90 Day Note

August 2017 Vol. 31, No. 2

A Young & Associates, Inc. Publication

The Changing Role of the Community Bank IT Manager

By: Mike Detrow, CISSP, Senior Consultant and Manager of IT

At small community banks, the IT Manager role was once, and in some cases still is, one of many hats worn by the President or CFO. However, this role is quickly evolving into a nearly full-time position even at smaller community banks. There are a number of factors that are contributing to this change, including increased use and sophistication of technology, increased regulatory scrutiny for cybersecurity, and the rapidly changing threat landscape.

It was not long ago that the IT Manager only needed to support a few internal servers and workstations. Over time, technology and customer expectations have evolved, leading to increased network complexity through the requirement for additional internal servers to support new services, the use of server virtualization, and connectivity to additional outside networks. In addition, the use of mobile technology has expanded dramatically leading to employees using mobile devices to access internal network resources, and banking services being provided to customers through their mobile devices.

The amount of time required to properly manage and monitor a bank's information systems has increased dramatically. However, in many cases, community banks have not significantly increased the human resources assigned to the management of their IT environment. We have had numerous discussions with bank IT personnel indicating that they do not believe that they have enough time and resources to properly address the changing IT regulatory requirements and new cyber risks. While some community banks have outsourced the management of their network and other systems to a service provider, this does not relieve the bank of its role in the oversight of these systems. Additionally, outsourcing increases the time that the bank must spend to manage these vendor relationships.

Here are some of the areas where we have seen community banks spending additional time to perform IT and information security functions:

- **Vendor Management.** As the bank implements new services or engages service providers to manage existing services, additional time is required to monitor these vendors. Significant time is needed to obtain the required documentation from each vendor and to review and analyze this documentation.
- **Threat Intelligence.** Threat intelligence sources are monitored to identify threat sources and their current activities to identify and implement mitigating controls that will limit the potential impact of these activities on the bank. Significant time can be spent analyzing the data from threat intelligence sources to determine its applicability to the bank and to then implement or modify mitigating controls.
- **Risk Assessment and Policy Maintenance.** As the bank adds or changes technologies or services, risk assessments and policies must be created or updated to address their risks. In addition, risk assessments need to

(continued on next page)

Inside This Issue:

"Many experts say that it is not a question of if a business will be hit by some form of breach, but a question of when it will happen. Banks must have a well-documented plan in place..."

be updated periodically to ensure that the risks associated with new or changing threats are evaluated and mitigated. A cybersecurity assessment must be completed and reviewed periodically based on changes within the bank's IT environment.

- **Ongoing Employee Information Security Awareness Training.** With most banks providing external email access and internet access to all of their employees, each employee has become a critical link in the security chain where the result of one employee clicking on a malicious link in an email can be an organization-wide catastrophe. Annual training is no longer adequate to keep employees apprised of current threats such as ransomware and phishing scenarios. A significant amount of time can be spent developing training materials and distributing them to employees on an ongoing basis.
- **Event Management and Monitoring.** Network devices, operating systems, and applications must be monitored to identify malicious activity. In the past, many banks were only monitoring perimeter devices such as firewalls and believing that the perimeter devices would stop any threats. However, many current attacks start with the installation of malicious code on an employee's workstation to bypass the controls imposed by the firewall and then the attacker moves around, potentially undetected on the internal network. Monitoring for malicious activity on all of the bank's internal network devices can require significant resources.
- **Patch Management.** Patch management is more than just patching Microsoft operating systems and applications such as Adobe Acrobat and Java. Patch management includes updating the software running on network devices such as firewalls, routers, switches, DVRs, and printers to address any known vulnerabilities. Additional time must be spent to identify the release of new patches, and in many cases the patches must be installed manually on each network device.
- **Disaster Recovery / Business Continuity Planning and Testing.** A bank's increased dependence on technology requires formal documentation for maintaining business continuity and testing the selected plans to ensure that the bank can recover from a disaster within a reasonable time frame to allow for the continued performance of its daily functions. Additional time is required to initially document recovery strategies and then modify the strategies based on system or vendor changes. Time is also required to prepare testing strategies, coordinate testing schedules with vendors, and analyze the test results.
- **Incident Response Planning and Testing.** Many experts say that it is not a question of if a business will be hit by some form of breach, but a question of when it will happen. Banks must have a well-documented plan in place to detect and respond to an information security incident. In addition, the plan needs to be tested periodically to ensure that all employees are aware of their roles to effectively and efficiently respond to an incident.

