



Deloitte.

Forward look

Top regulatory trends
for 2015 in banking

Foreword

This publication is part of the Deloitte Center for Regulatory Strategies' cross-industry series on the year's top regulatory trends. This annual series provides a forward look at some of the regulatory issues we anticipate will have a significant impact on the market and our clients' businesses in the upcoming year. For 2015, we provide our regulatory perspectives on the following industries and sectors: Banking, Securities, Insurance, Energy and Resources, and Life Sciences, and Healthcare.

The issues outlined in each of the six reports will serve as a starting point for the crucial dialogue surrounding the challenges and opportunities for the upcoming year and will assist executives in staying ahead of regulatory trends and requirements. We encourage you to share this whitepaper with the senior executive team at your company. In addition, please feel free to share your questions and feedback with us at centerregstrategies@deloitte.com.

Best regards,

Tom Rollauer

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

Introduction

In 2014, banks were scrambling to comprehend a wave of new regulations triggered by Dodd-Frank and the residual effects of the economic downturn. As they enter 2015, the focus shifts to the even bigger task of implementation and compliance. Fewer new regulations are being introduced, with most designed to clarify or refine existing rules. In addition, the themes of ethics and culture are emerging frequently in the regulatory dialogue-taking place now as fines and penalties can lead to questions about the corporate cultures that led to them. With a cycle of cost-cutting likely ahead, one key question arises: Will the investments necessary to bolster a culture of compliance and ethics — and the governance programs to support that culture — face operational pressures within financial institutions?

Meanwhile, the Office of the Comptroller of the Currency (OCC) and other regulators' "heightened standards" surrounding governance and risk management stand as a distinct issue. Wrapped up in the issue is culture — culture as part of the problem and culture as part of the solution. A "strong" institution has a strong risk culture

that promotes accountability, consistency, transparency, and strategic alignment — relying on employees who possess the knowledge, skills, and abilities to understand the importance of risk and who know how to execute in a risk-intelligent manner. But developing that culture takes work — ongoing work that involves continual assessment of rule changes, internal messages, internal processes, and internal capabilities.

And as companies enter 2015, that ongoing work will touch on a host of trends affected by the regulatory environment — from concerns over credit quality and data quality to consumer protection issues and the growth in cyber threats. Other trends blending into the regulatory picture in 2015 will include governance and risk management, issues surrounding "too big to fail," the Volcker Rule, liquidity reserve requirements, anti-money laundering and sanctions activities.

In the pages that follow, this report takes a look at these trends and offers some possible steps that banking institutions can take as part of their continual efforts to meet heightened regulatory expectations.

1. Governance and risk management:

Banks must elevate their standards of governance and enterprise risk management to meet increased and more formal expectations.

The developments fueling this change include the Federal Reserve Board's (FRB) Enhanced Prudential Standards (EPS) rule, the OCC's Heightened Standards (HS) formal guidance, and the emphasis on governance in supervisory findings, such as Comprehensive Capital Analysis and Review (CCAR) determinations.

In March 2014, with the FRB issuing its final rule on EPS for large bank holding companies and foreign banking organizations, the FRB set capital and liquidity stress-testing requirements, as well as requirements for a global risk-management framework.¹ The FRB also set Risk Management Committee standards and requirements for Chief Risk Officer (CRO) qualification and reporting.

Not many months after the EPS rule, the OCC finalized HS enforceable guidelines, requiring that large banks have a robust board-approved risk-governance framework with well-defined roles and responsibilities for frontline units, for independent risk management, and for internal

audit.² They require a comprehensive risk-appetite statement, a written strategic plan, concentration-risk-management processes, strong risk data aggregation and reporting, and well-specified talent management and compensation programs.

As governance and enterprise risk management practices move forward under these codified rules and enforceable guidance, banks will need to prioritize their practices for adhering to the standards.

