Introduction

Transformation aptly describes what the banking industry has undergone since the financial crisis, driven primarily by a thicket of new rules and prohibitions aimed at strengthening a bank’s ability to withstand losses and stress. Regulators initially focused on increasing oversight while simultaneously reducing the amount of risk that banks may take, which pressured banks to exit entire lines of business, reduce total headcount, realign their remaining business functions and recalibrate objectives around operational efficiency. Even as banks continue to digest and respond to the recent changes to their industry, regulators are now catalyzing additional change by increasing the intensity of supervision around governance, risk management and culture.

This paper assesses regulators’ current positions on risk governance and culture in an effort to identify a risk governance framework that banks of all sizes can use as a reference. But before doing so, the paper establishes a chronology of post-crisis developments to provide the context of the current regulatory environment. A patchwork of regulatory standards, guidelines and expectations emerges that collectively provide an outline of an acceptable risk governance framework. Banks are then, for the most part, left with discretion to interpret and implement the framework in light of the complexity of their products, services, risk profile and scope of operations. A follow-up paper will seek to provide banks further help in these areas by offering prescriptive insight on the implications that an appropriate risk governance framework has on organization design and talent management.

At the outset, banks need to recognize that establishing a risk governance framework that attempts to adopt best practices is an iterative process that will require continuous upkeep in response to emerging risks, technologies and regulator concerns. In this regard, a holistic approach to governance and culture assessment, framework restructuring and business model innovation can help design and implement a risk governance framework that is both compliant and supportive of business strategies. The bottom line is that the post-crisis transformation of the banking industry is not complete; rather, it has entered a new phase.
Risk Governance has Recently Emerged as a Key Focus Of Regulators

Regulators responded to the banking crisis from 2007-2009 with financial triage, focusing initially on the quantity and quality of bank capital, which the Office of the Comptroller of the Currency (OCC) has described as the “bulwark of a safe and sound banking system.”

In 2010, the primary global standard setter for the prudential regulation of banks, the Basel Committee on Banking Supervision (Basel Committee) issued Basel III, an amended international framework to standardize bank capital measurements and regulation that revises the definition of regulatory capital and increases capital holding requirements for banking organizations. In the same year, Congress enacted a sweeping financial sector reform package that included enhanced capital requirements among numerous other provisions in the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd Frank).

From 2010 to 2012, U.S. regulators focused on establishing a U.S. version of Basel III and on implementing the changes to the banking industry required by Dodd-Frank. In conjunction, the Board of Governors of the Federal Reserve System (Federal Reserve) implemented its Comprehensive Capital Analysis and Review (CCAR) requirements under its capital plan rule, as well as Dodd-Frank Act Stress Testing (DFAST), two complementary exercises to assess whether banking organizations with total consolidated assets over $10 billion have sufficient capital to continue operations in times of economic and financial stress.

While implementing Dodd-Frank and Basel III preoccupied regulators through 2012, the OCC simultaneously established a series of “heightened expectations” for corporate oversight and governance at the largest U.S. banks, requiring them for the first time to achieve an examination rating of “strong”, as opposed to merely “satisfactory”, in their governance, audit and risk management functions. In so doing, the OCC effectively required, as part of the transition from “satisfactory” to “strong”, that the largest and most complex U.S. banks increase their level of maturity with respect to governance, risk management and compliance. In parallel, the Federal Reserve proposed rules to implement “enhanced prudential standards” required by Dodd-Frank to impose, among other requirements, measures around risk-based capital, liquidity and risk management.

On October 11, 2013, the Federal Reserve and the OCC adopted a final rule that provides an implementation timetable for the U.S. version of Basel III and additional capital reforms required by Dodd-Frank. Nearly contemporaneously, the OCC was able to sound an optimistic note in its annual report, when it observed that “In the years since the financial crisis, the OCC-supervised banks and thrifts have recovered significantly, and that trend gained momentum in the fiscal year ending on September 30, 2013.”

On March 27, 2014, the Federal Reserve System issued enhanced prudential standards for bank holding companies (“Federal Reserve’s Enhanced Prudential Standards”). Then, on September 11, 2014, the OCC issued a final rule that adopted its heightened “expectations” as enforceable “standards” for risk governance frameworks (“OCC’s Heightened Standards”).

On July 8, 2015, the trend continued when the Basel Committee issued corporate governance principles for banks (“Basel Committee’s Guidelines on Corporate Governance”).
The Federal Reserve’s Enhanced Prudential Standards and the OCC’s Heightened Standards apply by their terms only to the largest and most complex U.S. banks, which generally includes banks with total consolidated assets of at least $50 billion. Nevertheless, regulators have already displayed a willingness to apply the standards below the $50 billion threshold through reservations of authority included in the rules, supporting the view espoused by the Financial Stability Board that, while the focus of regulator attention since the financial crisis has been on the largest, systemically important financial institutions, the underlying recommendations and principles “are relevant to the supervision of financial institutions and groups more generally, including insurers, securities firms and other non bank financial institutions.”

