90 Day Note

May 2017 Vol. 31, No. 1

A Young & Associates, Inc. Publication

Inside This Issue:

Excess Capital is Hurting Shareholder Return

By: Gary J. Young, President and CEO

The Mantra

As community bankers, we have all heard the mantra to increase capital. This is heard by the banker that has an 8% leverage ratio who needs to increase capital to 9%, by the banker who has a 9% leverage ratio that needs to increase capital to 10%, and by the banker who has a 10% leverage ratio that needs to increase capital to 11%. Based on this view regarding capital, more is always better. I disagree.

Capital Adequacy

I agree with the OCC. Capital adequacy at each bank is uniquely based on the current and planned risk within the bank. And, it is the responsibility of the bank board to determine capital adequacy with the input from executive management. Capital adequacy is the point in which a capital contingency plan is implemented if actual capital falls below that level. In other words, let's assume capital adequacy has been defined as a 7.5% leverage ratio, or an 11.25% total risk-based ratio. If actual capital falls below either measure the bank should implement the methodology for improving capital as described in the capital contingency plan.

Capital Target

A bank's target or goal for capital is higher than capital adequacy. It is an estimate of the amount the board of directors has decided is needed to take advantage of opportunities such as additional organic growth, branch expansion, purchase of a bank or branch, stock repurchase, etc., or to use as additional insurance or protection against negative events that could hurt profitability and capital. As an example, a 7.5% leverage ratio could be defined as capital adequacy, but the target level of capital is 9.0%.

Cost

Excess capital has a cost. Let's assume you had to eliminate $1 million of excess capital. To balance that transaction, you would also eliminate $1 million in assets which would be investments. Let's assume that the investments had an average yield of 1.5%. After taxes, that would be approximately 1.0%. Based on this example, the return on equity of the $1 million of excess capital is 1.0%. We must agree that 1.0% is unacceptable. Well, it is unacceptable unless that is your return for opportunity capital or insurance capital as described above.

Another example of the cost of excess capital can be seen in the table on page 2. There are four banks with a 1% ROA. However, the equity/asset ratio at each is different, ranging from an 8.0% leverage ratio to a 12.0% leverage ratio. By dividing the ROA by the leverage ratio, you get the ROE. By multiplying the ROE by an assumed PE, you get the multiple of book. In this example, the bank with an 8.0% leverage ratio has a value of $30 million while the bank with a 12.0% leverage ratio has a value of $20 million. This is a simplified example that provides information on the cost of excess capital.

(continued on next page)

ROA	EA	ROE	PE	X Book	(in millions) Book	(in millions) Value
1.0%	8.0%	12.5%	12	1.50	$20.0	$30.0
1.0%	9.0%	11.1%	12	1.33	$20.0	$26.7
1.0%	10.0%	10.0%	12	1.20	$20.0	$24.0
1.0%	12.0%	8.3%	12	1.00	$20.0	$20.0

ROA - Return on Assets
EA - Equity/Asset Ratio
ROE - Return on Equity
PE - Price-Earnings Multiple
X Book - Value in Terms of Multiple of Book
Book - Shareholder Equity
Value - Franchise Value in Terms of a Casual Trade

The Right Amount

There is no right amount. The average $300 million - $1 billion bank has a 10.3% leverage ratio and a 15.4% total risk-based capital ratio. Most everyone would agree that banks do not need that level of capital. But, every bank is unique with different levels of risk and different levels of risk appetite. The important thing is that executive management and the board of directors understand that there is a shareholder cost to holding excess capital. That doesn't make it wrong.

The board of directors has multiple responsibilities and at times they can be conflicting. From the shareholder perspective, you want to maximize the return on equity and shareholder value, which assumes leveraging capital, but you must also oversee the operation of a safe and sound bank. And, at the heart of safety is capital adequacy. It takes balance and awareness of both to determine the right level of capital for your bank. My concern is that through the Great Recession and after, the capital mantra has been "more is better." Well frankly, more is not necessarily better. I am suggesting that it is time to balance the capital need for risk management with the capital need for improving shareholder value.