Banks have an opportunity, however, to get ahead of these challenges and put in place robust frameworks that can help them comply with the new rules ahead of their peers. The payoff for these institutions, in addition to the innate benefits of better risk-management practices, is that they can gain flexibility in capital actions, acquisitions, and strategic initiatives.

A prudent and strategic move for bank management would be to conduct a comprehensive assessment of risk-management frameworks and to benchmark the structure and processes against regulatory standards. From such an assessment, management could develop and put in place a well-defined remediation plan.

¹ US Federal Reserve System, "Enhanced Prudential Standards for Bank Holding Companies and Foreign Banking Organizations; Final Rule," March 27, 2014, <http://www.gpo.gov/fdsys/pkg/FR-2014-03-27/pdf/2014-05699.pdf>.

² Office of the Comptroller of the Currency, "OCC Finalizes Its Heightened Standards for Large Financial Institutions," September 2, 2014, <http://www.occ.gov/news-issuances/news-releases/2014/nr-occ-2014-117.html>.

2. Consumer protection:

The Consumer Financial Protection Bureau (CFPB) continues its supervision of large banks as it advances into nonbanks — such as nonbank auto lenders, student loan servicers, mortgage servicing firms, and debt collectors.

The CFPB's enforcement actions have included high-dollar restitution requirements and fines, such as for the marketing of credit card add-on products. It has expressed concern with reward programs,³ and continues to focus attention on banks' residential mortgage servicing with resultant restitution, fines, and operating restrictions.

The CFPB is expanding its nonbank activities into areas such as residential mortgage, private education, and payday markets. Even the Financial Stability Oversight Council (FSOC) has gotten into the mortgage servicing picture, identifying nonbank mortgage servicing as a potential emerging threat and noting the large amount of servicing rights being sold by nonbanks in recent years.

Banks and nonbanks alike face challenges in meeting CFPB expectations. Continued improvement in Compliance Management Systems (CMS) requires vigilance with a “compliant” tone coming from top leadership, as well as effective policies, procedures, training, monitoring and audit. Aggregating and reporting of customer-product-level data, including customer complaint data analytics, remains a significant challenge for many institutions. Although regulated banks are familiar with such basic requirements, many nonbanks likely won't have the same level of familiarity.

The CFPB is here to stay. Regulated entities, both bank and nonbank, can be expected to meet a standard in which systems are put in place to strengthen compliance and to identify, analyze, and remediate problems when they occur. To better manage their CMS, firms should assess and consider enhancing their compliance infrastructure—including systems, controls, and testing—in a way that is sustainable and repeatable.

³ Consumer Financial Protection Bureau, “CFPB Finds Card Act Reduced Penalty Fees and Made Credit Card Costs Clearer,” October 2, 2013, <http://www.consumerfinance.gov/newsroom/cfpb-finds-card-act-reduced-penalty-fees-and-made-credit-card-costs-clearer/>.

3. Vendor risk:

Bank regulators continue to throw a spotlight on risks associated with bank oversight of third-party providers. Major security breaches with customer information have prompted discussion for new initiatives.

Regulators continue to cite weak vendor oversight when referencing violations of consumer-protection requirements. While banks rely on outside vendors for key services, regulators hold banks responsible for problems even when the services are provided by affiliates.

With the complexity and nature of vendor services, regulators expect that bank management will devote close attention to the risks. Regulators have noted, in particular, that some vendor services have not kept pace with bank growth, with the release of new products, or with the adoption of new technology.

Regulatory actions, such as Unfair, Deceptive or Abusive Acts or Practices (UDAAP) citations, have illuminated the issue. Regulators expect that effective risk oversight of

third-party relationships involving critical activities includes written contracts and plans that outline the bank's strategy, identify the inherent risks of the activity, and detail how the bank selects, assesses, and oversees the third party.