When distilled, the foregoing chronology reveals that, under cover of an improving economy, regulators have been able to segue to a new phase in post-crisis financial reform. In this regard, though several regulators and multilateral organizations have contributed to risk governance discussions since the financial crisis, the OCC’s Heightened Standards emerge as an appropriate starting point to identify best practices, inasmuch as the OCC issued the Heightened Standards in September 2014 as part of an effort to have its standards integrated and remain consistent with previously articulated frameworks.
Standards for a Risk Governance Framework

Memorializing the Framework and Its Scope

The OCC’s Heightened Standards require that the framework be written, designed by independent risk management and approved by the board of directors or the board’s risk committee. The framework should also include delegations of authority from the board of directors to management committees and executive officers as well as risk limits for material activities.

The framework should cover at least eight categories of risks: credit risk, interest rate risk, liquidity risk, price risk, operational risk, compliance risk, strategic risk, and reputation risk. The Federal Reserve’s Enhanced Prudential Standards and the Basel Committee’s Guidelines on Corporate Governance also emphasize the enterprise-wide nature of a bank’s risk management program, regardless of how risks are categorized.

Notably absent from the named categories of risks is any mention of cyber risks, though it is worth noting that cyber risks have captured the attention of regulators and bank executives alike after large scale and coordinated denial of service attacks on banks’ websites occurred in 2012-13 and a high profile criminal hacking into J.P. Morgan’s computer system occurred in 2014.

On June 30, 2015, in a move that may foreshadow a decision by regulators to elevate cyber risks to a ninth category of risk on par with those currently named, the Federal Financial Institution Examination Council (FFIEC) released a Cybersecurity Assessment Tool that banks may use to evaluate their risks and that regulators will incorporate into their bank examinations.

To be sure, while the significance of cyber threats to banks are now widely acknowledged, those threats seem to be metastasizing in quantity and intensity at a rate faster than banks and regulators can respond.

Though the FFIEC’s Cybersecurity Assessment Tool is an attempt to change that equation, cyber risk management and cyber governance have nonetheless emerged as specialized aspects of a bank’s risk governance framework that warrant a separate and detailed examination independent of this paper’s more general discussion.

Roles, Responsibilities and Structure

The risk governance framework should adopt a “three lines of defense” structure that includes three distinct units comprised of: (1) front line units, (2) independent risk management, and (3) internal audit. Depending on the bank’s nature, size, complexity and risk profile, the specifics of the three lines may vary, though in all cases the responsibilities for each line should be well-defined and communicated.

The OCC’s Heightened Standards acknowledge that compliance needs to be more than a check-the-box exercise of placing an organizational unit into one of the three lines of defense, and that units may have many different functions, only some of which implicate one of the three lines of defense. Accordingly, the OCC’s Heightened Standards include definitions of the lines of defense that seek to assure that banks retain flexibility to identify and classify organizational units, functions, or both depending on the relationship of the unit/function to a given risk.

1. Front Line Units

A front line unit is part of the first line of a bank’s three lines of defense and comprises any organizational unit or function in a bank that is accountable for one of the named categories of risks within the framework, and that also:

- Engages in activities designed to generate revenue or reduce expenses for the bank or its parent.
• Provides operational support or servicing to any organizational unit or function within the bank for the delivery of products or services; or
• Provides technology services to any organizational unit or function covered by the risk governance framework.

Front line units should also take responsibility and be held accountable by the Chief Executive Officer (CEO) and the board of directors for appropriately assessing and effectively managing all of the risks associated with their activities. Front line units must also adhere to all applicable policies, procedures and processes established by independent risk management.

2. Independent Risk Management
Independent risk management is the second of a bank’s three lines of defense, with the responsibility of overseeing the bank’s risk-taking activities and assessing risks and issues independent of the CEO and front line units. To fulfill its duties, independent risk management should:

• Take primary responsibility and be held accountable by the CEO and the board of directors for designing the bank’s written risk governance framework commensurate with the size, complexity and risk profile of the bank;
• Identify and assess, on an ongoing basis, the bank’s material aggregate risks and use the assessments to determine if actions need to be taken to strengthen risk management or reduce risk;
• Establish and adhere to enterprise policies that include concentration of risk limits;
• Establish and adhere to procedures and processes to ensure compliance with its enterprise risk policies;
• Identify and communicate to the CEO and the board of directors or the board’s risk committee instances when independent risk management and the CEO differ in their assessment of material risks and when the CEO is not adhering to or holding front line units accountable for adhering to the risk management framework; and
• Include an independent compliance function. Independent risk management is led by a Chief Risk Officer (CRO) who is one level below the CEO in the bank’s organizational structure. A bank may have more than one CRO, which permits banks to organize around risk specific CROs. Banks with multiple CROs should have effective processes for coordinating the activities of all the independent risk management units so that they can provide an aggregated view of all risks to the CEO and board. The CRO(s) should report directly to both the CEO and the board of directors or risk committee.

