3 KEY ISSUES FOR FINANCIAL INSTITUTIONS

By Barry M. Pelagatti

The weather may be cooling, but year-end planning is heating up.

As financial institutions prepare to close the books on 2016 and finalize strategic initiatives for 2017, boardrooms across the country will debate several key issues that could impact planning and results.

As an introduction to our first ever Financial Institutions in Focus newsletter, we'll explore three challenges that have executives burning the midnight oil:

REGULATION MAKES WAVES

Regulation changes over the past several years have significantly altered the way financial institutions deliver, market and evaluate their services. The election year is likely to keep regulation at the forefront of executives' concerns. But the biggest change—the elephant in the room—is CECL (current expected credit loss model).

Issued on June 16, 2016, ASU No. 2016-13 Financial Instruments – Credit Losses (Topic 326) created a new standard for calculating expected credit losses, changing the way credit losses on many financial assets, especially loans, are recorded. The standard, which will go into effect on a rolling basis starting in 2019, will apply to all banks, savings associations, credit unions and financial institution holding companies, regardless of asset size.

Designed in the shadow of the 2008 financial crisis, these new standards are meant to be more forward-looking and increase transparency. With that in mind, the new guidance requires that financial institutions...
CONTINUED FROM PAGE 1

3 KEY ISSUES

measure all expected credit losses for financial assets within the scope of the CECL model based on three key factors:

- Historical experience,
- Current conditions,
- Forward-looking, reasonable and supportable forecasts.

The most notable change will be when companies recognize a potential loss. Under current guidelines, losses are not recorded until they meet the "probable threshold." The new standards eliminate the probable initial recognition threshold, and instead reflect an organization’s current estimate of all expected losses.

These changes require organizations to develop models for measuring expected credit losses. The new standards provide guidance, but do not specify a single method of measurement. In the coming months and years, we should expect organizations to begin designing their expanded data collection and measurement methods.

BREXIT RAISES UNCERTAINTY

On June 23, 2016, the United Kingdom shocked the world, when the country voted to leave the European Union. Followed swiftly by global market turmoil, the plummeting value of the pound and the resignation of David Cameron, the markets and UK government have since stabilized, to a degree.

While global market volatility has eased, the implications for large and middle-market financial institutions are still largely unknown. Of the many questions, there are four critical issues for financial institutions to monitor:

- Will the UK upend its financial regulatory framework? Until Britain’s exit from the EU is complete, the current EU directives remain in place. This means that the UK must still work toward the implementation of pending legislation, such as MiFID II and MiFIR, effective in January 2018.

- Will UK firms retain access to the EU single market? Under the passport system, financial services firms authorized in one of the member states have authorization to conduct business throughout the region. What happens if the UK loses its passport privileges? Firms with European headquarters in London may need to relocate, or at the very least expand, their operations.

- What is regulatory equivalence, and how will it impact operations in the wake of Brexit? Even if the separation moves forward, it’s worth noting that EU regulations are largely based on UK common law. But unless it is granted special status, the UK would need to obtain a regulatory equivalence decision from the European Commission to get full access to the single market and sustain current trading, clearing and settlement operations.

- What market provisions should you watch? The big question is whether UK managers will continue to benefit from the MiFID, AIFMD and UCITS platforms for distribution—a possibility if the UK becomes a member of the European Economic Area, or if the UK can negotiate grandfathering provisions.

While regional U.S. banks have less direct exposure to what happens overseas, the U.S. economy overall remains sensitive to global market trends. After the Brexit vote, regional banks suffered in the market as analysts predicted that any interest rate increase plans would be tabled by the Federal Reserve. In a margin-constrained market, financial institutions will be closely watching the exit and negotiations in the UK.

FINTECH BRINGS NEW OPPORTUNITY, COMPETITION

Technology is the great disruptor of all industries, and now it’s the financial services industry’s turn. A wave of tech-driven startups, and evolving consumer expectations are changing the way consumers bank, borrow and invest.

These new entrants into the banking sphere promise to make payments convenient, borrowing accessible and investing easier. Along the way, they are turning the heads of long established and larger institutions—squeezing margins, changing customer service norms and forcing large corporations to rethink business models—so much so that larger companies are even trying to get into the game themselves.