Risk, compliance, and audit programs at many banks may have to focus more attention on regulatory compliance when it comes to consumer protection rules and vendor information security requirements. Business continuity includes not only recovery processes in the event of a service disruption, but also consideration of a bank's ability to ensure data integrity, security, and access. The Federal Financial Institutions Examination Council (FFIEC) has formed a Cybersecurity and Critical Infrastructure Working Group aimed at enhancing communication among FFIEC member agencies and building on efforts by other interagency and private-sector groups.

When it comes to vendor risk, regulators and the public will hold banks accountable for weaknesses, even when they arise via third-party vendor arrangements. Banks should consider assessing and improving their oversight of third-party providers.

4. Resolution Planning:

Systemically important financial institutions (SIFIs) will need to pay more attention to regulatory cross-border resolution protocols, gone-concern loss-absorbing capacity (GLAC), and regulatory expectations for legal structures and inter-affiliate agreements.

Recently, the FRB and the Federal Deposit Insurance Corporation (FDIC) found that several SIFIs will need to shore up their institutional resolution plans, or “living wills” in 2015.

On August 5, 2014, the FDIC and the FRB issued their feedback on second-round resolution plans from 11 large, complex global banks or “first-wave filers,” and the two bodies reached slightly different conclusions. The FRB concluded, “that the 11 banking organizations must take immediate action to improve their resolvability and reflect those improvements in their 2015 plans.” The FDIC went a bit further and “determined pursuant to section 165(d) of the Dodd-Frank Act that the plans submitted by the first-wave filers are not credible and do not facilitate an orderly resolution under the U.S. Bankruptcy Code.”⁴ In either case, the industry faces a lot of work before submitting the 2015 plans.

Beyond resolution planning, substantial work continues to strengthen the resiliency of global banks. The implementation of Basel III and Dodd-Frank-related

liquidity and capital standards is well under way. Large banks’ enterprise-governance structures are under increasing scrutiny and banks deemed as SIFIs need to demonstrate that they are resolvable. Leaders are eager for clarity from the international regulatory community regarding resolution protocols (and some agreements from G-20 on GLAC). In November, the Financial Stability Board took a big step in this direction by releasing the details of its proposal on TLAC (Total Loss-Absorbing Capacity), which aggregate GLAC debt securities and current capital eligible instruments. FSB proposed a minimum TLAC requirement of between 16% and 20% of risk weighted assets, not including required buffers such as the 2.5% capital conservation buffer and applicable surcharges. For example, a global bank with a global systemically important banks (G-SIB) surcharge of 2.5% would be required to hold TLAC of at least 21% – 25% of RWA. Liabilities counting toward TLAC would only be those that could be converted to equity during resolution without disrupting critical operations or incurring significant legal challenges. Comments on the proposal are due in February 2015.

As various resiliency-related rules reach their final form, implementation will present its own set of challenges, but it will be a key to success going forward. The reward for successful demonstration of resolvability and implementation of other resiliency-related rules will be more flexibility to pursue desired business models and types of customer services. To reach that goal, it will help to understand developing industry leading practices and to incorporate them into planning processes.

⁴ US Federal Reserve System, “Agencies Provide Feedback on Second Round Resolution Plans of “First-Wave” Filers,” August 5, 2014, <http://www.federalreserve.gov/newsevents/press/bcreg/20140805a.htm>.

5. Volcker rule:⁵

As even the "final" rule awaits possible regulatory adjustment, institutions face a significant new compliance challenge. At stake is the kind of business they do, and the systems and processes they'll need to keep track of it all.

Restricting banks from making investments that don't benefit their customers and ending their proprietary trading operations is a comparatively clear regulatory goal. But making it happen involves complexities in areas such as data, compliance, and ethics. The "Volcker Rule," which was issued on December 10, 2013, requires banking entities to demonstrate that impermissible activities are not occurring at their firms.

While smaller, less complex banks obtain some relief in the final rule, medium-sized and larger banks must implement a rigorous compliance program. Even though full compliance with the rule is not yet required, major institutions are already shedding the investments that it will eventually forbid them from holding.