"...it is time to balance the capital need for risk management with the capital need for improving shareholder value."

Best Practices

The question for executive management is what should I do? It is my opinion that best practices would indicate that every bank develop a definition of capital adequacy based on inherent risk. Furthermore, a capital contingency plan should be part of that plan that indicates the steps the bank might take if capital falls below or is projected to fall below the bank's definition of capital adequacy. You should then have a frank discussion at the board level on the amount of capital that is your goal or meets your comfort level. If you then find that your capital is above that consider the following:

- Focus on additional organic growth, if possible.
- Consider expansion opportunities. I would suggest looking for opportunities that begin turning a profit in two years or less.
- Develop a stock repurchase plan. This is a win for the shareholders that want to sell and the shareholders that want to hold. Everyone wins and shareholder value should increase.
- Achieve a slow, steady increase in dividends to shareholders.

Consider how all of these items might impact your capital adequacy, return on equity, and shareholder value over a 3-5 year period. Remember, the goal of executive management is to maximize profitability and shareholder value within capital guidelines approved by your board of directors.

Conclusion

If you would like to discuss this article with me, you can reach me by phone at 330.422.3480 or by email at gyoung@younginc.com. ❑

38 YEARS 1978 - 2016

The Director's Role in Information Security

By: Mike Detrow, Senior Consultant and Manager of IT

Technology has changed significantly at community banks over the past 15 years. For many years, banks only had to manage a core processing system, a standalone Fedline PC, and a few workstations that were used for word processing and maintaining spreadsheets. These systems were relatively easy to secure as data was maintained in-house and connectivity to external networks was limited. Fast forward to 2017 and community banks now have connections to numerous outside networks including the internet and those of core processing vendors. Services are being offered to customers through cell phones and tablets, customer data is processed through websites, and data is stored in many locations that are not controlled by the bank.

Whether making a loan, depositing a check, or checking a customer's account balance, nearly every function within the bank now relies on some form of technology. To remain competitive, the implementation of new technology is necessary to meet the needs of customers and to reduce a bank's operating expenses. However, information security has often been an afterthought rather than being incorporated during the implementation process.

Regulators are emphasizing the need for a change to the security culture within community banks to make information security a higher priority, and this change must begin with the board of directors. The board must take a more active role in the oversight of the bank's information security program. All too often, information security is treated as something that only the "IT person" can understand, and directors do not properly scrutinize the decisions made by the IT Manager or an outsourced technology support provider. The board of directors is ultimately responsible for the security of the customer information maintained by the bank and the third parties that the bank uses. As such, directors must have a clear understanding of the regulatory requirements for protecting customer information, as well as defining and monitoring the bank's information security program. While directors may not fully understand all of the technical aspects, I have provided some general recommendations for overseeing the information security program within this article.

Recommended Documents

The following documents should be reviewed and approved by the board of directors on an annual basis, or more frequently depending on the changes that occur within the bank. While much of the information in these documents will not change, there will typically be some changes each year due to employee turnover, technological changes, or new regulatory guidance. These changes should be clearly documented to allow directors to evaluate the changes before approving the updated documents. If there are no recommended changes to these documents over a period of several years, directors should request an explanation from management.

- **IT Strategic Plan.** An IT Strategic Plan should be in place to align IT initiatives with the bank's overall strategic plan. This may include the implementation of additional products and services to compete with other financial institutions or the implementation of technologies to create internal efficiencies. The IT Strategic Plan may also identify systems that are approaching the end of their manufacturer's support lifecycle and identify upgrade/replacement strategies.
- **IT Budget.** The budgeting process should include information technology and information security expenses such as hardware and software maintenance, technology service provider expenses, contract renewals, recently approved project expenses, training expenses, and risk mitigation expenses.
- **Information Security Program**. The Information Security Program identifies the technical, physical, and administrative safeguards that must be implemented to maintain the confidentiality, integrity, and availability of the bank's information systems.