To maintain further independence from front line units, independent risk management should also be structured to assure that:

• The board of directors or the board’s risk committee reviews and approves the risk governance framework;
• Each CRO has unrestricted access to the board of directors and its committees to address risks and issues identified through independent risk management activities;
• The board of directors or its risk committee approves the annual compensation and salary adjustment of each CRO; and
• No front line unit executive oversees any independent risk management unit.

3. Internal Audit
Internal audit is the third of a bank’s three lines of defense, with the responsibility of ensuring that a bank’s risk governance framework complies with applicable rules and regulations and is appropriate for the size, complexity and risk profile of the bank. In carrying out its responsibilities, internal audit should:
• Maintain a complete and current inventory of all of the bank’s material processes, product lines, services and functions, and assess the risks, including emerging risks, associated with each, which forms the basis of an audit plan;

• Establish and adhere to an audit plan that takes into account the bank’s risk profile, emerging risks, and issues, and that rates the risk presented by each front line unit, product line, service, and function and that is periodically reviewed and updated;

• Report in writing conclusions and material issues and recommendations to the board’s audit committee and, in the process, determine (a) the root cause of material issues and whether it has an impact on an organizational unit or units, and (b) the effectiveness of front line units and independent risk management in identifying and resolving issues in a timely manner;

• Establish and adhere to processes for independently assessing the design and ongoing effectiveness of the risk governance framework at least annually;

• Identify and communicate to the board’s audit committee significant instances where front line units or independent risk management are not adhering to the risk governance framework; and

• Establish a quality assurance program that ensures that internal audit’s policies, procedures and processes comply with applicable regulatory and industry guidance, are appropriate for the size, complexity and risk profile of the bank and are updated to reflect changes to internal and external risk factors, emerging risks and improvements in industry internal audit practices, and are consistently followed.

Internal audit is led by a Chief Audit Executive (CAE) who is one level below the CEO in the bank’s organizational structure. The CEO or the board’s audit committee oversees the CAE’s administrative activities. The CAE’s primary reporting line is to the board or the audit committee, which is also responsible for the CAE’s selection, and oversight of performance. The CAE should have unrestricted access to the board’s audit committee to address risks and issues identified through internal audit’s activities. No front line unit oversees internal audit.

**Strategic Plan, Risk Appetite Statement & Culture**

The CEO is responsible for developing a written strategic plan covering at least a three-year period with input from front line units, independent risk management, and internal audit. At least annually, the board of directors should evaluate and approve the strategic plan and monitor management’s efforts to implement it. The strategic plan should include: (a) a comprehensive assessment of risks that impact or could impact the bank during the covered period; (b) an overall mission statement and strategic objectives of the bank; (c) an explanation of how the bank will update the plan as necessary; and (d) a way to modify the plan to address changes in the bank’s risk profile or operating environment.

A bank should also have a comprehensive written statement that articulates its risk appetite, serves as the basis for the risk governance framework, and includes both qualitative and quantitative components (Risk Appetite Statement or RAS). The qualitative components of the RAS should describe how a bank will assess and accept risks, and describe a safe and sound risk culture, which in this context is defined as “the norms of behavior for individuals and groups within an organization that determine the collective ability to identify and understand, openly discuss and act on the organizations current and future risk.” The RAS should also be reinforced by an appropriate “tone at the top” that is critical to establishing a sound risk culture. The quantitative limits in the RAS should incorporate sound stress testing processes, as appropriate, and address the bank’s earnings, capital, and liquidity. The RAS should be developed with both top-down board leadership and bottom-up involvement.

A bank can also evaluate its risk culture using the Financial Stability Board’s (FSB’s) guidance on risk culture issued in April 2014 that identifies risk governance, risk appetite and compensation...
practices as the foundational elements of a sound risk culture. The FSB has underscored the importance of a sound risk culture by noting that “[w]eaknesses in risk culture are often considered a root cause of the global financial crisis, headline risk and compliance events.” By issuing its guidance on risk culture and suggesting a causal connection between weaknesses in culture and the financial crisis, the FSB has highlighted the inter-relationship between culture and governance and has put its imprimatur on the need to have both included in any discussion of sound banking practices.

Risk Limits, Breaches and Administration
The risk governance framework should include concentration risk limits and, as applicable, front line unit risk limits. The limits, when aggregated across front line units, should constrain excessive risk taking and prohibit the aggregated risks from exceeding the limits established in the bank's RAS.