Potential Costs of a Breach

Why should changes to the technology used by the bank, changes to regulatory requirements, and the evolving threat landscape be a significant concern for the board of directors? The board of directors is ultimately responsible for the management of the information security program, and failing to provide the appropriate resources to manage the IT and information security functions at the bank can lead to regulatory enforcement actions, harm to the bank's reputation, and significant costs associated with a data breach.

According to the Ponemon Institute's 2017 Cost of Data Breach Study: United States, performed June 2017, the average cost for each lost or stolen record containing sensitive and confidential information is $225. This study also indicated that breaches involving businesses within the financial services industry had a per capita cost of $336.

↓ *(continued on next page)*

Insurance Coverage

Another consideration for the board of directors is insurance coverage. While a bank may have a cyber insurance policy, management needs to thoroughly understand the requirements for this policy and ensure that it is meeting all of the minimum security requirements of the policy. Insurance companies may reject a claim or even seek repayment of a settlement if defined controls were not in place at the bank at the time of a breach.

Using the example of a community bank with assets of 100 million and 12,000 customer records, a breach of those 12,000 records could cost the bank 4 million dollars. This would be a substantial loss for the bank if insurance coverage is not appropriate, and even more significant if an insurance claim is denied due to the bank's failure to maintain the minimum security requirements defined within the policy.

Continuing Education

With the rapid changes in technology and the changing threat landscape, continuing education for the bank's IT staff is also a critical consideration. A bank's IT Manager must learn how to change the bank's mitigation strategies to address evolving cyber threats rather than relying solely on the strategies that have been used in the past. There are numerous options for continuing education such as cybersecurity conferences sponsored by state banking associations and webinars.

Cybersecurity Assessment Tool Staffing Requirements

With the regulatory focus on cybersecurity, another illustration of the need to evaluate the human resources required to effectively manage the bank's information systems can be found in the declarative statements within the staffing section of the FFIEC's Cybersecurity Assessment Tool as shown below. Attainment of the baseline cybersecurity maturity level is required for all banks as this level identifies the minimum expectations required by law, regulations, or supervisory guidance. The declarative statements within the evolving cybersecurity maturity level will also need to be attained by small community banks as they increase their maturity level over time.

Baseline

- Information security roles and responsibilities have been identified.
- Processes are in place to identify additional expertise needed to improve information security defenses.

Evolving

- A formal process is used to identify cybersecurity tools and expertise that may be needed.
- Management with appropriate knowledge and experience leads the institution's cybersecurity efforts.
- Staff with cybersecurity responsibilities have the requisite qualifications to perform the necessary tasks of the position.
- Employment candidates, contractors, and third parties are subject to background verification proportional to the confidentiality of the data accessed, business requirements, and acceptable risk.

Conclusion

In summary, the board of directors and senior management must carefully consider the resources required to appropriately manage its information systems based on the rapid technological, regulatory, and threat landscape changes. Strategic plans should consider the additional workload that will be created to support changes within the bank's IT environment to achieve management's strategic goals, and ensure that appropriate human resources are included within its plans.

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

Developing a Consensus on Capital Adequacy

The First Step in Strategic Planning

By: Gary J. Young, Founder and CEO

The most critical component of every strategic plan is a thorough understanding of your position on capital adequacy and your target for capital. They are not the same.

The Regulator View of Capital

As community bankers, we have all heard the mantra that we need to increase capital. It may be an over simplification, but to the regulator more is always better. The regulator does not have interest in your shareholders. And as I will discuss later in this article, an increase in capital lowers the return on equity, or the return to shareholders. The regulator's #1 job is to ensure a safe and sound banking system. Your job is to satisfy the regulators and your shareholders. You have to balance the interests of both. You need to proactively communicate your bank's opinion regarding capital.

An example of the need to balance is shown below. 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. The amount of capital provides a significant difference in the return to shareholders.

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

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 that if capital falls below, the Capital Contingency Plan must be implemented. 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 desired 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%.

(continued on next page)

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 these 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.**

Strategic Planning

After there is agreement on capital based on risk, planning can begin on the methodology or methodologies to best utilize any existing or planned excess capital. The recommended considerations that follow do not address all of the issues within your mission statement or vision statement. Rather, these address your desire to maximize shareholder return and to maintain your bank's independence.

