan. Effective statements clearly spell out which risks are acceptable to the institution, and are supported by risk limits, risk monitoring, analytics and metrics. Meanwhile, the Risk Management function should be delivering data-supported insights to the board and management team on key risks the institution is facing at any given moment. The information presented should not only reflect the current environment, but also be forward looking.

What now?

In some large banks, the risk appetite statement and the business strategy may be managed in silos. They are often conceived of separately, by different groups, at different times—and as a result, the risk appetite statement may not account for all of the current strategies being pursued by the business. Likewise, the business strategy might not be consistent with the risk appetite statement.

Just as important, the risk appetite statement may not be supported by the governance, processes, monitoring capabilities, and controls that give it the power to actually work throughout the organization. We call the related and supporting effort the “risk appetite framework,” and it is the context in which any risk appetite statement should be considered. In light of the recently proposed guidelines, we have identified some immediate actions that risk leaders might take in order to bring their risk appetite more in line with strategy—and begin building out a framework to support the risk appetite statement itself.

Review, strengthen and document links to the strategic plan

What strategy is your bank pursuing today in order to grow? Are you ramping up marketing efforts? Acquiring new branches? Offering more aggressive pricing on rates to consumers? Strategies such as these can introduce new types and levels of risk to the organization—and if they are developed without the risk appetite in mind, the bank may not have a complete understanding of the risks it faces, much less whether those risks run afoul of its own risk appetite. Understanding the risk implications as a result of new strategies and/or business activities will help improve the alignment of risk and strategy.

Account for additional types of risk

Many current risk appetite statements have a more narrow focus that may not include reputational, strategic or operational risks. While these risk categories may be more difficult to define and measure, they can be equally important—and they are facing more regulatory scrutiny. In addition, emerging risks need to be identified, monitored and aligned with the risk appetite statement, as appropriate. For example, as banks move into new products or businesses, these activities may lead to new or emerging risks. Such activity should be evaluated within the context of the risk appetite set by the Board. The risk appetite statement may also need to be updated to address such risks that may have previously escaped notice.

Double down on data

Without the systems in place to monitor and report risk using reliable data, it is difficult for the risk appetite statement to have the impact regulators are seeking. Data is an important part of the overall risk appetite framework. Start by asking those responsible for risk whether they have the data-driven insights they need to manage risk as dictated by the risk appetite statement and its system of cascading limits. Then, work with technology leaders and others to close the gap between the data they have today and what they may need to make more informed risk decisions and manage risk more effectively.
2. Direct impact on the board

While the issue of risk has always been a board-level concern, the new guidelines amplify its importance to board members. Institutions need to consider whether any changes are necessary to ensure the board has the capacity to provide effective, independent oversight of management. The proposed OCC guidance requires at least two independent directors, an expectation likely achieved by publicly traded companies already. Further, there will be a high degree of regulatory focus on the level of independent oversight by the Board, taking into consideration an institution’s size, complexity and risk profile.

Even if a formal restructuring is not required, a fundamental reorientation of the board with respect to risk issues may be unavoidable. Board members need to be both knowledgeable and hold management accountable for controlling and managing risk—and to offer “credible” challenges to the management team both as part of the regular reporting process as well as when their efforts are falling short. This requires a deep understanding of the risks underlying the bank’s activities today, not to mention a clear understanding of the bank’s risk appetite.

There is a considerable administrative component to the board’s role as it relates to risk. Board members will likely need more documentation to support management’s assertions about risks and how they’re being managed. The reporting that is provided to them will need to be able to highlight the current state of risk and emerging themes in ways that is understandable. Emerging industry practice is focused on quality data that is supported by sufficient analysis and synthesis to make it relevant and transparent. Board members are expected to challenge management in greater depth. This may require enhanced training, more meetings, better information, and a greater command of the specific details of risk management than they have today.

What now?

A lot of this may sound familiar to senior executives and board members of large banks, many of which already have at least two independent board members, for example. As a result, it may be tempting to assume that the board is already moving in the right direction. But these guidelines bring a new level of detail to board-level issues, and may necessitate a gap analysis for institutions to ensure compliance—and meet the spirit of the regulators’ expectations. Here are three ways many institutions may find it most useful to start.