(continued on next page)

- **Information Security Risk Assessment.** The Information Security Risk Assessment should identify the information systems that are in use, classify the data that the information systems store or process, identify the threats and vulnerabilities associated with each information system, identify the likelihood and impact of the risks, identify the mitigating controls that have been implemented, and evaluate the effectiveness of the mitigating controls. The risk assessment should be updated before implementing new information systems and as new threats are discovered.
- **Incident Response Plan.** The Incident Response Plan should identify the procedures to be performed in response to an incident involving loss of data availability, confidentiality, and/or integrity, such as a breach. The steps of this plan should include containing the incident, recovering from the incident, the investigation process, and the notification process. This plan should be tested on a regular basis to evaluate the effectiveness of the response procedures for various types of incidents.
- **Business Continuity/Disaster Recovery Plans.** The Business Continuity and Disaster Recovery Plans identify procedures for performing the bank's business processes during or following various types of operational interruptions. These procedures must be tested on a regular basis to ensure the continuity of these business processes during a variety of disruptive events, such as natural disasters, service provider interruptions, and cyber-attacks.
- **Cybersecurity Assessment**. A formal Cybersecurity Assessment should be performed to evaluate the bank's inherent cyber risk and the effectiveness of its cybersecurity controls. If the bank is utilizing the FFIEC's Cybersecurity Assessment Tool, an understanding of the relationship between the Inherent Risk Profile and the Cybersecurity Maturity Level is required. Plans for attaining the recommended Cybersecurity Maturity Level should be developed and the status of this process should be monitored. The Cybersecurity Assessment should be reviewed annually and updated when changes occur that affect the bank's Inherent Risk Profile.

Recommended Reports

The Information Security Officer should provide information security program status reports to the board of directors on at least an annual basis. These reports should identify the risk assessment process, risk management and control decisions, service provider arrangements, results of independent testing of the information security program, security breaches, and recommendations for updates to the program. While some of the content within these reports will not change, these reports should reflect the actual activity since the last report and should not just be the same report with a new date at the top.

While many community banks have implemented a steering committee to manage their information security programs, directors still need to ensure that the program is effectively managed. If a steering committee is used, a formal charter should be in place to define the committee's purpose and responsibilities. The board of directors should receive copies of the steering committee's meeting minutes to monitor committee activities and to ensure that it is fulfilling its requirements.

Information system reports and service provider reports should be regularly monitored to identify any events that require further investigation. Some examples of the reports that should be reviewed by the steering committee or the board of directors include:

- Patch management
- Firewall
- Intrusion detection system
- Intrusion prevention system
- Anomalous operating system events
- Malware/virus protection
- Managed services provider tickets
- Vendor management

If the reports that are provided never indicate any anomalous activity that requires further investigation, directors should question the validity of the reports and request a review of the reporting parameters for the system(s).

(continued on next page)

Independent Audits

To assist the board of directors with its evaluation of the effectiveness of the bank's information security program, periodic independent audits should be performed. These audits are typically performed on an annual basis depending on the size and complexity of the bank and its risk assessment. The board of directors or the audit committee should be involved in the external auditor selection process and the audit scoping process. At least one director should participate in the auditor's exit meeting to ensure an understanding of any recommendations made by the auditor.

Conclusion

The use of a top-down approach to manage information security and holding employees accountable for complying with the bank's information security program will greatly strengthen the security culture within the bank. A strong security culture will help to enhance the bank's reputation among its customers, community, and the financial industry.

For more information on this article or on how Young & Associates, Inc. can assist you in this process, contact me at 330.422.3447 or mdetrow@younginc.com. ❑

Capital Market Commentary

By: Stephen Clinton, President, Capital Market Securities, Inc.