Recently, Goldman Sachs introduced Marcus, its consumer lender, and GS Bank, its online-only bank offering savings accounts and CDs. Seven large banks, including Bank of America, Chase, Wells Fargo and Capital One, have come together to create a payments network—called Zelle. All are examples of large financial institutions making forays into the fintech space, designed to compete with the likes of PayPal and Venmo, Lending Club, Prosper, Ally and others.

While some in the industry believe that fintech startups can coexist with established financial institutions, at present it is larger banks that are taking advantage of the opportunity by investing in or partnering with startups or funding their own incubators to launch products and services.

For middle market and community banks, the opportunity to take advantage of technology is now. Since the 2008 financial crisis, there’s been significant consolidation among local and community banks, financial regulation has increased the need for compliance, and customers are demanding greater scale and convenience. Fintech offers community banks the opportunity to partner with or acquire the resources and services that customers want and need without the overhead required of brick-and-mortar branches. While the big players may need to form nontraditional alliances to gain market share, community banks have a chance to be more experimental and even leading-edge when it comes to technology-enhanced services.

2017 is likely to see continued change and innovation in the financial institutions industry. As boards and executives plan ahead, there’s one other factor likely to influence investment and product development: cybersecurity. Read on for a Q&A with Mike Dombrowski where he discusses some of the top cybersecurity topics for financial institutions in the year ahead.

Barry M. Pelagatti is an assurance partner and leader in BDO’s Financial Institutions & Specialty Finance practice. He can be reached at bpelagatti@bdo.com.
Tell us about your background and areas of focus. What led you to work in the financial services industry, and what types of services do you provide?

My career path has followed technology. As IT and security evolved and became more tightly integrated, I wanted to evolve with it, and that’s what led me to financial services. At the time, information security was the biggest challenge in the financial services industry, and so it was an opportunity to develop standard-setting best practices and solutions and expand to new areas.

Working as both a consultant and within a global financial institution has helped me expand my toolkit. The challenges were not just U.S.-based. The international perspective really took the complexity to unprecedented levels. That opportunity allowed me to get closer to cybersecurity and opened up other opportunities in Anti-Money Laundering technology. Now at BDO, as a member of the Technology Advisory Practice, I work with clients across all of our service lines including IT strategy and governance, IT optimization and cybersecurity. While I work across industries, my financial services experience provides more advanced and customized offerings to our clients in that industry.

Financial services, and banking in particular, is one of the most targeted industries for cyberattacks. How are you seeing the threat landscape evolve?

The threat landscape is much more sophisticated than it was 10 years ago, particularly when it comes to the actors. Attacks used to be indiscriminate, without an understanding of the industry. Now, attackers are more knowledgeable: they know how banks work, how money moves and the regulations that apply. The attack leveraging SWIFT was a clear example of that level of sophistication.

Methods of attack also continue to evolve. While ransomware is making headlines in the industry, it’s not having as much of an impact as it might in other industries like healthcare because financial institutions have been building cyber capabilities for years and are better positioned to deal with it. I recently attended the Black Hat conference and a key takeaway was that the healthcare industry is under siege. A decade ago, that is where financial services was. Still, no one and no industry is ahead of the hackers.

Financial institutions are increasingly shifting investments from prevention to speed of detection and response.

What are your thoughts on the role of blockchain in cybersecurity and data privacy, particularly in financial services?

Blockchain is an interesting data architecture that creates a digital ledger that is shared among others participating in the blockchain. The premise is to be able to clear transactions at network speeds versus what can take days to settle a transaction through the current central clearinghouse approach used in financial services. While it shows promise regarding increasing the speed of processing and clearing transactions, there are still many questions regarding security. It’s being looked at by financial institutions, but it’s unclear whether the challenges can be adequately addressed, including security and how other risk management solutions such as fraud detection and anti-money laundering would need to be adjusted to be effective.

Are financial institutions adequately investing in cybersecurity? What areas of risk mitigation may be overlooked or under-prioritized?

Most major banks are in a good position. They can invest a great deal, and they have years of experience under their belts. Middle market, regional and community banks have a huge challenge as their capabilities and resources are typically more constrained. Middle market banks are familiar with cybersecurity regulations, but are less clear about what they need to do at their organization and how to get it done effectively given their constraints. But there is good news to address that challenge. The advancement in cybersecurity capabilities and resources are making it easier and more cost-effective for banks to take advantage. For example, middle market companies can subscribe to a threat intelligence monitoring service through cloud-based Software-as-a-Service (SaaS) rather than having to invest in internal talent, tools and technology.