The risk governance framework should require:

- Review and approval of the RAS by the board of directors or the board's risk committee at least annually;
- Initial communication and ongoing reinforcement of the bank's RAS throughout the bank to align all employees’ risk-taking decisions with the applicable aspects of the RAS;
- Monitoring by independent risk management of the bank's risk profile relative to its risk appetite and compliance with concentration risk limits and reporting of such monitoring to the board of directors or the board's risk committee at least quarterly and more often, as necessary, based on the size and volatility of the risks and any material change in the bank's business model, strategy, risk profile, or market conditions; and
- When necessary due to the level and type of risk, monitoring by independent risk management of the compliance of front line units with their risk limits, ongoing communication with front line units regarding adherence to the limits, and reporting any concerns to the CEO and the board of directors or the board's risk committee.

A bank should establish and adhere to processes that require front line units and independent risk management to identify breaches of the RAS, concentration risk limits, and front line unit risk limits. Banks should also establish escalation policies, based on the severity and impact of the breach, regarding when to disclose the existence of a breach to the board of directors, front line unit management, independent risk management, internal audit, and regulators. Banks should also establish policies to establish accountability for reporting and resolving breaches.

A bank’s risk governance framework should include policies and supporting processes for effectively identifying, measuring, monitoring and controlling the bank's concentrations of risk, keeping in mind that any product or service may expose a bank to multiple risks and the risks may be interdependent and that concentrations can occur on and off the balance sheet. The bank's concentration risk management policies should be appropriate for the bank's size, complexity, and risk profile.

A bank should include in its framework a set of policies, supported by appropriate procedures and processes, designed to provide risk data aggregation and reporting capabilities to support supervisory reporting requirements. Collectively, they should ensure that the bank's risk data aggregation and reporting capabilities, including its information technology infrastructure, are appropriate for its size, complexity and risk profile.

A bank’s front line units and independent risk management should incorporate at a minimum the RAS, concentration risk limits and front line unit risk limits into the bank's strategic and annual operating plans, capital stress testing and planning processes, and other processes, including decisions regarding acquisitions and divestitures, and compensation programs.

Talent Management Processes
A bank should establish and adhere to processes for human resource planning to ensure that management and employees who are responsible
for or influence material risk decisions have the knowledge, skills, and abilities to effectively identify, measure, monitor and control relevant risks. The board or an appropriate committee of the board should:

- Appoint a CEO and appoint or approve the appointment of a CAE and one or more CROs with the skills and abilities to carry out their roles and responsibilities within the risk governance framework;
- Review and approve a written talent management program that provides for development, recruitment, and succession planning regarding the CEO, CAE, CRO(s), their direct reports and potential successors; and
- Require management to assign to individuals specific responsibilities within the talent management program, and hold those individuals accountable for the program’s effectiveness

The board of directors is not required to be involved in the hiring of the CAE and CRO(s) and may rely on management to hire them. Nevertheless, the board or its risk committee should approve the appointment or removal of the CRO. The board’s audit committee should approve the appointment or removal of the CAE.

Compensation and Performance Management Programs

Incentive compensation practices at banks and other financial institutions also contributed to the financial crisis. In response, in 2010, regulators issued inter-agency guidance on incentive based compensation that became known as the Sound Incentive Compensation Policy (SICP) Guidance. In 2011, the Federal Reserve Board released the results of a horizontal survey of the compensation practices of 28 large complex banking organizations to help banks implement the SICP Guidance. Also in 2011, in an effort to comply with certain requirements of Dodd-Frank, regulators proposed incentive-based regulations that would effectively extend the SICP Guidance to include non-bank entities.

From 2011 through 2014, the proposed compensation rules remained under review as regulators struggled to reach agreement on a final version of the rules. In early 2015, incentive-pay rules received renewed media attention when regulators reportedly neared an agreement on regulations that would implement Dodd-Frank provisions requiring employees to return bonuses for egregious errors or fraud. On July 1, 2015, with the input of bank regulators presumed, the Securities Exchange Commission (SEC) proposed a rule that would require public companies, including publicly-traded banks, to adopt policies that would require executive officers to pay back incentive-based compensation that was “awarded erroneously”. The comment period on the SEC’s proposed rule ended September 14, 2015.

Against the foregoing backdrop, the OCC included compensation and performance management provisions in its Heightened Standards, while simultaneously acknowledging that “other authorities have addressed compensation issues in greater detail” and admonishing banks that “employee compensation arrangements should comply with all applicable rules and guidance.”

The compensation provisions of OCC’s Heightened Standards are adapted from the incentive compensation provisions of section 956 of Dodd-Frank, and direct a bank to establish and adhere to compensation and performance management programs that:

- Ensure the CEO, front line units, independent risk management, and internal audit adhere to an effective risk governance framework;
- Ensure front line unit compensation plans and decisions appropriately consider the level and severity of issues and concerns identified by independent risk management and internal audit, as well as the timeliness of corrective action taken to resolve issues and concerns;
- Attract and retain talent needed to design, implement and maintain an effective risk governance framework; and
• Prohibit an incentive-based payment arrangement that encourages inappropriate risks by providing excessive compensation or that could lead to material financial loss.