Market Update – The Trump Effect

The election of President Donald Trump was followed by a strong upward movement in the market. Hopes related to lower taxes, less regulation, and economic stimulus led the market to new highs. Since the election, the Dow Jones Industrial Average moved up 14.22% through April 30th. Banks moved upward even more, increasing 21.29% (as measured by the Nasdaq Bank Index). Much has been made of the first 100 days of the new administration, with many Executive Orders being issued but no real legislative actions accomplished. The March failure to pass legislation to repeal the Affordable Care Act was a stark reminder that enacting legislation is a difficult process. However, the market appears to remain optimistic that President Trump's initiatives will be delivered.

Economic Developments of Note

- April marks the 94th month for the current economic expansion, the third longest in U.S. history (1960's and 1990's were the two longest).
- The U.S. economy grew at its weakest pace in three years in the first quarter as consumer spending barely increased and businesses invested less on inventories. Gross domestic product increased at a 0.7% annual rate, the weakest performance since the first quarter of 2014. The economy grew at a 2.1% pace in the fourth quarter of 2016.
- The latest annual inflation rate for the United States is 2.1%, exceeding the Fed's target of 2% for the first time in nearly five years. The increase in inflation may provide support for the Fed to continue its plans to move interest rates up in 2017.
- In March, it was reported that employers slowed their pace of hiring. However, unemployment was reported at 4.5%. The March unemployment rate was the lowest in almost a decade. It was also reported that private-sector workers saw average earnings rise 2.7% in March compared to the previous year. This is a sign that we are nearing "full employment" and competition is heating up to attract and retain employees.
- Activity in the manufacturing sector remained solid in April marking the eighth consecutive month of industrial expansion. One concern for the future, however, is the auto industry. After seven straight years of sales gains, including two consecutive record performances, auto demand has cooled in 2017 despite soaring discounts. Overall, auto makers sold 1.43 million

(continued on next page)

vehicles in the U.S. in April, down 4.7% from a year earlier. A record 17.55 million vehicles were sold in 2016.

- Exports were reported to be higher by 7.2% this year. This is a positive sign to future economic growth.
- Home prices have continued their impressive climb upward. The S&P/Case-Shiller Home Price Index, covering the entire nation, rose 7% in the 12 months ending in February. We anticipate that these gains will continue, perhaps at a slower rate, due to high demand, low inventories, as well as the overall positive financial condition of home buyers.

We expect that the economy will remain on a positive trend this year. We project GNP to be at 2% for the year as a whole. Job growth should remain positive this year. We expect home building and home sales to be positive. We think that the Fed will increase rates, but anticipate them to be cautious in how quickly they raise rates and reduce their holdings of securities.

Interesting Tid Bits

- It has been reported that several large auto lenders have decreased their emphasis on auto lending due to concerns about credit quality issues and auto resale values. A portion of this concern is related to the length of new car loans being made. Loans with original terms of between 73 and 84 months accounted for 18.2% of the market. It was further reported that 31% of consumers who traded in a car in 2016 did so in a negative equity position.
- China's banking system was reported as the largest by assets, reaching $33 trillion at the end of 2016. This compares to $16 trillion for the U.S. banking market.
- U.S. household net worth was reported at a record $92.8 trillion at year-end 2016. U.S. households lost approximately $13 trillion during the 2007-2009 recession. The eight-year rally since has added $38 trillion in net worth principally from rising stock prices and climbing real estate values.
- The Farm Credit System (a government sponsored enterprise) has over $314 billion in assets which would place it as one of the country's ten largest banks.
- A bankruptcy judge recently issued a $45 million fine against Bank of America. The action was in connection with a $590,000 residential mortgage loan and servicing issues related to its delinquency.
- We have been led to believe that small businesses employ the majority of Americans. This is no longer the case. Large companies (10,000 employees or more) employ over 25% of the workforce. Employers with more than 2,500 workers employ 65% of total employees.
- Nonbank lenders (i.e., Quicken Loans) were responsible for 51.4% of the consumer mortgage loans originated in the third quarter of 2016. This is up from 9% in 2009.
- People in the United States ages 65 to 74 hold more than five times the debt Americans held two decades ago.