As the rule is written, most banks will need to support the compliance requirements beginning July 21, 2015, but that timeline — and the requirements themselves — may yet change.

One effect of the ramp-up to Volcker compliance affects the talent pool: Many proprietary traders are leaving large

banks to work for hedge funds instead.⁶ Another effect is in collateralized loan obligations, which many banks may have to restructure or move away from to become Volcker-compliant. No matter when Volcker does take effect or what it looks like when it does, the core intent of the new rule will require firms to enhance compliance monitoring capabilities as well as more sophisticated data analysis tools.

Differences by institution size are written into the rule. Banks with no covered activities and less than \$10 billion in assets can avoid implementation altogether, while small banks with some covered activities can implement "simplified" compliance less involved than the "standard" compliance for larger, more fully involved institutions. There may be other, less explicit differences based on bank size, because larger banks already have policies, procedures, and workflows in place that they can adapt to the needs of Volcker compliance. Many medium-sized banks will have to build those capabilities from the ground up.

Once the conformance period ends on July 21, 2015, institutions with greater than \$10 billion in assets will be required to subject their compliance and their internal controls over compliance to independent testing by a qualified independent party, as defined within the Rule. Institutions that have assets that exceed \$50 billion will also be required to furnish an attestation by the firm's CEO. In anticipation of these requirements, firms are hastening to implement their compliance processes and controls to subject them to pre-compliance testing and evaluation.

⁵ Sabri Ben-Achour, "Dodd-Frank spawns software to comprehend Dodd-Frank," Marketplace Business, October 22, 2014, <http://www.marketplace.org/topics/business/dodd-frank-spawns-software-comprehend-dodd-frank>.

⁶ "Volcker Rule," Wikipedia, http://en.wikipedia.org/wiki/Volcker_Rule (accessed December 23 2014).

6. Data quality:

Data management and reporting is a perennial problem for the financial services industry. Regulatory pressure in recent years has led to some improvements, but there is still work to be done before systems and practices will be up to the new demands that stakeholders are placing on them.

The OCC's heightened standards and the finalized liquidity-coverage rule are among the developments that put a premium on timely, accurate, and aggregated data. Going forward, regulators will continue to look for banks to provide more information about capital and liquidity planning, stress testing, resolution planning, consumer protection, and Volcker Rule compliance. And as before, regulators will expect bank management to be able to aggregate and analyze data across the enterprise, giving insights that can help efficiently and effectively identify risks and overall risk exposure.

Challenges and opportunities exist to continue data governance initiatives that can help ensure efficient and effective capture, transformation, and retention of quality data. Extensive manual processes are costly, are not easily documented, and are prone to higher error rates.

Effective enterprise-risk and performance-data reporting, as well as aggregation capabilities, are critical to reducing operating inefficiencies and reliance on manual data-reporting processes — and for more fully showing evidence of ownership and effective management of risk. Organization-wide engagement will be required to achieve coordinated, efficient and broad data collection, aggregation, and management of risk/performance data and reporting.

Enterprise data governance activities require the active engagement, input, and historical perspective of the "three lines of defense" to effectively implement processes, controls, and solutions to enhance oversight and decision making that is consistent with business objectives and regulatory expectations.

7. Credit quality concerns:

A benign credit environment and rising anxiety over financial firms' earnings have contributed to a loosening of underwriting standards. Regulators have noticed this development, and they are determined to prevent irrational exuberance from returning to the credit markets.

The credit environment has turned the page from the cautious and conservative lending following the recession. Banks have become flush with liquidity and have sought to put it to work. Historically low interest rates have persisted longer than expected, compressing spreads in the process. Firms have begun to feel pressure to improve margins, enhance earnings, and increase returns on the higher level of capital they are now forced to hold. In this environment, banks have begun to move down the credit-quality spectrum to take on more risk and boost returns. For example, the volume of leveraged loans has returned to pre-crisis levels, leverage multiples have increased notably, and "covenant-lite" structures have returned to the market.