Consider the following:

- **Ways to generate additional organic growth.** This means growth from your market without any significant increases in infrastructure. This is normally the most profitable short-term methodology.
- **Expansion opportunities.** I would suggest looking for opportunities that begin turning a profit in two years or less. While this is long-term, most bankers are in for the long haul. Remember, a branch that increases net income by $500,000 increases shareholder value by $6,500,000, assuming a 13 price-earnings ratio.
- **The purchase of another bank or branches.** This can significantly impact capital, but once the target is effectively absorbed by your bank, the value rewards can be great. But, also make sure you adequately consider the risks.
- **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. I look at this as buying your bank as opposed to buying another bank. I recommend to every client that has a tier-1 leverage ratio in excess of 9% that they should at least consider a stock repurchase.
- **A slow, steady increase in dividends to shareholders.** If after all other approaches to capital utilization excess capital remains, then increase the dividend. This will increase dividend income to shareholders without jeopardizing capital adequacy.

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.

Contact

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

Mary Green Earns CAFP Designation

Young & Associates, Inc. is pleased to announce that Mary Green, Consultant, has earned the industry designation of Certified AML and Fraud Professional (CAFP) by the Institute of Certified Bankers, a subsidiary of the American Bankers Association (ABA). This certification demonstrates the ability to detect, prevent, monitor, and report current and emerging money laundering and fraud risks. ❑

Capital Market Commentary

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

Market Update

The U.S. has entered the ninth year of economic expansion. While the growth has not been spectacular, it has been steady. GDP expanded at a 2.6% annual rate in the second quarter. The GDP growth in the current recovery has averaged 2.1%. This compares to the 3.6% average of the 1990's recovery and the 4.9% average for the 1960's expansion. (These are the most recent economic recoveries of comparable length to the current expansion.)

- American's largest companies were reported to be on pace to post two consecutive quarters of double-digit profit growth for the first time since 2011. Factors explaining the growth in profitability include a weaker dollar that helped U.S. exports, limited wage growth, and cost cutting programs.
- Unemployment was reported at 4.4% in June, near the lowest rate in a decade.
- Despite nearing full employment, wage growth has increased only modestly. It was reported that wages increased .5% in the second quarter.
- At the Federal Reserve meeting in July, the Fed held interest rates unchanged but announced that it soon will begin to shrink its securities portfolio. The Fed currently holds more than $4 trillion of investments; a large portion of these were purchased as part of the Fed's quantitative easing programs.
- Consumer spending rose at a 2.8% pace in the second quarter, an increase from 1.9% in the first quarter. However, concerns remain about the spending outlook at a time of soft wage growth, stalling car sales, and a growing overhang of auto and student-loan debt.
- U.S. business investment rose for the second straight quarter. In the second quarter, nonresidential fixed investment advanced at a 5.2% pace. That comes on the heels of a 7.2% gain the prior quarter. The continuation of strong business spending suggests firms have confidence in the durability of the economic expansion.
- The U.S. housing market continues to improve. After falling throughout the usually busy spring season, the monthly index of signed contracts to purchase existing homes increased 1.5% in June compared with May. The Case-Shiller Index, which measures the increase in home prices across the country, rose 5.6% in the 12 months ending in May.
- Overall, inflation continues to be held in check. The U.S. inflation index was 1.4% in May, well below the Fed's 2% target.

The stock market has reached all-time highs. This has occurred despite the lack of action on President Trump's plans for lowering taxes and economic stimulus. Should these initiatives be enacted, 2017 should be a very good year for investors.

Interesting Tid Bits

- The New York Times recently reported that homeowners now stay in their homes for an average of 8½ years, up from the 3½ year average in 2008.
- Twenty years ago, there were 7,322 listed public companies in the U.S. At the end of 2016, there were only 3,671 companies publicly traded on U.S. exchanges.
- Deer & Co., the maker of farming equipment, is the fifth largest agricultural lender. This is in addition to the billions that they lend to farmers to fund purchases of their farming equipment.
- It is widely anticipated that the Libor index will be phased out over the next five years. Libor is used to set the price on trillions of dollars of loans.

Short-term interest rates have moved up in response to the Fed's actions of increasing short-term rates with the 3-month T-Bill ending July at 1.07%.

(continued on next page)

The 10-year T-Note ended July at 2.30%. The yield curve has flattened this year with the 10-year T-Note falling 14 basis points while short-term rates moved up 56 basis points.

The general stock market reached historic highs in July. The Dow Jones Industrial Index ended July 31 at an all-time high and was up 10.77% for the year. The Nasdaq Index closed up 17.93% for the year. Banks have under-performed the general stock market this year. The Nasdaq Bank index was down 3.10% for the year. However, since the election, bank stocks are up 22.50%, which is a larger increase than the Dow Jones Industrial Index since the election.