Short-term interest rates ended April 30 up 29 b.p. from year-end with the 3-Month T-Bill at 0.80%. The 10-Year T-Note ended April at 2.29%. This is lower than December 31, 2016, when they were at 2.45%. This reflects a flattening of the yield curve.

The general stock market continued to climb to record levels in the first four months of 2017. The Dow Jones Industrial Index ended April up 5.96% for the year. Banks, after their spectacular rise after the election, retreated somewhat in the first four months of 2017. The broad Nasdaq Bank Index fell 4.05%. Larger banks were more fortunate (as measured by the KBW Bank Index) falling only 0.60%. Banks appear to have been more impacted by the uncertainty surrounding proposed tax cuts and less regulation than other companies.

(continued on next page)

38 YEARS 1978 - 2016

Merger and Acquisition Activity

For the first four months of 2017, there were 77 bank and thrift announced merger transactions. This compares to 83 deals in the same period of 2016. The median price to tangible book for transactions involving bank sellers was 159% compared to the 133% median value for all of 2016.

Capital Market Services

Young & Associates, Inc. has been a resource for banks for over 38 years. Through our affiliate, Capital Market Securities, Inc., we have assisted clients in a variety of capital market transactions. For more information on our capital market services, please contact Stephen Clinton at 1.800.376.8662 or sclinton@younginc.com. ❑

Young & Associates, Inc. Welcomes Two New Consultants

Will Enhance Lending and Compliance Divisions

We are pleased to announce the addition of 2 new consultants to the company.

David Dalessandro, Senior Consultant

David Dalessandro brings over 30 years of banking, regulatory, and industry experience to Young and Associates, Inc. Building on financial and tax basics from an accounting degree at Penn State and work at large and regional accounting firms, David has focused on detecting and resolving problem commercial loans, including workout, legal, and documentation strategies. He has specialized in improving loan and credit administration functions where financial institutions were under an increased level of regulatory scrutiny. Most recently, David served as Chief Credit Officer of a $1B community bank in Northeast Ohio. Prior to that, he served as Credit Audit Director for a large regional bank where he was responsible for the credit risk management auditing for $35 billion of commercial credit. He was also responsible for all commercial and credit activities as a Senior Vice President for a number of community banks, and has developed and delivered training for the Federal Reserve Bank of Cleveland, the Federal Reserve Board in Washington, DC, and the Ohio Society of CPA's. He has also been an Accounting instructor for Kent State University, East Liverpool and Ashtabula campuses. David has been awarded Examiner status with the Federal Reserve Bank of Cleveland and Certified Public Accountant (inactive) by the Pennsylvania Institute of CPA's.

David can be reached at 330.422.3487 (direct line), 800.525.9775 (main line), and ddalessandro@younginc.com.

Dale Neiss, CRCM, Consultant

Dale Neiss is a compliance consultant with Young & Associates, Inc. With over 30 years of banking experience in Denver, CO, Dale has developed and implemented compliance management systems, loan review and community reinvestment act (CRA) programs, and enterprise risk management (ERM) framework for multiple banks. He has held the titles of Compliance and Loan Review Manager, BSA and CRA Officer, and Enterprise Risk Management Director. Prior to his Denver, CO banking experience, Dale began his banking career with the Office of the Comptroller of the Currency in Indianapolis, IN as an associate national bank examiner. At Young & Associates, Inc., he provides consulting and training, as well as writes articles and compliance manuals. He holds the designation of Certified Regulatory Compliance Manager (CRCM) by the Institute of Certified Bankers in Washington, D.C. Dale earned a Bachelor of Business Administration degree in Finance and Management from Kent State University.

