5 strategic considerations for financial institutions in 2017

From regulation to technology, where to focus now

January 2017

Financial institution will continue to face new challenges in 2017. Here are five key issues you face today along with strategies to address them. For a deeper dive into these topics, watch our webcast, Top strategic considerations for financial institutions.

1. Know the regulatory hot topics for 2017

Financial institutions continue to face escalating scrutiny from a variety of regulatory agencies. The following list offers strategies for how you should respond in 2017:

- Take a look at your compliance management system. Regulators are taking a different approach to examinations at banks and credit unions. Until recently, they focused almost exclusively on files and transaction testing, but they are now also taking a harder look at each institution's overall risk management approach to compliance across the three lines of defense. With the Consumer Financial Protection Bureau (CFPB) leading the charge, regulators are now taking a top-down look at the overall compliance effort. For more information, see 4 steps financial institutions should take to strengthen compliance management systems.
- Evaluate your fair lending practices. Regulatory agencies are increasingly focused on compliance with fair lending regulations, and more specifically with particular attention to residential, auto, dealer, credit card and small business lending programs. They are also spending more time investigating potential redlining practices.
- Self-assess your Truth in Lending Act-Real Estate Settlement Procedures Act (TILA-RESPA) Integrated Disclosure (TRID) compliance. TRID amendments to Regulation Z have been effective for just over a year. So far, regulatory agencies have been sensitive to the complexities of compliance with the amendments, but they are likely to begin spending more time performing testing on technical compliance during examinations. Financial institutions should evaluate and monitor

TRID compliance to allow time to document potential weaknesses, formulate corrective action plans and train your employees now to promote compliance with TRID.

- Ensure integrity of Home Mortgage Disclosure Act (HMDA) and Community Reinvestment Act (CRA) data. Regulators continue to identify data integrity issues with HMDA and CRA data submissions. Financial institutions with data issues face potential fines and costly projects to scrub their historical data. What steps you should take now?
  - Make sure that your changes to HMDA/CRA data collection are linked to your operational procedures to promote a consistent and reliable reporting environment
  - Conduct monthly quality control testing of data collection
  - Provide ongoing training and feedback to all involved personnel
  - Institute data analytics and population controls as part of your HMDA/CRA data efforts
  - Conduct independent testing well in advance of your annual reporting deadlines to provide enough time to remediate issues and record correcting entries

Evaluate your models. Financial institutions rely on a variety of models to evaluate and manage risk, as well as forecast scenarios and results. These models range from sophisticated rules- and assumption-based software systems to simple spreadsheets, and they are used to manage risk and make forecasts for everything from interest rate risk and liquidity to loan scoring and money laundering or fraud detection. Financial institutions must regularly review the accuracy and adequacy of their models and how they fit into their overall control environment across the three lines of defense.

Take a close look at incentive compensation plan (ICP) practices. The recent regulatory scrutiny at Wells Fargo underscores the risks associated with ICP, but regulatory attention here is nothing new. Dodd-Frank contained a variety of provisions to curtail ICP that do not have sufficient linkages between risk and reward. Proposed rules published in July 2016 would prohibit ICP that encourages inappropriate risks.

Reconsider your diversity and inclusion practices. To date, section 342 of the Dodd-Frank Act has attracted relatively little attention. Section 342 addresses diversity policies and practices at several regulatory agencies and at the companies that those agencies regulate. In addition, section 1071 of Dodd-Frank contains standards on diversity and discrimination in lending practices that will be part of new HMDA rules effective in January 2018. To date, compliance with section 342 has been voluntary, but regulators have noted a lack of progress, which may lead to enforcement activity. Consider a self-assessment, and recognize that increased focus on diversity compliance as a risk factor in your hiring and lending practices. For more information, see Dodd-Frank, shifting demographics drive a new emphasis on diversity.

2. Focus on anti-money laundering and Bank Secrecy Act compliance

BSA/AML compliance continues to be a major focus for regulators and a significant concern for financial institutions. Recent fines imposed on small and mid-sized banks for program deficiencies and governance concerns demonstrate that regulators aren't just focusing on large institutions.