Launch a board self-assessment

Where is the board already doing the right things when it comes to the OCC’s guidance? Where is it falling short? Given the new level of detail provided by these guidelines, the job of conducting a self-assessment can be fairly straightforward. Without such an assessment, the board may be at risk of investing its time in the wrong activities.

Refresh board training

Most boards have training—but is it sufficient? Does it follow regular training protocols? Does the current board training regimen address the regulatory landscape, industry practices in risk management, and the bank’s own risk processes and approaches based on the bank’s businesses? Are board members comfortable with these new expectations for governance and oversight? For example, the board is asked to sign off or attest to more regulatory filings than in the past and do they understand key regulatory requirements, such as stress testing, capital plans, and recovery and resolution plans.

It is beneficial to review training programs, content and calendars to facilitate alignment with what is happening in the industry and at the bank. If this has not yet occurred, consider moving it to the top of the agenda and establishing an appropriate training framework to ensure the board is properly educated on relevant topics. These new guidelines mean it is a good time for a refresh. This is the time to act—training can help the board move ahead comfortably with their increased level of responsibilities.

If you’re going to be large, and you’re going to be complex, we expect more from you.²

—Thomas Curry, Comptroller of the Currency

² “OCC Ratchets Up Pressure on Big Banks” by Ryan Tracy and Stephanie Armour, Wall Street Journal, January 16, 2014
Reevaluate internal reporting requirements

These guidelines require a board that is even more active and informed when it comes to risk issues. At the same time, board members don’t operate at the front lines of the business—they rely on senior executives and a network of reporting processes to remain informed about the risk environment. What if the old ways of reporting don’t match up to new requirements? There are a number of signs that may indicate problems. For example, if the board doesn’t hear about risk management breaches, or if board members have never observed disagreements between senior executives about risks (indicating a healthy environment of challenges and attention to risk issues), the board may be operating in the dark.

Documentation can also tell the story—Is risk considered a serious agenda item? Do meeting minutes reflect discussions around risk management? Regulators have stepped up their expectations on this topic, encouraging institutions to document discussions around risk. Expect regulators to also focus on the number of Risk Committee meetings and their duration, the quality of information provided, and active committee membership. All of these can demonstrate the level of interaction and presence of effective challenge and the importance of risk. Finally, in the wake of challenges, it is beneficial to document evidence that management is working through the insights uncovered as a result of these challenges at the transaction, portfolio, or process/control level.

3. Three lines of defense:
In the spotlight

Institutions are already familiar with the “three lines of defense” governance framework for risk and compliance management, which employs front line units, Risk Management, and Internal Audit. There is also wide recognition that all three lines of defense are responsible for managing risk and that together, an appropriate system to control risk taking can be established. But how strong is their ability to effectively implement this risk and compliance framework? Are they able to clearly determine which units have which responsibilities when it comes to addressing risk? These considerations can make the difference between a “three lines” approach that delivers the desired results, and one that falls short. The new guidelines place added pressure on institutions to clearly establish roles and responsibilities within the three lines of defense.

Quality assurance is another big part of these new guidelines. Each line of defense benefits from its own process that enhances quality assurance and control effectiveness. This process can serve as a feedback loop from analyzing lessons learned and root causes when things go wrong. What’s more, such processes enable the respective lines to self-assess and improve over time, based on these insights.