One emerging area of interest is a “user-centric” approach to cybersecurity. No matter what policies, procedures or systems a company has in place, security issues
are most often a result of human error. Companies are beginning to step back and examine if their cybersecurity practices are effective and designed for the user in mind. I believe that’s the next wave of progress that can make a big impact on reducing risk.

**Regulators have increased their examination of financial institutions’ cybersecurity measures and protocols in recent years. Do you expect to see additional regulation in the year ahead?**

Believe it or not, we are still in the early stages of cybersecurity regulation. As an example, in the state of New York, Governor Cuomo just announced proposed cybersecurity requirements for financial services companies. The proposed requirements have the intent to set minimum standards, but not be overly prescriptive on the financial institutions. This says two things to me: 1) financial institutions must take steps towards improving cybersecurity measures—it’s not optional; and 2) there are certain specifics that need to be followed, whether it’s in the domains covered by a cybersecurity program, the roles or reporting requirements or specific implementation requirements such as audit logs and multi-factor authentication.

However, the most telling parts of the proposed requirements are the enforcement capabilities, the requirement for the board of directors to be briefed at least twice a year on the cybersecurity plan and progress, and having a senior officer sign off on the institution’s compliance to the requirements. It feels similar to how Sarbanes-Oxley changed the financial reporting requirements.

This is perhaps the most direct and specific set of requirements I’ve seen to date. These are the trends I expect to continue across regulated industries: clarity, more specifics, stronger enforcement and accountability up to and including the board of directors. No one is expected to be perfect, but there must be an absence of ignorance. Understanding your risks, the steps you have taken, the steps you are taking, the remaining gaps that need to be addressed and making consistent and appropriate progress towards closing those gaps are key. Not knowing is unacceptable.

Along with continued regulation requirements, I expect we’ll also see progress at an even more detailed level. For example, standards bodies like NIST (National Institute of Standards and Technology) are taking additional steps toward more clarity on the types of multi-factor authentication, such as SMS (short message service), that they consider no longer good enough to be part of the solution. Financial institutions need to have cybersecurity programs that are adaptive and agile so that the continued evolution to regulations, as well as the threats and risks themselves, can be effectively addressed without being disruptive to the business.

Outside of cybersecurity, what issues and priorities are at the top of the list for CIOs at financial services firms?

I think CIOs have some of the toughest challenges in the industry. Their top priority remains providing the business with the capabilities to enable strategy and drive growth. They’re asked to do more with less and have to deal with multiple competing priorities including cybersecurity.

Board-level attention on cybersecurity has also elevated the focus on the CIO in financial institutions. Over the last 10-15 years, financial institution CIOs had to expand their expertise to include cybersecurity, fraud detection and anti-money laundering all while continuing to enable the business strategy through core applications and financial products.

With that being said, the biggest challenge that CIOs have is speed: speed to market, speed to detecting risks or issues and speed to recovery. More so today than ever before, speed has become the critical challenge across all fronts.

Michael Dombrowski is a Managing Director in the Technology Advisory practice at BDO Consulting. He can be reached at mdombrowski@bdo.com.
CONSIDERING COMPLIANCE IN YOUR GROWTH STRATEGY

By Laurence Talley

The economic downturn and recession have led banks to operate in the most regulated and scrutinized environment in history.

New and more rigorously enforced regulations like Dodd-Frank are designed to enhance risk management and protect the going concern of financial organizations and the consumers who rely upon them. But, in some cases, the environment may be causing banks to delay growth while they prepare internally to meet future compliance needs. In this article, we will identify regulations that banks need to prepare for at key asset milestones and offer a readiness road map.

Regulation is a broad term. For the purpose of this discussion we consider regulation to encompass: 1) rulemaking—congressional authority to issue banking rules; 2) supervision—power to examine bank and instruct remediation required for compliance; and 3) enforcement—authority to take legal actions for noncompliance.