The following are some steps you should consider in order to improve your BSA/AML capabilities:

- Use data analytics. All institutions are looking for more efficient AML monitoring with fewer false positives. Simultaneously, most have to find ways to do more with less. Data is increasing exponentially and the technologies available to analyze that data are maturing rapidly. You can increase the coverage and frequency of your monitoring and testing through data analytics, which offers the following benefits:
  - Improved efficiency of suspicious activity monitoring and reporting
  - Improved continuous risk monitoring with focus on key performance indicators and key risk indicators
  - Automated dashboards enabling continuous monitoring and testing and real-time insight into BSA/AML activities
  - More effective sampling for deeper dives in specific compliance areas
- Understand the new customer due diligence (CDD) rule. FinCEN published the final rule on enhanced CDD on May 11, 2016. It requires financial institutions to identify and verify beneficial owners of legal entity customers. Covered institutions must comply by May 1, 2018.
- Understand New York Department of Financial Services Rule 504. Rule 504, issued on June 30, 2016, imposes new rules and certification requirements for financial institutions doing business in the state. Rule 504 requires:
  - Risk-based transaction monitoring and watch list filtering programs based on the financial institution's BSA/AML and Office of Foreign Assets Control (OFAC) risk assessments
  - The programs must have governance and oversight (including policies and procedures), they must have complete and accurate data, and the programs must be validated
  - Annual certification must be completed by board or senior compliance officer

For more information on a wide variety of AML/BSA issues, see RSM's AML/BSA Resource Center.

3. Strengthen credit administration

The United States is currently in the fourth longest economic expansion since World War II, which begs the question of where are we in the current economic cycle? RSM's Middle Market Business Index (MMBI) shows a strong rebound in middle market confidence in the fourth quarter of 2016. Developed in partnership with Moody's Analytics, the MMBI is designed to accurately reflect business conditions in the U.S. middle market, while providing a statistically significant measure of the health and outlook for these businesses. Going forward, the MMBI will serve as a leading indicator for the middle market (the real economy), a vital segment of the U.S. economy that represents more than 200,000 firms, 40 million jobs and one-third of private sector gross receipts. For more on the MMBI's current findings, read RSM US Middle Market Business Index rebounds strongly in Q4.

But not all the news is positive. The Trepp® November 2016 CMBS Delinquency Rate increased to more than 5 percent, which is the highest level since December 2015.

To ensure sustainable credit quality going forward, consider these five credit administration resolutions for 2017:

- Clean up the tickler and establish or enforce existing escalation processes to resolve exceptions
- Stress test, stress test, stress test
- Update, enhance or implement credit risk reporting depending on the maturity of the reporting in your institution
- Refresh your approach to executing and reporting on loan review results
- Develop and document your CECL implementation plan

4. Understand the cybersecurity threat landscape

Cybersecurity remains a key risk for all financial institutions. The NetDiligence/RSM 2016 Annual Cyber Claims study reveals the following:

- When examining records exposed by type of data, personally identifiable information accounted for the largest share of records, at 51 percent. Payment card industry data was second at 24 percent.
- Hacker activity, at 23 percent, and malware and viruses, at 21 percent, were the most common causes of loss.

From using malicious code to remotely manipulating ATMs into dispensing cash, to new tools that access the USB drives of locked computers and bypass security to steal desired files, financial institutions continue to face new and evolving threats. Our webcast, How to protect your financial institution against today's top cyberthreats, and our recent article Effective cybersecurity means more than protecting your perimeter offer more detail on key cybersecurity issues.

5. Explore IT outsourcing and cloud computing

A number of factors are driving an accelerated trend toward outsourcing and cloud computing among financial institutions. Many institutions, especially regional and community banks, are struggling to find sufficient IT talent. The speed of change and the continually evolving regulatory environment are putting more demands on technology. The need for a more agile workforce coupled with aging IT infrastructure and stagnant budgets are demanding new technology solutions.

As a result, financial institutions are outsourcing more than ever before. Some of the common areas include:

- Human resources and payroll
- Marketing
- Risk management
- Compliance
- Security
- IT functions
- Core processing
- Independent sales organizations
- IT committee advisors