The Basel Committee’s Guidelines on Corporate Governance reinforces the OCC’s Heightened Standards with similar compensation provisions.\textsuperscript{70}
Standards for Boards of Directors

Standards of good governance at the board level revolve around the “tone at the top” that has already been identified as necessary to establish a culture that reinforces appropriate norms of responsible and ethical behavior. As the Basel Committee has observed, “These norms are especially critical in terms of a bank’s risk awareness, risk-taking behavior and risk management (ie the bank’s ‘risk culture’).”

Towards that end, a bank’s board of directors must assure that the bank has adopted an effective risk governance framework, and should require as part of its strategic and oversight role that management establish and implement a framework that meets best practices standards. The board must also be willing to provide a credible challenge to management’s decision-making, and should approve any significant changes to the risk governance framework and monitor compliance with the framework.

The board should actively oversee the bank’s risk-taking activities and hold management accountable for adhering to the risk governance framework. In providing active oversight, the board may rely on risk assessments and reports prepared by independent risk management and internal audit. Nevertheless, when actively overseeing management, each member of the board of directors should exercise sound, independent judgment.

To promote effective, independent oversight of management, at least two members of the board should be independent, which means that they: (1) are not, and have not been, an officer or employee of the bank or its corporate parent within the last three years; and (2) are not a member of the “immediate family” of a person who has been an “executive officer” of the bank or its corporate parent within the last three years.

The Federal Reserve’s Enhanced Prudential Standards also require the boards of publicly traded bank holding companies with total consolidated assets of $10 billion or more to establish risk committees that approve the risk-management policies of the bank’s operations and oversee the risk management framework. The risk committee must have a formal written charter approved by the board, meet at least quarterly, be chaired by an independent director and have at least one member having experience in identifying, assessing, and managing risk exposures.

FDIC rules require boards of directors of depository institutions with over $500 million in assets to establish audit committees, to hire the outside auditor, and to oversee the performance of the bank’s internal audit function. For institutions with assets over $1 billion, all of the directors on the audit committee must be independent.

Bank regulators have further recommended as part of their SICP Guidance that banking organizations that use incentive compensation to a significant extent should establish a board compensation committee that reports to the full board of directors and that has the primary responsibility for overseeing the organization’s incentive compensation programs, and that is comprised of independent directors.

The board should also establish and adhere to a formal, ongoing training program for all directors that considers the directors’ knowledge and experience and the bank’s risk profile. The training should cover (1) complex products, services, lines of business and risks affecting the bank, (2) laws, regulations, and supervisory requirements applicable to the bank, and (3) other topics identified by the board of directors.

The bank’s board of directors should also conduct an annual self-assessment that includes an evaluation of its effectiveness in meeting the standards that underlie its risk governance framework.
The Path Forward for Banks Around Risk Governance and Culture

Since the financial crisis began in mid-2007, over $100 billion in fines have been imposed on the six largest U.S. banks alone for credit and mortgage-related activity that contributed to the crisis.84 Unfortunately, the fines failed to have sufficient deterrent effect and the pattern of bad behavior continued, as exemplified by the Libor and foreign exchange rate setting scandals that involved collusive behavior that lasted into 2013.85 The fact that misbehavior was occurring at the same time as regulators were discussing with banks how to avoid future crises, while clearly appalling, also highlighted to regulators the central role that the management of human capital plays in assuring a sound banking system.86

Regulators’ heightened scrutiny of risk governance, culture and the “tone at the top” serves as notice that boards and senior management will be held accountable when a risk governance framework or culture fails to meet published standards. Regulatory oversight of these areas also lends itself to more lengthy and intrusive scrutiny due to the qualitative factors involved and the time horizons necessary to nurture self-sustaining change.

Banks can be proactive and prepare for increased oversight in these areas if they:

• Assess the cultural drivers over which management has control, including leadership and talent (the “tone at the top”), behavioral norms and traditions of individuals and groups within the organization, risk governance structure, roles and responsibilities, and people programs around incentive compensation and performance management;

• Build a recommended risk governance framework, risk appetite statement, and compensation program that uses benchmarks and the current state assessment to perform a gap analysis of what is needed to construct the desired future state organization, risk governance framework and culture;

• Deliver the recommended future state with a regulatory compliant risk governance framework, risk culture and compensation program that are part of an organization structure aligned with and supportive of the delivery of operational, customer and financial value.