Dale can be reached at 330.422.3488 (direct line), 800.525.9775 (main line), or dneiss@younginc.com. ❑

38 YEARS 1978 - 2016

Annual Reviews of Commercial Credits

By: David G. Dalessandro, Senior Consultant

What is the overall condition of your commercial loan portfolio? Do you focus on net charge-offs? Delinquencies? Financial statement exceptions to policy? Number and level of TDR's and non-accruals? The percent of the ALLL to total loans? While all of these broad measures can be helpful, the number and nature of grade changes coming from internal annual reviews are likely to be more timely and accurate than all of the other measures combined.

Does your credit policy contain specific criteria describing relationships which must receive annual reviews? If so, have you recently evaluated whether that level remains appropriate for your portfolio today? The commercial annual review threshold should be set at a level where the required reviews will cover at least 50% of commercial exposures. Each bank should do a sort of the commercial portfolio and determine what level of exposure will yield the desired coverage ratio. Note that the annual review requirements should differ from the Watch List or Special Asset requirements as the annual reviews should be separate from those assets already identified with some level of weakness.

Now that you have set an annual review requirement, what elements of a credit analysis should be completed? Although the ultimate goal is to determine the accuracy of the risk rating, regulators will be looking for the robustness of the annual review in order to "sign off" or accept the annual review results. Note that in addition to providing executive management and the board with timely and accurate results, a solid and meaningful annual review process can help to build confidence in your systems with the regulators and potentially allow for a more efficient third-party loan review.

Minimum requirements for annual review activities should be built into the loan or credit policies so that management and the board can demonstrate to regulators that they are determined to ensure risk ratings and, therefore, that the ALLL and criticized and classified reporting is accurate.

The annual review procedures should include the following:

a) Detail of the relationship being reviewed including borrower, guarantors, SBA or other guarantees, and note numbers included.

b) Update of all borrower/co-borrower financial information used in the original approval or the latest renewal which would include spreads, debt coverage calculations, loan-to-value calculations, borrowing base analysis, etc.

c) Update of all guarantor financial information including a new complete and signed personal financial statement, most recent tax returns, and, for individuals, an updated credit report.

d) Statement of how the account has been handled since the previous annual review (or approval), including any delinquency of payment, financial information, or supporting information such as insurance, borrowing base reporting, etc.

e) In most cases, site visits by the loan officer or relationship manager or other representative of the company should have occurred since the previous annual review or approval. For CRE loans, the documentation of the visit should include perceptions by the representative of the condition of the property, occupancy trends, whether or not any deferred maintenance was noted, and if there were any changes in the neighborhood. For all credits, the representative should also use this visit to become updated on any material changes in the customer base, management, operating personnel, market conditions, condition of equipment or other fixed assets, and any other information that would help to understand the customer.

f) Update of any approval conditions and whether or not the borrower is maintaining those conditions, including any promises of deposit accounts,

(continued on next page)

financial reporting, property improvements, and compliance with any financial or other covenants.

g) Confirmation that the existing risk rating is accurate or recommendations to change the risk rating up or down, and the factors that the change is based on.

The financial institution that is covering 50% of its commercial portfolio, every year, with robust and timely annual reviews should provide executive management and the board with sufficient information to understand the level and direction of credit risk and whether or not these are in accordance with the desired risk appetite.

For more information on this article or on how Young & Associates, Inc. can assist your institution in this area, please contact me at 330.422.3487 or ddalessandro@younginc.com. ❑

Regulatory Compliance Update

By: Bill Elliott, Senior Consultant and Manager of Compliance

We usually try to use this space to share information that will help you prepare for what has been released, and for what will be required in the coming months. However, at this writing we find ourselves in a unique position; almost nothing (at least in the near term) is changing is the world of compliance. That does not mean that we can relax too much, just that we have a little time to catch up and get ready for the next round of changes.