Merger and Acquisition Activity

Through July there were 147 bank and thrift announced merger transactions. This compares to 151 deals for the comparable period in 2016. Despite the slightly lower number of deals, the total assets involved in transactions increased from $109 billion to $124 billion. The median price to tangible book for transactions involving bank sellers was 162%.

Where is the UCA/FAS 95 Analysis?

By: David Dalessandro, Senior Consultant

In the summer of 1987, the savings and loan I was working for at the time sent me to a "cash flow" seminar in Norman, OK. I had graduated from Penn State a few years before and had recently accepted my first of what would prove to be many positions in banking as a credit analyst. At that point, my experience at financial analysis was limited to what I had absorbed from two accounting firms I had worked for and studying for (and passing) the CPA exam. The seminar topic was "The Implications of FASB 95."

FASB 95, for those of you asking, was issued in November 1987 and was to be utilized in all financial statements finalized in fiscal years ending after July 15, 1988. The requirement replaced the famous APB 19, Statement of Changes in Financial Position, which we all knew and loved as a pretty worthless financial statement at the time, because no one without a CPA attached to their name understood it, and most CPAs had difficulty explaining it.

The seminar turned out to be one of the most beneficial events in my life. As it was explained, the Statement of Cash Flows, as required by FASB 95, was a financial disclosure that would trace every dollar of cash through an accounting period. How awesome, I thought, because only cash pays back loans. So now if I have a tool to trace every dollar of cash, credit analysis would be a cinch.

Well, fast forward 30 years…and the Statement of Cash Flows is still not a household name in Credit Analysis. Most financial institutions, even the largest, still hang onto EBITDA for "cash flow" or multiples of EBITDA for "value." The EBITDA analysis may approximate real cash flow for real estate rental properties, but for those thousands of enterprises that carry Accounts Receivable, Accounts Payable, Inventory, Other Assets, and Other Liabilities, pay distributions, report gains and losses on sales of assets,

(continued on next page)

take charge downs on intangibles, write off bad debts, and enter into other "non-cash" transactions, the Statement of Cash Flows is the only real way to "follow the money."

The question here is, why would any financial institution NOT at least include FASB 95/UCA in cash flow analysis when it was appropriate? EBITDA, or even EBITDA adjusted for one-time items, may give the analyst an estimate of total cash flow, but true operating cash flow can only be obtained from a properly and timely prepared Statement of Cash Flows. The Statement separates the movement of cash into three primary categories: Operations, Investment, and Financing. From a bank or financial institution standpoint, if there is positive cash flow from the Investing segment or from the Financing segment, then the enterprise is selling assets or obtaining more loans or selling stock in order to make its loan payments. Are those sources sustainable? Are those sources where you want your customer to come up with the funding to make your loan payments? Is the quality of cash flow from Investing or Financing equal to that of Operating Cash Flow? Probably not. But if the cash flow from operations is positive, and it has been positive for a number of years and it is sufficiently positive to fund all loan payments, then that should be a sustainable source of cash flow far into the future. If the Operating Cash Flow is positive enough to fund loan payments, pay distributions/dividends, AND fund capital expenditures, then that enterprise is more than likely to enjoy a very strong financial condition with relatively easy debt coverage.

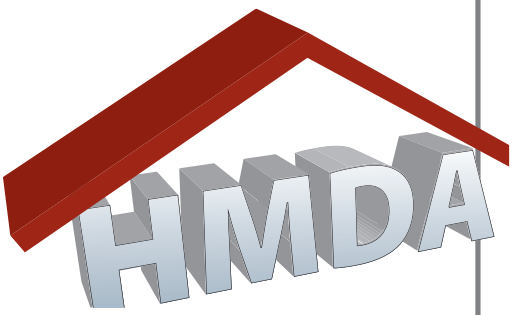
"...true operating cash flow can only be obtained from a properly and timely prepared Statement of Cash Flows."

If your underwriting protocols do not include UCA/FAS 95/Statement of Cash Flow analysis, then you risk being surprised when a borrower who had "good" EBITDA coverage shows up past due or comes to you needing more money. Use this tool in conjunction with your standard analysis and it will enable you to rethink loan structures where the expected cash flows do not match up.