This raises some fundamental questions for institutions regarding organizational design and operating models. When considering the three lines of defense, what is appropriate to handle at the headquarters level, and what should be addressed by the business units? Institutions with a decentralized risk organization may find it more difficult to meet these new requirements. As regulators have raised their expectations over the past several years, they seem to prefer a structure that facilitates a clear line of sight into and across all business and functional units.
What now?
In many ways, the three lines of defense are the foundation of the OCC’s guidelines—and as a result, they face more scrutiny than ever. Structure, accountabilities, roles and responsibilities are the focus of much of the OCC’s attention. For example, for the first time ever, the OCC has formally defined the expectations for business units as the first line of defense as front line managers of risk. These units create risks for the bank, “own” these risks associated with their activities, and perform ongoing risk assessments to determine if additional actions are necessary to strengthen risk management practices or reduce risk. Meanwhile, the second line—the independent risk management function—takes on a more prominent role in the wake of these guidelines, and should be able to clearly demonstrate its independence and oversight in monitoring and testing of the front line units on a regular basis. Their focus is on identifying, measuring, monitoring and controlling aggregate risks, as well as establishing an enterprise framework and policy for the organization. Similarly, Internal Audit is given new responsibilities to review and validate the risk governance framework on at least an annual basis.

Given the intense scrutiny focused on the three lines of defense, a gap assessment is likely to be the first step for many institutions. Here are some top-line considerations that can be addressed by any assessment.

Clarify roles and responsibilities in the organization
Too often, the responsibilities for risk ownership, management, control, oversight and assurance are not clearly understood within the institution. This problem becomes more acute when a complex and diverse business model or a global footprint exists. Clarifying who is accountable for which decisions and actions can go a long way to establish a stronger three lines of defense model.

Deepen risk management in the front-line business units
How deep does ownership for risk management really reach? If it stops with top executives, the first line of defense may be the weakest link. Both business unit-level executive leadership and many rank-and-file employees need to better understand the relationship between the risk appetite statement, the system of limits, the risk framework and the work they do every day. An assessment can identify just how deep that understanding goes.

Strengthen the independent risk management and control functions
The independence of risk management and control functions can be reinforced through their active monitoring and testing of businesses’ risk processes and controls, compliance with policies, and risk appetite and risk limits. These control functions should have input on the development of plans related to strategy, capital, and liquidity on behalf of the institution. In addition, it is essential that the independent risk management and control functions be able to identify, aggregate, and report on its view of risk to the board or risk committee. The leaders of risk management and control functions are expected to have adequate stature and authority to command a “seat at the table,” as well as report to and have direct access to the board and board committees. Fundamental to effective control functions will be to further clarify roles and responsibilities for the second line.

Elevate the stature and brand of Internal Audit
Does Internal Audit have the authority and stature that it needs to make a difference in the organization? Some would say that its clout is wrapped up in the skills and capabilities its people bring to the job every day. Developing a better understanding of existing resources and competencies is a good place to start, especially given the proposed requirement to assess the risk governance framework. Focus can then turn to other areas to enhance Internal Audit’s brand and stature.
4. Pushing Internal Audit to the next level

Under the new proposed guidelines, Internal Audit will be responsible for reviewing the institution’s framework for risk management and ensuring that it is aligned with leading industry practices. For many, this will require capabilities, skills and methodologies that may not have been required in the past, giving Internal Audit the capacity to be more proactive and forward-looking. Active involvement in industry groups, regulatory conferences, peer networking and monitoring of trade journals are examples of methods used to gain this industry insight.

In short, these guidelines require Internal Audit to step up its game. Quality assurance and continuous improvement will rise in importance for Internal Audit teams, all in service to a vision of being more proactive. What does external data suggest about the risks we might be facing today? Which emerging risks should we be preparing for today? Which aren’t even on our radar—but should be? These are the types of questions that Internal Audit may need to address. The rising importance of Internal Audit as a component of risk management will likely enhance their ongoing regard by the institution itself. Further, an overall rating of “strong” risk management cannot be achieved until the Internal Audit function is rated “strong.”

What now?
As previously noted, the “three lines of defense” model is a focal point of the OCC’s new guidelines. It comes as no surprise that Internal Audit, the third line of defense, faces a new level of scrutiny. Institutions may benefit by taking a series of actions to strengthen and enhance existing capabilities, and set the stage for the bigger role that Internal Audit is expected to play in risk management. Here are some things to consider.

Improve the Internal Audit brand
The Internal Audit function is only as strong as its people, which means that training, development and retention activities become more important. But there is another factor to consider here. In the past, Internal Audit staff members may not have been given the credibility and stature they deserve in the organization. Today, there is little question that the people who make up Internal Audit are viewed by the OCC as a central asset in the campaign to effectively report on risk management. Here are some things to consider.