Lastly, it should be self-evident that “tone at the top” is synonymous with “buy-in at the top”, meaning that, as the post-crisis transformation of the banking industry enters a new phase, the path forward must begin with senior leaders and the board of directors acknowledging a need, and then embracing and supporting efforts to develop and implement best practices in the areas of risk governance and culture. To further assist banks in this regard, a follow-up paper will be provided that offers prescriptive insight on the implications that an appropriate risk governance framework has on organization design and talent management.

2 A comprehensive review of the U.S. regulatory framework applicable to banks is beyond the scope of this paper, though a high level and non-comprehensive summary is as follows: In general, the Board of Governors of the Federal Reserve System (Federal Reserve) is the federal supervisor and regulator of all U.S. bank holding companies, including financial holding companies and state-chartered commercial banks that are members of the Federal Reserve System, as well as the U.S. operations of foreign banking organizations. *See Federal Reserve, 101st Annual Report* (2014) at 49. The Office of the Comptroller of the Currency (OCC) is the primary federal regulator for national banks. *See OCC Guidelines Establishing Heightened Standards*, 79 Fed. Reg. 54518, 54518 (Sept. 11, 2014). The Federal Deposit Insurance Corporation (FDIC) is the primary federal regulator for FDIC-insured, state-chartered institutions that are not members of the Federal Reserve System. *FDIC, 2014 Annual Report* (2014) at 138. Further, in 2011, the Office of Thrift Supervision (OTS) was wound down and the regulatory authority of thrifts was divided amongst the Federal Reserve (savings & loan holding companies), the OCC (federally chartered savings and loan associations), and the FDIC (FDIC-insured state chartered savings and loan associations). Federal Reserve, Interim Final Rule, 76 Fed. Reg. 56508 (Sept 13, 2011), available at www.gpo.gov/fdsys/pkg/FR-2011-09-13/pdf/FR-2011-09-13.pdf. This paper focuses on the regulations of the Federal Reserve and the OCC because the FDIC’s rules and regulations, at least in the areas to be addressed in this paper, are normally substantially similar to those of the Federal Reserve and the OCC. The FDIC is also the primary regulator of community banks, which are largely exempted from the regulations discussed in this paper.


5 The Basel Committee is an international supervisory group consisting of banking supervisors from 28 nations, including the U.S. The U.S. bank regulators on the Basel Committee include the Board of Governors of the Federal Reserve System, the Federal Reserve Bank of New York, the OCC, and the FDIC. *See* www.bis.org/bcbs/membership.htm. The Basel Committee’s actions do not have the force of law in any jurisdiction.


10 *OCC, Annual Report Fiscal Year 2012* at 5.


17 The Federal Reserve’s Enhanced Prudential Standards implement requirements under section 165 of Dodd-Frank for bank holding companies and foreign banking organizations with total consolidated assets of $50 billion or more. Federal Reserve’s Enhanced Prudential Standards, Summary, 79 Fed. Reg. 17240, 17240. The OCC’s Heightened Standards establish minimum risk governance standards for large insured national banks, insured Federal Savings associations, and insured Federal branches of foreign banks with average total consolidated assets of $50 billion or more. OCC’s Heightened Standards, 79 Fed. Reg. at 54518. The Basel Committee’s Guidelines on Corporate Governance do not, as noted, have the force of law in any jurisdiction.


19 The Financial Stability Board (FSB) is an international body to promote financial stability formed in 2009 as the successor to a previous forum. Its member institutions include financial regulators, central banks, and finance ministries of major global economies. The U.S. member institutions of the FSB include the Federal Reserve, the U.S. Securities & Exchange Commission, and the U.S. Department of Treasury. See http://www.financialstabilityboard.org/about/ The FSB is similar to the Basel Committee in that its actions do not have the force of law in any jurisdiction.

21 OCC’s Heightened Standards, Background, 79 Fed. Reg. at 54518 n.4, 54538 n.55.

22 Id., sec. II.A.

23 Id.

24 Id., sec. II.B.


28 The FFIEC comprises the principals of the following: The Federal Reserve, FDIC, National Credit Union Administration, OCC, Consumer Financial Protection Bureau, and State Liaison Committee. See https://www.ffiec.gov/about.htm.


30 The FFIEC emphasizes that the content of its Cybersecurity Assessment Tool is consistent with its own examination handbook and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (Feb 12, 2014). Id. at 1. See also Commissioner Luis A. Aguilar, Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus, Speech at “Cyber Risks and the Boardroom” Conference (June 10, 2014), available at http://www.sec.gov/News/Speech/Detail/Speech/1370542057946.

31 The FFIEC’s Cybersecurity Assessment Tool facilitates management’s evaluation of the banking organization’s maturity level for cyber risk management and oversight, which includes assessment factors such as governance, risk management, resources, training and culture. FFIEC’s Cybersecurity Assessment Tool at 19-29. Because the FFIEC’s Cybersecurity Assessment Tool notifies banks that the assessment will be incorporated into bank examinations, regulators appear to be taking the position that the prospect of examinations will be sufficient to encourage banks to meet the standards set forth in the cybersecurity assessment.