Here is a sampling of where we are today:

- **Expedited Funds Availability (Regulation CC) Update:** The CFPB promised it for late last fall, but have not yet released it. (Note: this is maybe their fifth release date.) They have been working on it for about 6 years.
- **Privacy (Regulation P) Update:** This was also promised for last fall, but it has not yet appeared. In the interim, the prudential regulators have stated that banks that do not share (and therefore have no opt out) can follow the new privacy law. This means no annual privacy notice mailings of any kind, unless your privacy notice has to change. If you do change your notice and/or start to share, you will have to mail the new notice to all customers annually, so you may want to think about the mailing expense before you make any changes that would require the annual mailing.
- **Prepaid Cards Update:** The new prepaid card rule has been delayed for six months (April 2018) to allow for the changes that will essentially turn all prepaid cards that have the ability to be reloaded into an "account." They will then have rights similar to an account holder; they can ask for transaction histories, dispute items, etc. This is probably going to make these cards more expensive and therefore less attractive to your customers, and may end up not being a profitable item for many banks.
- **TRID Update:** They have published a proposal, but we will have to wait to see what the final rule looks like. It will be a number of months at least before anything is finalized on this subject.
- **Home Mortgage Disclosure Act Update:** The major item on the compliance agenda for 2017 is the Home Mortgage Disclosure Act. Management needs to assure that staff training occurs – and soon. We created a manual for our live seminars that runs 210 pages. We also created a listing of every possible code that might be needed, and that runs 33 pages in Excel. So this will not be an easy transition, and waiting until December to think about it does not seem like a good idea. If you do not have an LEI number and you are a HMDA bank, you should get it very soon. It will be required for 2018. We should also mention that the CFPB published a 150-page update with changes and corrections to the HMDA rule. These changes should be final by the first of the year.

"The major item on the compliance agenda for 2017 is the Home Mortgage Disclosure Act."

(continued on next page)

Stay Tuned

We will continue to use the newletter to keep you informed as the CFPB finally publishes updates and new regulations. But in the near term, the staff can work on absorbing what already has been issued. If we can help in any way, please feel free to call Karen Clower at 330.422.3444 for assistance. She can also be reached at kclower@younginc.com. ❑

ADA Website Audits

By: Mike Lehr, HR Consultant

Clients of Young & Associates, Inc. have been receiving demand letters from plaintiffs' law firms, alleging that their websites aren't accessible to individuals with disabilities. In effect, these letters claim that they are violating Title III of the Americans with Disabilities Act (ADA). More press and training have surfaced on this issue too.

If your bank has received such a letter, don't ignore it. Attorneys we know have had to defend their clients in court over these letters. If your bank has not received one, it's best to begin working with your legal counsel and reviewing your website before you do. Proactivity can help here.

In our audits to date, the main problem has been clients relying too heavily on assurances from their website vendors and on results from compliance software. Auditing software is a tool, not a judge. As a result, individuals with disabilities might be able to access the website, but they have unreasonable difficulty doing so. The website still isn't in the clear.

That's why Young & Associates audits employ four tests:

1. Compliance software tests
2. Manual audit of home pages, main navigation pages, and high problematic pages
3. Screen reader test by Young & Associates consultant
4. Screen reader test by a sight-impaired person observed by Young & Associates consultant

Young & Associates audits use the **Web Content Accessibility Guidelines (WCAG) 2.0** and the **Section 508 Standards** for federal agencies as their baselines. To meet our clients' many different needs, we have three different audits to select from:

1. **ADA Developmental Website Audit:** The purpose of this audit is to assist the bank in the development of a new website or to provide a cost-effective first look at a current website that has never been audited or tested in any manner. It employs the compliance software test, the manual audit, and a modified screen reading test.

1. **ADA Compliance Website Audit:** The purpose of this audit is to perform a formal compliance audit of the website. It employs the full complement of tests.

1. **ADA Follow-Up Website Audit:** The purpose of this audit is to review the changes made to the website in response to the findings of other audits. It usually employs just the compliance software test or a modified application of the full complement of tests.

For more information on ADA Website Accessibility Compliance or how Young & Associates, Inc. can assist your bank in this area, download our "Better Understanding ADA Website Compliance & Young Associates Audit," or contact Mike Lehr, Human Resources Consultant at 1.330.777.0094 or mlehr@younginc.com. ❑

ADA Policies

For information on our customizable ADA Accessibility Policies see page 11.