REGULATIONS BY MILESTONES

In an attempt to reduce compliance burdens, some regulators are staggering the application of certain regulations by bank size and activities. Many new regulations have been adjusted to provide relief for smaller banks, specifically to balance and mitigate the risk of regulations becoming unduly burdensome. Most are trigged by a bank’s asset size. Significant regulatory milestones begin when bank assets reach $1 billion, $10 billion and $50 billion.

Savvy regional and community banks are managing growth and integrating compliance readiness into growth strategy and initiatives, allocating time and resources to prepare people, process and technology for resulting compliance requirements.

The following outlines key regulations compliance milestones that warrant additional consideration and preparation:

<table>
<thead>
<tr>
<th>REGULATION</th>
<th>TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Banks with $1B+ in assets</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Basel III</td>
<td>Safety and Soundness</td>
<td>This installment of the Basel Accords was developed in response to trends of deficiencies in financial regulation revealed by the financial crisis. Basel III is intended to strengthen capital requirements by increasing liquidity and decreasing leverage.</td>
</tr>
<tr>
<td>FDICIA (FDIC I... Act)</td>
<td>Safety and Soundness</td>
<td>FDIC requires that an insured depository institution with total assets of $1B or more confirm the adequacy of its system of internal control based on a generally accepted framework (i.e., COSO 2013).</td>
</tr>
<tr>
<td><strong>Banks with $10B+ in assets</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Volker Rule (Propriety Trading Restrictions)</td>
<td>Safety and Soundness</td>
<td>The Volcker Rule of Dodd-Frank was established to restrict U.S. banks from making certain kinds of speculative investments that do not benefit their customers. The rule is often referred to as a ban on proprietary trading by banks, whereby deposits are used to trade on the bank’s own accounts.</td>
</tr>
<tr>
<td>Durbin Amendment (Debit Card Fee Restrictions)</td>
<td>Consumer Protection</td>
<td>The Durbin amendment, passed as part of Dodd-Frank, limits fees charged to retailers for debit card processing. Banks with over $10B in assets have to charge debit card interchange fees that are “reasonable and proportional to the actual cost” of processing.</td>
</tr>
<tr>
<td>Enhanced Prudential Standards (EPS)</td>
<td>Safety and Soundness</td>
<td>The Fed’s enhanced prudential standards (EPS) impose specific risk management requirements on banks with $10B or more in assets. The requirements include the establishment of a risk committee to establish and oversee the bank’s risk management framework and stress testing.</td>
</tr>
<tr>
<td>Dodd-Frank Act Stress Testing (DFAST)</td>
<td>Safety and Soundness</td>
<td>Banks with $10-$50B in assets must assess the potential impact of various economic scenarios—baseline; adverse; and severely adverse—on revenues, balance sheet and capital.</td>
</tr>
<tr>
<td>Model Risk Management</td>
<td>Safety and Soundness</td>
<td>OCC 2011-12 defines a model as a quantitative method, system or approach that applies statistical, economic, financial or mathematical theories, techniques and assumptions to process input data into quantitative estimates. The regulation requires validation of the core components and application including model governance, data input, processing, results and reporting.</td>
</tr>
</tbody>
</table>

Read more ➤
Supplemental Guidance on Internal Audit

As a result of the supervisory experience during and following the financial crisis, the Fed identified areas for improving regulated institutions' internal audit functions. This supplemental policy statement addresses the characteristics, governance and operational effectiveness of an institution’s internal audit function.

Continuous Supervision

Bank exceeding $10B in assets are designated as mid-size and assigned regulatory teams to provide ongoing and enhanced supervision. The team will perform more frequent and in-depth examinations.

Banks with $50B+ in assets

Heightened Standards for Large Banks

The Office of the Comptroller of the Currency (OCC) issued 13 risk governance standards to formalize the heightened expectations for banks with ≥$50 billion in assets. These standards provide guidance for banks to establish a rigorous risk management framework focusing on governance, people and processes.

CCAR

The Comprehensive Capital Analysis and Review (CCAR) is a supervisory assessment by the Fed of the capital planning processes and capital adequacy of large, complex bank holding companies. The CCAR is the Fed’s central mechanism for developing supervisory assessments of capital adequacy at these firms.

Banks with $250B+ in assets

Liquidity Risk Measurement Standards

This standard establishes a minimum liquidity (cash) requirement for FDIC-supervised institutions with total consolidated assets equal to $250 billion or more, as reported on the most recent year-end Consolidated Report of Condition and Income.