Gear up for the risk framework assessment
The new guidelines are clear: Internal Audit must conduct an independent assessment of the risk framework at least once a year. In a number of institutions, this will require a range of capabilities that are not current strengths within Internal Audit. Internal Audit members can contribute by bringing an understanding of regulatory standards and leading industry practices, key expectations regarding organizational structures, risk appetite statements, rules and responsibilities, and much more. If that knowledge is not currently held within Internal Audit, it may be time to look for additional talent, pursue new training and development, or consider outside help.

Establish or strengthen the quality assurance function
Every Internal Audit organization should have a quality assurance function; however as the stature of Internal Audit grows, so do the stakes. Quality assurance can help ensure that Internal Audit delivers at a consistently high level—and keeps improving. Institutions can consider measuring its current function against the proposed standards and proactively address potential enhancements.

Absent—but not to be ignored
A close review of the newly issued proposed guidelines will reveal that two areas go unmentioned. But just because they weren’t explicitly mentioned, these control functions should not be ignored:

Compliance
The Corporate Compliance function is considered to be a risk function and therefore, an independent, second line of defense subject to the considerations outlined in the guidelines. Similar to the Risk Management function, Corporate Compliance establishes the enterprise-wide compliance program and policy, and focuses on monitoring, testing, and reporting of compliance risk on an aggregated basis. Managing compliance risk, like the other risk types, is the responsibility of all three lines of defense.

Credit review
This function is viewed as a third line of defense, and while it is not explicitly called out, it remains highly relevant. Regulators are looking for attributes similar to those expected of Internal Audit: Credit review should have independence and stature within the organization, should report to the board or the board’s Risk or Audit Committee, and should possess the skills, knowledge, and programmatic depth to effectively identify and detect risks.
5. Required data and infrastructure changes

Considering all the changes introduced by the new guidelines, it may be clear to those at many institutions that their infrastructure likely will have to evolve quickly, as well. For some institutions, their risk infrastructures may not be flexible or transparent enough to meet current regulatory demands, effectively monitor risks, or connect their risk portfolio to their risk appetite.

Gap analysis is a good place to start, to determine current infrastructure capabilities and identify where additional investment may be required. The infrastructure should be able to deliver varying levels of detail and aggregation—transaction-level details with portfolio-level views are the norm today. Following are several of the more important aspects to be considered:

- Aggregate risk exposures
- Concentrations of risk at the bank level, across business lines and legal entities
- Stress testing results
- Material risks
- Emerging risks
- Breaches of risk statements
- Concentration risk limits
- Front-line unit risk limits
- Capital requirements calculations
- Liquidity risk and regulatory measures

It almost goes without saying that policies, procedures and processes should be established to support risk data aggregation and reporting, appropriate to the size of the organization, its complexity and risk profile. Demonstrating the ability to aggregate risk data in a way that is accurate, complete and transparent for its senior management and the board to make informed decisions is also essential. Controls surrounding risk data should be as robust as those applied to accounting data.

What now?

Even without the proposed OCC guidelines, the twin issues of data and infrastructure already loom large over banks. After all, data has always been viewed as a major asset within banks, and the rise of big data and business analytics has only raised the stakes. So when approaching data and infrastructure in the context of these guidelines, it is important to look beyond mere compliance to larger business objectives regarding data. If compliance is the primary goal, the bank will likely miss out on opportunities to gain a competitive edge through data, even as it remains compliant. Here are some important, immediate steps to improve business insight and decision making on the way to compliance.

Set clear business goals
As with anything else worth doing in business, establishing objectives for data- and infrastructure-focused initiatives makes it more likely that the institution will reach those goals—and measure its progress along the way. Resist the temptation to merely set data and infrastructure goals to meet the requirements spelled out in the guidelines. A bank’s objectives in this area are likely more far-reaching than those required by the OCC, affecting everything from risk management to reporting and growth. Consider the OCC guidelines to be a catalyst for improvement in this business-critical area.