38 YEARS 1978 - 2016

Capital Planning System – Updated 2/17

Assess capital adequacy in relation to your bank's overall risk and develop a customized capital plan for maintaining appropriate capital levels in all economic environments. **Our 2017 Update addresses the impact of growing cybersecurity risks, as well as the impact of the anticipated tax reduction from a capital planning perspective.**

Allows you to:

Develop a Base Case Scenario in which minimum capital adequacy standards are established.

Identify and Evaluate Risk for Your Bank. Parameters in this analysis have been field-tested in our work with banks over the years and closely resemble adequacy standards established in consent orders.

Stress Test Capital by loan classification (as recommended by the FDIC and OCC).

Perform Contingency Planning for stressed events. All assumptions are stressed to determine the amount of capital needed and possibilities for increasing capital are examined.

Generate Your Capital Plan in as Little as 1 Day! Data from the Microsoft® Excel spreadsheets can be easily transferred directly into a Word document that can be customized to fit the unique circumstances at your bank. Sample language and suggestions for changing the narrative are provided.

First Year License Fee (#304) – $1,095
Update/Annual License (#306) – $495

American with Disabilities Act (ADA) General Accessibility Accommodations Policy (#328) – $125

Describes the bank's intention to ensure that its services are accessible and accommodating to individuals with disabilities. Includes a policy statement; roles and responsibilities of bank board, executives, committees, and employees; grievance processes; and contact for inquiries, questions, assistance, and general information.

American with Disabilities Act (ADA) Website Accessibility Accommodations Policy (#327) – $125

Addresses the need for the bank's website to provide equal treatment to all its customers and the public under Title II of the ADA, the Rehabilitations Act of 1973, and Department of Justice (DOJ) web accessibility directives in accordance with Web Content Accessibility Guideline (WCAG) 2.0 Level AA and the United States Access Board's Section 508 Standards. Includes a policy statement which is suitable for public documents; policy application; roles and responsibilities; complaint process for improving accessibility and accommodations; and contact for inquiries, questions, assistance, and general information.

Liquidity Toolkit (#273) – $1,250

Includes:

- **Liquidity Cash Flow Planning Model (#271):** Forecast funding sources, funding needs, and cash flow gaps. Monitor availability of contingent liquidity. Monitor funding concentrations and dynamic cash flow ratios. Perform liquidity stress testing and multiple-scenario what-if analyses. (*regularly $950*)
- **Liquidity Contingency Funding Plan (#272):** Delineates strategies and actions addressing potential liquidity shortfalls in emergency situations. Includes identification of stress events, stress levels, early warning indicators, parameters for liquidity stress testing, sources of funds and funding strategies, lines of responsibility and communication, as well as a detailed crisis action plan. (*regularly $275*)
- **Liquidity Management Policy (#096) :** Customizable policy designed to ensure that the bank is managed to provide an adequate level of liquidity to meet both predicted and unexpected cash needs while maintaining a planned net interest margin. (*regularly $225*)

System Requirements: Microsoft Word 2007 and Excel 2007 or higher

Save $200 when you purchase the Liquidity Toolkit.

Threat Intelligence Program (#324) – $299

Includes:

- **Threat Intelligence Program:** Documents the requirements for the institution's threat intelligence program, including threat intelligence sources, the monitoring process, the analysis and response process, documentation requirements, and the reporting process
- **Threat Tracking Summary Worksheet:** Microsoft® Excel-based workbook for tracking threat notifications and responses
- **Threat Tracking Detail Worksheet:** Microsoft Word-based worksheet for tracking details about the threat analysis and response process performed for each specific threat
- **Information Systems Event Management Policy**: Policy template that documents the requirements for information systems event management procedures
- **Event Management Procedures for Specific Systems Worksheet:** Excel-based workbook for documenting the event management procedures for each information system

System Requirements: Microsoft Word 2007 and Excel 2007 or higher