32 OCC’s Heightened Standards, sec. II.C.

33 Basel Committee’s Guidelines on Corporate Governance at ¶39; see also OCC’s Heightened Standards, Description, reprinted in 79 Fed. Reg. at 54528.

34 OCC’s Heightened Standards, Description, reprinted in 79 Fed. Reg. at 54524. For example, the portion of a CFO’s organizational unit that is responsible for overseeing enterprise-wide expense reduction initiatives would be a front line unit, but that portion of the CFO’s group that prepares and reports the bank’s financial statements would not be a front line unit. Id.
The OCC’s Heightened Standards also provide flexibility to accommodate the situation where a risk or compliance employee is embedded in an operational unit, which some organizations identify as part of 1a/1b or 2a/2b lines of defense depending on the capacity and compensation arrangements of the employee.

The OCC’s Heightened Standards also address how the standards apply to a bank with a corporate parent, namely a bank holding company. For instance, the OCC’s Heightened Standards address when a bank may use its corporate parent’s risk governance framework in its entirety, without modification. Id. For simplicity, this paper excludes from the scope of its discussion when a bank may adopt the risk governance framework of its corporate parent in whole or part.

For simplicity, this paper excludes from the scope of its discussion when a bank may adopt the risk governance framework of its corporate parent in whole or part.

See also Basel Committee’s Guidelines on Corporate Governance, Principle 6 at 25 (“Banks should have an effective independent risk management function, under the direction of a chief risk officer (CRO), with sufficient stature, independence, resources and access to the board.”).

See Basel Guidelines on Corporate Governance, Principle 9 (Compliance) ¶ 132 at 31 (“An independent compliance function is a key component of the bank’s second line of defence.”).

Note that the OCC’s Heightened Standards identifies the CRO as the Chief Risk Executive (CRE). CRO is used in this paper because the term is more widely used by other regulators. See also Explanation of multiple CROs in 79 Fed. Reg. 54518, 54523-24.

The requirement of dual reporting by the CRO to both the risk committee and the CEO is part of the Federal Reserve’s Enhanced Prudential Standards and is applicable by its terms to bank holding companies with assets of $50 billion or more. Id. at § 252.30. The Federal Reserve adopted the requirement over objection because it believed that dual reporting would “help the board of directors to oversee the risk-management function and may help disseminate information relevant to risk management throughout the organization” and is supported by Basel Committee guidance. Id., 79 Fed. Reg. at 17252 & n.44.

OCC’s Heightened Standards, sec. II.C.3., reprinted in 79 Fed. Reg. 54545, 54546. See also Basel Guidelines on Corporate Governance, Principle 10 (Internal Audit) ¶ 142 at 33 (“[T]he head of the internal audit function’s primary reporting line is to the board (or its audit committee) . . .”).

See also Basel Guidelines on Corporate Governance, Principle 4 (Senior Management) ¶ 93 at 20 (“Consistent with the direction given by the board, senior management should implement business strategies, risk management systems, risk culture, processes and controls for managing the risks-both financial and non-financial-to which the bank is exposed . . .”).

See also infra text and accompanying notes at p. 9, discussing the role of boards of directors in reinforcing corporate culture and the “tone at the top”.

Basel Guidelines on Corporate Governance, ¶ 37 at 10-11 (Risk appetite, management and control).

FSB’s Guidance on Risk Culture at 2-3.

Id. at 1.

OCC Heightened Standards, sec. II.F. See also Basel Guidelines on Corporate Governance, (Corporate Culture and Values) ¶¶ 29-30.
54 Id., sec. II.G.
55 Id., sec. II.H.
56 Id., sec. II.I.
57 Id., sec. II.J. See also, Basel Committee, Principles for Effective Risk Data Aggregation and Risk Reporting (Jan. 2013), Principle 1 (Governance)(“A bank’s risk data aggregation capabilities and risk reporting practices should be subject to strong governance arrangements consistent with other principles and guidance established by the Basel Committee.”) available at http://www.bis.org/publ/bcbs239.pdf.
58 Id., sec. II.K.
59 Id., sec. II.L.
61 Federal Reserve, Proposed Guidance on Sound Incentive Compensation Policies, 74 Fed. Reg. 55227, 55228 (Oct. 29, 2009) (Proposed Guidance on Sound Incentive Policies). In the Proposed Guidance on Sound Incentive Policies, the term “large, complex banking organizations” (LCBOs) was used by the Federal Reserve to describe those organizations. The Proposed Guidance on Sound Incentive Policies noted that the reviews, policies, procedures and systems used by smaller organizations on a limited basis would be substantially less extensive than those at LCBOs. Id.
62 OCC, Federal Reserve, FDIC and OTS, Guidance on Sound Incentive Compensation Policies, 75 Fed. Reg. 36395 (June 25, 2010) (Sound Incentive Compensation Policy (SICP) Guidance). In the SICP Guidance, the term Large Banking Organization (LBO), in contrast to the term LCBO, was used as that term encompasses terminology used by the other regulators. SICP Guidance, 75 Fed. Reg. 36395, 36397 & n.2.
68 Id.
69 Id., sec. II.M.
20 Basel Committee’s Guidelines on Corporate Governance, Principle 11 (Compensation) ¶147 at 34 (The remuneration of employees in control functions (risk, compliance, internal audit) “should be determined independently of any business line overseen, and performance measures should be based principally on the achievement of their own objectives so as not to compromise their independence.”) The Basel Committee also supports “clawback” provisions under which compensation can be reduced or reversed after compensation vests if new facts emerge showing that the compensation paid was based on erroneous assumptions. Id., ¶150 at 35.