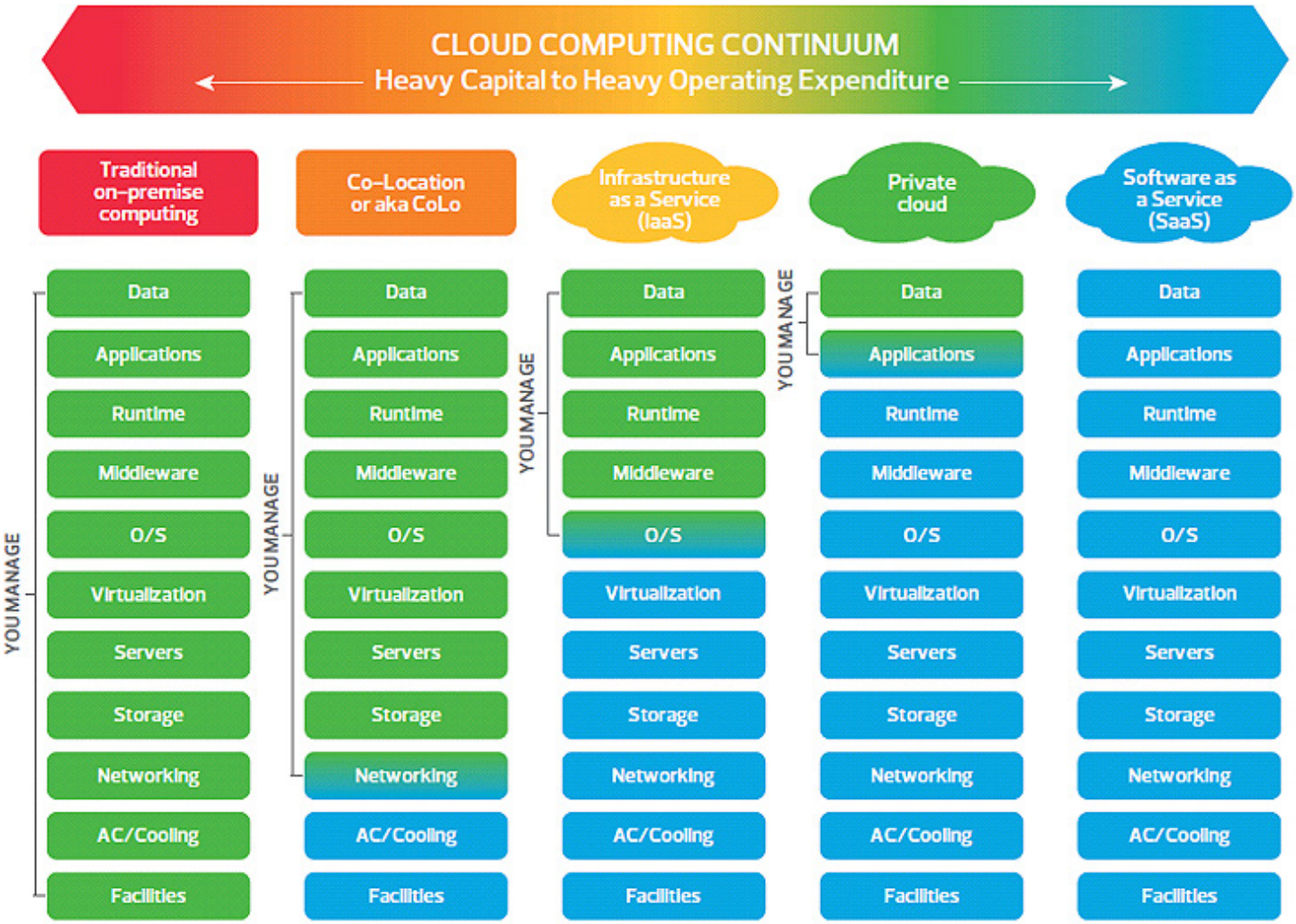
IT outsourcing models

Financial institutions typically utilize the following three primary outsourcing options:

- IT outsourcing: Instead of keeping your technology functions in-house, IT outsourcing involves farming out some—or all—of your IT functions to a third-party provider. IT outsourcing can be designed to fit the technology needs of any organization, transitioning functions to a company with IT as its core competency.
- Managed services: Managed service providers are the most definable form of outsourcing with specific, detailed costs and expectations, as well as inherent flexibility. This strategy is very attractive as it provides scalability and defined expectations at a consistent month-to-month expense.
- Staff augmentation: Staff augmentation provides the ultimate level of flexibility, filling a specific skill set in times of need such as extended staff absences, special projects or increased seasonal demand. Many companies also use this strategy after experiencing difficulty finding specialized talent or lacking the resources for full-time internal staff.

Cloud computing

Cloud computing is another increasingly popular technology strategy. As financial institutions weigh the benefits of operating expenses versus capital expenditures and consider the specific technology aspects they wish to continue to manage, cloud computing can offer a broad continuum of options. For example, Microsoft Office 365 is an increasingly popular cloud computing option.



Outsourcing and security

Outsourcing components of technology or using cloud computing does not diminish the responsibility of management and boards of directors to ensure that any third-party activity is conducted in a safe, sound manner and in compliance with all applicable laws and regulations. Due diligence of vendor security policies, procedures and practices is a vital component of any outsourcing effort.

+1 800 274 3978
www.rsmus.com

wc-nt-con-fi-1216

RSM