Regulators are pressuring banks to enhance their ability to

aggregate credit exposures across the firm, and leveraged lending is receiving heightened focus. Financial firms must specifically monitor their leveraged exposures and they are expected to routinely discuss exposure levels with their boards of directors. Regulators are increasingly likely to issue critical comments based on their discomfort with a firm's underwriting practices.

Regulators are also looking closer at the accuracy and effectiveness of a firm's credit-grading process. As underwriting standards deteriorate, regulators want banks to fully understand the impact of credit exposures to their balance sheets. Grading is the cornerstone in that process. An inaccurate grading scheme can possibly lead to inadequate provisions for credit losses and erroneous public reporting.

The new standards for credit governance have caused banks to raise their game on technology and aggregation capabilities and to pursue a relentless focus on grading, modeling, and stress testing. Those who fall behind industry progress run the risk of adverse selection, regulatory criticism, and increased credit losses.

The credit game has changed

Steps firms can consider now as standards change and scrutiny tightens

- Make sure your management and board of directors understand the new expectations on aggregation, portfolio stress testing, leveraged lending, and mortgage underwriting
- Discuss with regulators what they are seeing as developing practice elsewhere in the industry
- Invest in the technology necessary to enable state-of-the-art monitoring and management of credit exposures. Impose discipline over data management to enhance integrity and reliability of credit information
- Understand the assumptions used in stress testing and consider their appropriateness. Are they reasonable? Are they so extreme that no one believes their outcome? Take action when a scenario with a plausible probability produces an uncomfortable result — while the markets are still open to doing so
- Relentlessly test your grading accuracy. Reward honesty in grading, and discourage an approach that is overly optimistic or pessimistic. Remember that other key processes such as Allowance for Loan and Lease Loss adequacy, stress testing, risk modeling, and capital adequacy are all critically dependent on accurate loan grades
- Know your concentrations of credit risk: individual, product, geographic. Understand where contagion may arise when credit issues occur. Set limits for the firm and ensure that they are consistent with the risk appetite
- In keeping with the CFPB's Ability-to-Repay and Qualified Mortgage Rule, enhance underwriting practices employing the eight qualifying factors, including: verifying income, total debt and debt-to-income ratio
- Have frequent discussions with the board of directors regarding credit, including concentrations of credit, leveraged loans, portfolio trends, peer group comparisons, and stress testing results, as well as other means to maintain continuous vigilance on a risk that poses some of the greatest threats and rewards for the firm

8: Increased cyber threats:

Threat types, threat vectors, and the scope of required preparation are all growing as organizations fight to keep an edge in the cyber arms race.

The volume and number of cyber attacks shows what one corporate security chief called “exponential growth,”⁷ and the financial services industry is a top target.⁸ In this setting, banks are investing more to protect themselves, double-digit increases in security budgets expected in the next two years.⁹ And regulators are likely to continue their own focus on organizations’ ability to detect and respond to a broad array of potential incidents.

In early 2014, in adherence to a presidential executive order, the National Institute of Standards and Technology (NIST) released a preliminary Framework for Improving Critical Infrastructure Cybersecurity.¹⁰ This document offers companies guidelines and leading practices on how to thwart cyber malfeasance. Banks will continue to incorporate NIST into their existing security frameworks, which have been driven by FFIEC guidelines.

Practices and resources aren’t the only elements of the cybersecurity picture that are becoming broader. So are the targets: Smaller institutions are now facing the

adoption of security and response measures that were once needed only in larger banks and will struggle to find right balance of cost and risk posture. So are the threats: In addition to financial crime and operational disruption, add the potential threat of hactivism leading to reputational damage and destructive attacks, often brought forth by terrorists or nation-states. So are the internal implications: Governance and accountability must be changed. What was historically a purely an IT matter now extends horizontally across business, operations, technology, legal, communications, and other areas. The “KYC” (know your customer) ethic remains strong, but now “know your vendor”, “know your employee” and “know your data” are riding alongside KYC.