Foster participation across business units
Without full participation from business units, data and infrastructure efforts tend to devolve into a massive compliance exercise strung together by the risk organization, supported by a handful of willing business leaders. That is not a recipe for delivering real business value. True data-driven decision making in risk management (and throughout the business) relies on participation, adoption and adherence across business units and legal entities.

Establish a framework for data stewardship
It is one thing to collect and house data—and quite another to understand how it fits within the broader context of risk management. Effective data stewardship requires a small community of leaders who understand the real value of the data their organization is gathering, how different parts of the data picture work together, and how to make sure it serves organizational goals. Data stewardship doesn’t tend to happen on its own. A formalized framework for data stewardship that unites data users, subject matter experts, collection processes, IT systems and reporting tools may be warranted.

Don’t skimp on measurement and testing
Data management and quality are important, but shouldn’t come at the expense of measurement and testing at the back end. In fact, it’s unlikely that the institution will consistently reach long-term goals for data quality (OCC-mandated or not) without a rigorous testing and measurement apparatus in place. Are your efforts meeting the needs of regulators and your own business leaders? Look to measurement and testing to know—and to constantly refine your bank’s efforts along the way.
6. New demands on talent and risk culture

Regulators are not just looking for institutions to adhere to the letter of the guidelines. “Strong” institutions are those that embrace the spirit of risk management—they have a strong risk culture, aside from their ability to remain compliant. Having the right culture takes people with the knowledge, skills and abilities to understand the importance of risk and know how to execute in a risk-intelligent manner, especially those responsible for or who influence material risk decisions. All of which place the connected issues of hiring and retaining talent in the spotlight, with a special focus on learning, development and succession planning. This focus extends all the way to compensation—the compensation structure should account for risk issues, foster and encourage desired behaviors, and balance risk-rewards. Why all the focus on culture? A strong risk culture promotes accountability, consistency, transparency, and strategic alignment—even as risk requirements and the overall risk environment evolve through the years.

What now?

While talent management programs and culture initiatives are indicative of a well-managed organization, the OCC guidelines mandate that risk talent become a standard feature of those programs and initiatives. In light of the guidelines, bank boards and management should determine how well they are developing, attracting, and retaining talent—especially in jobs held by those responsible for overseeing risk. Corrective steps will be expected, when necessary. Notably, regulators are quick to attribute identified problems to training, hiring, or compensation shortcomings, and in some cases will point to the broader issue of a deficient risk culture. Here are some ways to help keep your institution’s culture-focused efforts on track.

Encourage dialogue and effective challenge

The OCC expects banks to possess a culture that challenges excessive risk-taking. When risk takes a back seat to other issues, some banks have learned the hard way that those risks can spread quickly, before corrective measures can be executed. In “strong” organizations, senior executives set a tone in which risk is viewed as an important cultural element. For example, the board and CEO should set the tone from the top regarding the importance of risk management and the bank’s risk management framework. This tone from the top will help empower the Chief Risk Officer to challenge anyone on the topic of risk, including business unit leaders. And employees throughout the bank should be encouraged to raise and escalate issues as they are encountered. For example, it’s no longer sufficient for the risk team to simply identify risk breaches or exceptions—they need to be empowered to press the business to change in ways that allow it to avoid repeating the same mistakes.

Conduct a skills assessment

A strong risk organization is manifested by the knowledge, skills and abilities that people bring to the job every day—all of which can be bolstered through training and hiring practices. But if your bank isn’t aware of skills gaps, it will be difficult to bridge them. That’s where an assessment can be instrumental. When conducting an assessment, don’t stop at the board and executive level—probe one or two layers down into the organization.

Develop a strong succession plan

A sustainable risk governance framework depends on adequate staffing. Attracting or developing key risk staff can be challenging, especially in today’s environment. For those without succession plans, the proposed guidance focuses on developing the next level of risk leaders throughout the institution. For those with plans, banks may benefit from a thorough evaluation of their succession plans, acknowledging that risk skills have emerged as a top requirement.