Supplementary Leverage Model

This requirement is designed to reduce short-term liquidity risk for international banking organizations. This improves the bank’s ability to absorb the impacts of financial and economic stress.

COMPLIANCE MONITORS

Managing just these noted regulations requires significant resources and time, and understanding the responsible regulatory body adds another layer of complexity. Most safety and soundness regulations are governed by a bank’s prudential regulators (FDIC, Federal Reserve, OCC, National Credit Union Administration [NCUA]). Consumer protection is jointly regulated by prudential regulators and the Consumer Financial Protection Board.

Banks under $10B

<table>
<thead>
<tr>
<th>Regulation Activity</th>
<th>Safety &amp; Soundness</th>
<th>Consumer Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rulemaking</td>
<td>Prudential Regulators</td>
<td>CFPB</td>
</tr>
<tr>
<td>Supervision</td>
<td>Prudential Regulators</td>
<td>Prudential Regulators</td>
</tr>
<tr>
<td>Enforcement</td>
<td>Prudential Regulators</td>
<td>Prudential Regulators</td>
</tr>
</tbody>
</table>

Banks over $10B

<table>
<thead>
<tr>
<th>Regulation Activity</th>
<th>Safety &amp; Soundness</th>
<th>Consumer Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rulemaking</td>
<td>Prudential Regulators</td>
<td>CFPB</td>
</tr>
<tr>
<td>Supervision</td>
<td>Prudential Regulators</td>
<td>CFPB</td>
</tr>
<tr>
<td>Enforcement</td>
<td>Prudential Regulators</td>
<td>CFPB &amp; Prudential Regulators</td>
</tr>
</tbody>
</table>
HOW TO PREPARE
The complexity of the regulations and regulators begs the question: how should banks prepare? The responsibility for readiness is wide-ranging and may require participation from bank leadership, operations, compliance, IT and other stakeholders that can influence or will be subject to resulting changes.

Compliance Readiness Road Map
There are several key factors that banks should consider and plan for in order to successfully adopt and comply with new regulations:

**GOVERNANCE**
Ensure roles and responsibilities are identified and assigned for compliance owners and key stakeholders.

**POLICIES AND PROCEDURES**
Update or establish polices and operating procedures that may be influenced by regulations.

**TRAINING**
Ensure new and current employees are properly trained on the regulation’s objectives and the bank’s approach and procedures for compliance.

**ACCOUNTING**
Understand how new compliance requirements may influence technical accounting and reporting.

**HUMAN RESOURCES**
Understand any need for people or skills that may be prompted by new regulations.

**PROCESS DESIGN**
Understand processes that are needed to support compliance requirements. Walk through the design of activities and systems that are required to achieve the objective of each process.

**IT INFRASTRUCTURE, APPLICATIONS AND DATA**
Evaluate the IT tools that may be required to efficiently support and operate new compliance processes. This includes the development, operation and governance of bank models.

**IDENTIFICATION OF NEW RISKS AND CONTROLS**
Challenge the bank’s risk management framework and update it to include new operational and compliance risks that may be introduced by new regulations. Establish new controls as needed to ensure new risks are mitigated. This exercise should include IT access, data and infrastructure security.

**CONSULT**
Communicate with peer banks, external advisors and regulators to ensure common and leading practices are adopted and pitfalls are avoided.

**PROJECT PLANNING**
Compliance implementation should be supported by a sound project planning discipline that includes scheduling, budgeting, progress monitoring, milestone definitions, reporting and communication.

As bank executives and boards plot growth strategies for 2017 and beyond, including these proactive compliance stepping stones in the planning process will help ensure smoother transitions and fewer regulatory hurdles.

Laurence Talley is a managing director in BDO’s Risk Advisory Services practice. He can be reached at ltalley@bdo.com.
Many community banks are re-examining executive compensation programs in response to the introduction of new business models and improved earnings over the past year. Executive base salary budgets have risen 3.4 percent for executives this year, according to BDO research.

BDO recently reviewed proxy statements of 52 public banks in the Northeast with $500 million to $2.5 billion in assets, examining executive compensation for the top C-suite officers. While the analysis focused on one section of the country, BDO believes the trends it observed are consistent with patterns seen in banks across the nation.