To protect themselves, banks need to ensure they are investing appropriately not only in preventative controls but also detective and response/resilience efforts. They need to create an overarching governance process and answer strategic decisions about what to build, buy, or outsource. They need to test their incident response and recovery processes across all parts of the organization through cyber simulation exercises. Another trend is continued participation in the public-private partnership through industry forums like Financial Services Information Sharing and Analysis Center (FS-ISAC), BITS, etc. While this practice is formally voluntary, it will likely become more common to pool threat intelligence. Organizations should prepare to participate — and prepare to make use of what they learn from each other.

⁷ Vikram Bhat and Lincy Francis Therattil, “Transforming Cybersecurity: New Approaches for an evolving threat landscape,” Deloitte LLP, 2014, <http://www2.deloitte.com/us/en/pages/financial-services/articles/dcfcs-transforming-cybersecurity.html>.

⁸ Mandiant, “Not Your Average Cybercriminal: A Look at the Diverse Threats to the Financial Services Industry, September 23, 2013, as cited in Deloitte’s infographic “Transforming cybersecurity: New approaches for an evolving threat landscape.”

⁹ Daniel Huang, Emily Glazer, and Danny Yadron, “Financial Firms Bolster Cybersecurity Budgets,” Wall Street Journal, November 17, 2014, <http://www.wsj.com/articles/financial-firms-bolster-cybersecurity-budgets-1416182536>.

¹⁰ National Institute of Standards and Technology, <http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm>.

9. Liquidity reserve requirements:

A significant new rule establishes a standard determination of liquidity and a standard means for determining high-quality liquid assets (HQLAs). That makes it easier to evaluate and compare banks — but before they can live under the new rule, most banks have a lot of work to do.

On September 3, 2014, a trio of US regulatory agencies — the OCC, the FDIC, and the FRB — issued the final version of the Liquidity Coverage Rule (LCR) that was first circulated in late 2013. The newly finalized rule specifies required ratios of HQLAs to net stressed cash outflows for the financial institutions they oversee. The rule requires banks to maintain enough HQLAs to cover fully net stressed cash outflows over a 30-day period. The final rule is substantially similar to the original notice, but it offers modest relief in certain areas, including phased implementation according to the institution's asset size.

Overall, the new LCR complements the broad array of liquidity-risk-management requirements established earlier in the year in the FRB's enhanced prudential standards rule by putting certainty around regulatory definitions of liquidity and minimum requirements. Beyond the impact of any specific requirements or changes, the rule is significant simply because it establishes a standard definition of liquidity by specifying what constitutes HQLAs, which makes it easier to evaluate and compare banks.

Under the original notice, the rule would have required daily calculation of HQLAs for all affected institutions, effective upon adoption. The final rule pushes those requirements back for some institutions based on size: Banks with more than \$250 billion in assets can perform monthly calculations until July 2016. Those over \$700 billion will have to perform daily calculations starting in July 2015.

The final rule defines banks with between \$50 billion and \$250 billion in assets as "modified LCR companies." They will be required to make the HQLA calculation only once a month. Additionally, these companies calculate coverage ratios using stressed outflow assumptions that are 30 percent lower than the assumptions applied to the largest firms. Foreign banks and nonbank SIFIs are not included in the new rules, but may soon become subject to similar rules of their own.

Many firms are finding the new daily liquid assets calculation to be operationally intense, and institutions may pursue upgrades to address the requirements. The regulators' decision to ease the timetable will help some banks, but many still face a long process to prepare for implementation.

10. Anti-money laundering:

The government continues to raise expectations on the industry's ability to know its customers — and its own ability to find nefarious activity and impose sanctions. Complying with the law in both letter and spirit is a difficult task, and expectations continue to evolve.