21 See supra at p. 5 and text accompanying notes 46-50.


23 OCC’s Heightened Standards, sec. III.A.

24 Id., sec. III.C. See also, Basel Committee’s Guidelines on Corporate Governance, ¶33 at 10 (“As part of the overall corporate governance framework, the board is responsible for overseeing a strong risk governance framework.”).

25 Id., sec. III.D.

26 Federal Reserve’s Enhanced Prudential Standards, §252.22(a), reprinted in 79 Fed. Reg. 17315, 17317. See also, Basel Committee’s Guidelines on Corporate Governance, ¶¶71-75 at 17 (risk committee provisions).

27 Id. at §252.22(c).


29 Id. at §363.5(1), (2).

30 The Sarbanes-Oxley Act of 2002 has also imposed on publicly traded banks audit committee requirements, many of which are similar to the FDIC requirements; under Sarbanes-Oxley all of the members of the audit committee must be independent directors. Sarbanes-Oxley Act of 2002, 107 P.L. 204, 116 Stat. 745, §301.

31 See supra at p. 7-8 and notes 61-70; SICP Guidance, 75 Fed. Reg. 36395, 36413. See also Basel Committee’s Corporate Governance Principles for Banks, ¶76 at 17-18 (requiring compensation committees for systemically important banks).

32 OCC’s Heightened Standards, sec. III.E. See also, Basel Committee’s Guidelines on Corporate Governance, ¶55 at 14 (“In order to help board members acquire, maintain and enhance their knowledge and skills, and fulfill their responsibilities, the board should ensure that members participate in induction [programs] and have access to ongoing training on relevant issues which may involve internal or external resources.”)

33 Id., sec. III.F.


Contacts

David Sult  
+1.206.331.1340  
david.sult@aon.com

Khalid Ali  
+1.917.715.4904  
khalid.ali1@aon.com

Subha Chaudhuri  
+1.847.442.3522  
subha.chaudhuri.3@aonhewitt.com

Dennis J. Gaughan, CFA  
+1.808.222.6332  
dennis.gaughan@aon.com

Perry Buffet  
+1.708.278.0027  
perry.buffett@aon.com

The Aon Business Transformation Group is a unit of Aon Strategic Advisors & Transaction Solutions. Today’s ever-changing global business environment requires organizations to adapt to ever-changing market dynamics. New business realities, whether driven by rapid technological changes, aggressive industry consolidation, constraining governmental regulations, increasing cost pressures, or challenging talent dynamics, require organizations to reassess their business strategies and operating models to ensure they are structured effectively to allow them to change with the global business environment. That is where Aon’s Business Transformation group comes in – we’ve helped companies of all sizes and in various industries transform their organizations to compete effectively in the future.

About Aon Business Transformation Group

ASATS is a global practice group within Aon plc (NYSE: AON). ASATS provides innovative business transformation, risk management, human capital and insurance solutions to clients undertaking acquisitions, mergers, divestitures or organic growth strategies into new markets or territories. ASATS comprises 350+ M&A experts from a variety of backgrounds working across four continents, and offers primary capabilities on either a standalone or bundled basis to help out clients navigate all aspects of significant business transactions, including business transformation, human capital advisory, M&A solutions, transaction liability and corporate investigative solutions.

About Aon Strategic Advisors & Transaction Solutions
About Aon
Aon plc (NYSE:AON) is a leading global provider of risk management, insurance brokerage and reinsurance brokerage, and human resources solutions and outsourcing services. Through its more than 69,000 colleagues worldwide, Aon unites to empower results for clients in over 120 countries via innovative risk and people solutions. For further information on our capabilities and to learn how we empower results for clients, please visit: http://aon.mediaroom.com.

© Aon plc 2015. All rights reserved.
The information contained herein and the statements expressed are of a general nature and are not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information and use sources we consider reliable, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.