MULTI-LEVEL STRATEGIES
More community banks are moving away from one single executive compensation strategy for all of its executives. In part, as community banks expand business into new areas like Small Business Administration (SBA) loans, which are growing in popularity, it’s critical to update how success is defined in executive compensation programs. Often, it’s useful to have a separate compensation program for a new business area until it’s fully integrated into the business.

Many banks are also facing a baby boomer exodus in the C-suite. By some estimates, 40 percent of bank CEOs are over 60 years old and potential replacements are within five to 10 years of retirement. As a result, many banks are embracing two-tier strategies, with standard long-term compensation arrangements supplemented by programs more attractive to mid-career high potential employees, such as customized deferred compensation plans or special retention plans that acknowledge career milestones.

INCENTIVES
Our analysis revealed that annual incentives—which make up 14 to 20 percent of total direct executive compensation—were typically funded by one or more performance metrics. The most common metrics were:

- Custom metrics unique to the business model (44 percent)
- Net income (27 percent)
- Earnings per share (23 percent)
- Return on assets (19 percent)

The more frequent use of custom metrics over traditional metrics, like return on assets, reflects a closer alignment with the bank’s business model. Custom metrics typically contain a discretionary component, which can be used to reward executives for completion of increasingly burdensome compliance programs or activities.

Long-term incentives, which tend to comprise 15 to 20 percent of total direct compensation, have seen a slight increase in size since 2014. Stock options have fallen out of favor, instead replaced by performance shares or restricted stock unit programs that are anchored by performance vesting requirements.

COMPENSATION RISK
Boards are becoming more involved in monitoring executive compensation programs. Regulatory agencies are proposing new rules that may require greater disclosure on incentive plan arrangements and the definition of “significant risk taking.”

As new regulatory and business developments unfold, it’s critical to take a fresh look at how executive compensation will need to adjust course.

Tom Ziemba is a managing director in BDO’s Financial Services practice. He can be reached at tziemba@bdo.com.
The following is a list of upcoming conferences and seminars of interest for financial institution executives:

**NOVEMBER**

Nov. 1-3
New Jersey Bankers Senior Management Conference
Borgata Hotel and Casino
Atlantic City, N.J.

Nov. 13-15
ABA/ABA Money Laundering Enforcement Conference
Washington Marriott Wardman Park Hotel
Washington, D.C.

Nov. 15
New Jersey Bankers CFO Conference
Renaissance Woodbridge Hotel
Iselin, N.J.

**DECEMBER**

Dec. 6
BDO New Jersey Banking Seminar
Forsgate Country Club
Township, N.J.

Dec. 8
BDO Pennsylvania Banking Seminar
Downingtown Country Club
Downingtown, Pa.

**JANUARY 2017**

Jan. 19-20
iiBIG/CCA Marketplace Cloud Lending Summit & Expo
Aria Resort & Casino
Las Vegas, Nev.

Jan. 30-31
Alternative Lending Summit 2017
Fontainebleau Hotel
Miami Beach, Fla.

**FEBRUARY**

Feb. 19-22
National Conference for Community Bankers
JW Marriott Orlando, Grand Lakes
Orlando, Fla.

**MARCH**

March 6-7
LendIt USA 2017
Jacob Javits Center
New York

March 19-20
ABA Mutual Community Bank Forum
Washington Marriott Marquis
Washington, D.C.

March 15-19
ICBA Community Banking LIVE Expo
Ernest N. Morial Convention Center
New Orleans, La.

March 26-28
ABA Risk Management Conference
JW Marriott Indianapolis
Indianapolis, Ind.

**FINANCIAL INSTITUTIONS IN FOCUS**

BDO’s Financial Institutions & Specialty Finance practice has extensive experience providing audit, tax and consulting services with a focus on the financial institutions industry, including banks, savings institutions, credit unions and foreign banking organizations. For additional information on BDO’s services to the industry, please visit https://www.bdo.com/industries/financial-institutions-specialty-finance/overview.

ABOUT BDO

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, advisory and consulting services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 500 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of 1,408 offices in 154 countries.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your firm’s individual needs.

© 2016 BDO USA, LLP. All rights reserved.
People who know Financial Institutions, know BDO.