Anti-money laundering (AML) and Bank Secrecy Act (BSA) statutes were initially used as a tool in the war on drugs. The 9/11 attacks as well as a number of notable compliance failures by banks prompted a crackdown by regulators in the early 2000s. But the underlying issues have shown to be remarkably persistent for the industry, and enforcement shows no sign of relenting. Regulators have pursued numerous enforcement actions against financial firms, including sizeable money penalties and consent orders.

In response, banks have invested heavily in information technology to improve connectivity of their data systems. They also developed sophisticated models to flag suspicious activity, and they have increased the number of personnel assigned to investigate it. Information sharing among financial firms improved, as did the quality of suspicious-activity reports provided to the government.

Information systems prove to be a costly challenge as banks try to aggregate and analyze customer activity across the enterprise. Given the relatively small pool of talent available in the field, banks continuously poach talent from one another, which drives up talent costs. And bad actors continue to evolve their schemes, so financial firms play a perpetual game of catch-up.

However, KYC efforts can offer benefits. Improvements to data systems and analytics have provided a rich source of information to fine-tune marketing and enhance customer experience. When efforts to block money laundering are effective, it helps protect clients and the public — and bolsters the firm's reputation.

AML/BSA is not only the responsibility of the Compliance department. It is everyone's responsibility. Firms need a clear understanding of who plays what role in the AML/BSA process, and written policies and procedures should make clear the expectations across the "three lines of defense."

Conclusion

In 2015, moving from regulatory comprehension to regulatory compliance will rely on discrete actions — not only to maintain compliance, but to put in place the systems and processes that will help an organization respond to any new regulatory requirements that arise.

Thinking in terms of a culture — and in terms of the actions and people that make up that culture — can help position financial institutions for the necessary changes that come with the quest for compliance. While remaining internally focused is important, companies should also continue to be mindful of how they interact with and serve external parties (whether business partners, customers, or regulatory bodies) and how they collect, share, manage, and analyze information relevant to those parties.

Getting things right is what regulatory compliance is all about. And getting your business processes and systems right for your organization is part of that process. But making sure your processes and systems are “right” for the trends that are emerging on the regulatory front will take more than comprehension. It will take some extra strategic thinking and some meaningful action.

Regulatory compliance is ultimately about protecting the reputation of the organization and its management, both in the eyes of the regulators and the public whom the organization serves.

Moving Forward

The regulatory landscape for banking continues to evolve, making it imperative for firms in the industry to keep a watchful eye on new or modified requirements. For updated information about the latest regulatory trends and developments, please visit the Deloitte Center for Regulatory Strategies blog [here](#).

Contacts

Vikram Bhat

Principal
Deloitte & Touche LLP
+ 1 973 602 4270
vbhat@deloitte.com

Kevin Blakely

Senior Advisor
Deloitte & Touche LLP
+1 201 630 5085
kblakely@deloitte.com

Walter Hoogmoed

Principal
Deloitte & Touche LLP
+ 1 973 602 5840
whoogmoed@deloitte.com

Robert Maxant

Partner
Deloitte & Touche LLP
+ 1 212 436 7046
rmaxant@deloitte.com

Tom Rollauer

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

Chris Spoth

Director
Deloitte & Touche LLP
+1 202 378 5016
cspoth@deloitte.com

David Wilson

Senior Advisor
Deloitte & Touche LLP
+ 1 704 697 5974
daviwilson@deloitte.com

David Wright

Director
Deloitte & Touche LLP
davidmwright@deloitte.com

Tim Ward

Director
Deloitte & Touche LLP
+1 571 858 1964
tward@deloitte.com

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

Lara Hamilton, Senior manager, Deloitte & Touche LLP

Beth Leesemann, 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

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, 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 shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2015 Deloitte Development LLC. All rights reserved.
Member of Deloitte Touche Tohmatsu Limited