If you would like to discuss incorporating UCA/FAS 95/Statement of Cash Flow analysis in your institution, please contact me at 330.422.3487 or ddalessandro@younginc.com. ❑

HMDA 2018

By: Bill Elliott, CRCM, Senior Consultant and Manager of Compliance and Adam Witmer, CRCM, Senior Consultant



Beginning in 2018, you will be faced with two major changes to Home Mortgage Disclosure Act (Regulation C 12 CFR § 1003). They are:

1. Changes to the existing rules
2. Addition of new rules

While the new rules will be challenging to navigate, the changes to the existing rules could prove to be extremely challenging, as long-established procedures and understandings are going to change. The following are a list of some of the biggest modifications.

Reporting Changes

Loan Volume Test. The new rules have two separate loan volume tests, one for closed-end and one for open-end.

The closed-end test is 25 covered loans. If your bank originates 25 "covered" loans (defined as not excluded closed-end loans or open-end loans), you will then report closed-end loans.

The open-end test is 100 covered loans. If your bank originates 100 open-end covered loans, then you will report open-end loans. There is a regulatory proposal to change this to 500 open-end for a couple of years, and we expect that to occur. The challenge here relates to business purpose loans.

(continued on next page)

All consumer purpose loans (generally HELOCs) will count, but business purposes loans may also count. Excluded loans will be open-end loans (such as an equity loan for operating expenses) that are not for a purchase, refinance, or home improvement purpose. But open-end loans such as this are refinanced, and will become reportable.

If your financial institution only meets one test, you only report the type of loans for the test you meet. This means some institutions will only report closed-end loans. Some will only report open-end loans. And others will report both.

Dwelling Secured. Under prior HMDA rules, one definition of Home Improvement included loans that were not secured by a dwelling. Under the new rules, only loans secured by a dwelling will be reportable.

Temporary Financing. The rules now only talk about financing that will be replaced by new financing. The old rules specifically excluded construction and bridge loans.

Agricultural Loans. The new rules now exempt all agricultural loans. In the past, the agricultural loan exemption only applied to purchases, which meant that when an agricultural loan was refinanced, it required HMDA reporting. Now, all agricultural purpose loans are exempt.

Preapproval Requests. Preapproval requests that are approved but not accepted are now required reporting rather than optional reporting.

Submission Process. The CFPB is going to use a cloud-based program for HMDA submissions. This means that reporters using the FFIEC software are going to have a much more difficult time. You will want to think about software options. If you are not using third-party software already, you will need to work out logistics of using the new reporting system.

"Time is growing short. If your institution is going to be subject to the new rules, then training for everybody involved in the process is necessary."

Items to Consider

Our training manual for our live HMDA presentation runs 210 pages, so this is just an overview of some of the items that must be considered. Time is growing short. If your institution is going to be subject to the new rules, then training for everybody involved in the process is necessary. And for most readers, this will include more than one person.

For the future, if you are not subject to the HMDA regulation, be careful of expansion. If you open a branch in an MSA, suddenly HMDA will become part of your life. So beware of a good deal on the land or the lease – the costs of HMDA could easily dwarf the savings. If you are a HMDA reporter already, remember that any compliance requirement only gets paid for one of two ways – the applicants/customers pay for it, or it comes out of the stockholder's pocket. Fee changes may be in your future.

HMDA Tools – Coming Soon

Young & Associates, Inc. is currently developing a HMDA Toolkit which will be available shortly, as well as a customizable HMDA policy. As there is HMDA text that the CFPB is changing and correcting (due out soon, we hope), we are not ready for release just yet. But we hope to keep the timetable reasonable. The HMDA policy will be available to purchase September 1, 2017.

We will also be offering an off-site HMDA Review beginning in 2018. We will review as many or as few loans as you would like to make sure you are on track. Billing will be based on the number of files reviewed, so you will control your costs.

Detailed information for all of these items will be available soon. If you are interested in the HMDA toolkit, HMDA policy, or HMDA reviews, we will be happy to discuss these products and services with you at any time.

Good luck – we will all need it. For more information on this article or how Young & Associates, Inc. can assist you in this process, contact us at compliance@younginc.com or 330.422.3450. ❑

Capital Planning System – Updated 2017

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

Information Security Awareness Training Toolkit (#276) – $299

Designed to help your bank's Information Security Officer create a customized Information Security Awareness Training Program to educate bank employees on critical information security issues such as:

- Cybersecurity
- Intrusion Response
- Social Media
- Acceptable Use of IT Resources
- Workstation and Mobile Device Security

Includes:

- Training Script (provided in Microsoft Word)
- Customizable PowerPoint Training Presentation

Program Requirements: Training Script and Slides – Microsoft® Word 2007 and PowerPoint 2007 or higher

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