Review compensation plans

Risk should be embedded into compensation and performance management standards. An assessment can show whether a bank’s compensation and performance management programs sufficiently address risk for relevant personnel throughout the organization, including in the risk and front line units. One place to start is to determine whether incentive-based payment arrangements encourage inappropriate risks that could lead to losses.

Conduct a risk culture survey

Culture is influenced by an institution’s management systems, behavioral norms, and symbolic messages—it is the “intangible” and can be a critical component for a risk management framework. Risk culture can indicate how risk is managed within the institution and how widely risk management policies and practices have been adopted. Understanding internal attitudes, beliefs and behaviors with regard to risk offers a window into how “strong” the risk culture is. Conducting a risk culture survey can provide a baseline indication and highlight areas where levers can be pulled to strengthen risk culture.
The path to growth—through “strong” risk management

Whenever new regulatory expectations are introduced, it can be tempting to view them as a hindrance to growth and profitability. But in our view, meeting these requirements and maintaining a steady path to growth are not mutually exclusive endeavors. Strong risk management can help achieve both.

True strength is about cultivating a holistic view of the institution’s risk capabilities and potential vulnerabilities, and hewing to a strategic, top-line plan that accounts for all of the above.

An institution’s risk management strategy should be more closely aligned to corporate strategy and drive activities for managing critical areas—enterprise risk, capital, recovery and resolution planning, compliance, model risk and data. There are four fundamental components that play a central role in managing these activities—governance, policies and procedures, internal controls, and measurement, monitoring and reporting (Refer to Table 1). Along with these components, institutions should have the right talent, risk culture and effective communication to enable change and sustain a strong risk management framework.

Getting to strong is about building sustainability—with quality, repeatable processes that are continuously improved to enhance and maintain a robust risk management framework.

Table 1: Fundamental components of strong risk management
Key to building strong risk management is based on four fundamental components:

<table>
<thead>
<tr>
<th>Governance</th>
<th>Policies and procedures</th>
<th>Internal controls</th>
<th>Measure, monitor, and report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board of directors and senior management set the right “tone at the top,” establish the risk appetite, implement the appropriate operating structure and risk framework to manage and control risks, and drive a strong risk culture</td>
<td>Institutions should implement robust policies and procedures that address the complexity of their business and risk appetite as well as sound risk mitigation, including a framework for policy governance and processes to manage compliance</td>
<td>Effective internal controls should prevent and detect inappropriate/unapproved risk taking. Institutions should understand how business flows through the company, map applicable controls to process flows, test efficacy of controls, and implement formal escalation management</td>
<td>Institutions should have the ability to identify, measure, monitor and report all risks, including concentrations and risk appetite breaches. A robust IT infrastructure should be in place and provide quality, accurate and timely data that can be aggregated, modeled and stressed</td>
</tr>
</tbody>
</table>
The “how” of getting to strong begins with a strategic program and holistic view, and incorporates building an assessment framework, assessing risk culture, enhancing risk communication and learning programs, and setting direction, guidance and priorities.

While many institutions already have a multitude of ongoing and planned projects to enhance risk management, these projects too frequently are conducted in siloes—driven by a business or for a specific need. Outcomes are often uncertain and dependent on other projects, and the focus may not be on enhancing risk capabilities. Duplication and redundancies may exist, and prioritizing and allocating constrained resources and budget are a challenge.

Institutions face plenty of challenges, and will have to manage many moving parts, in the wake of the OCC’s heightened risk and governance expectations codified in the proposed minimum standards. In addition to making sure their risk and governance frameworks meet (and exceed) regulatory expectations, these institutions must continue to drive growth, performance and profitability in a constrained environment. While it may at first seem counterintuitive, we believe that by enhancing their risk capabilities and building a strong risk management framework, institutions can not only meet regulatory expectations, but can clear the path toward achieving growth and other strategic goals.
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

This publication contains general information only and is based on the experiences and research of Deloitte practitioners. Deloitte is not, by means of this publication, rendering business, financial, investment, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this publication.

Copyright © 2014 Deloitte Development LLC. All rights reserved.
Member of Deloitte Touche Tohmatsu Limited