CompliancePro®
and the Compliance Risk Management Process

A Paper Published by American Bank Systems, Inc.
14000 Parkway Commons Drive
Oklahoma City, Oklahoma 73134
405 607 7000  405 607 7005 (fax)

www.americanbanksystems.com  www.compliancepro.com

March 1, 2011
Enterprise Risk Management

“Enterprise risk management is a process, effectuated by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”

Background

The April 2005 Basel Committee on bank supervision paper entitled Compliance and the compliance function in banks (Compliance Paper) establishes ten principles of sound practices for compliance risk management and oversight. Principles one through four detail the responsibilities of the board of directors and senior management; five through eight cover compliance function principles; and principles nine and ten discuss cross-border issues and outsourcing, respectively. While all ten principles are vital to the establishment and maintenance of an effective enterprise-wide risk management program, this paper focuses on those principles covering the risk assessment and monitoring processes.

Consistent with COSO’s (the Committee of Sponsoring Organizations of the Treadway Commission) definition of enterprise risk management, the Compliance Paper assigns responsibility for approving and implementing a compliance program to the board and senior management. The program should include a process, conducted at least annually, to identify and assess the significant compliance risk issues facing the institution, provide for prompt reports of material compliance issues and annual reports to the board of sufficient detail for the board to reach a conclusion as to the efficacy of the institution’s compliance risk management program.

Further, the Compliance Paper stresses the need for the institution to have sufficient and independent compliance resources to perform its responsibilities under the program, including the responsibility to: identify, measure, and assess compliance risk; and monitor, test and report the results of compliance testing. While challenging for some institutions to attain, independence can be achieved through a variety of organizational structures and through strongly defined accountabilities. Resource sufficiency, however, is becoming increasingly difficult to attain. In fact, a recent Deloitte Center for Banking Solutions survey on compliance management concludes that “A top priority for financial institutions across the industry is to find ways to increase the efficiency of compliance process management, while becoming more effective at complying with increasingly complex regulatory requirements.” The Deloitte Study states that institutions need to systematize compliance management; reduce the redundancies in compliance processes; integrate compliance management with risk management; and, enhance compliance reporting.
Subsequent to the publishing of the Basel Compliance Paper, the Federal Reserve issued a Supervisory Letter (SR 08-8, dated October 16, 2008) which calls for a “firmwide” compliance risk management and oversight approach, especially for larger, complex financial organizations. Achieving a firmwide compliance risk management system requires the design and implementation of a comprehensive and cohesive automated approach. Separately based procedures usually are not brought together to achieve an overarching or firmwide risk management system. The purpose of this paper is to discuss the risk management process and how CompliancePro® provides a comprehensive, overarching system for compliance risk management.

The Risk Management Process

Regulatory agencies expect all financial institutions to implement and maintain a risk management system (commensurate with its size) to identify, measure, monitor, and control the risks associated with its various products and lines of business. Essentially, an effective system must have these four key elements and must be built on the foundation of active board and senior management oversight. In discharging its responsibility, the board will approve overall business strategies, approve significant policies, including those related to risk management, and retain a management team capable of managing the institution’s activities to meet identified goals within the defined risk framework and in compliance with laws and regulations.

Further, the board and senior management will establish policies and procedures to provide guidance for the day-to-day implementation of business strategies, including defining accountability, lines of authority, and risk limits designed to shield the organization from excessive and imprudent risks. The “inherent risk” in each product type within a line of business must be identified and measured, and internal controls established to manage the resulting “residual risk” within the predefined risk exposure limits for the organization.
Once the risks have been identified and risk limits established, adequate ongoing risk measurement, monitoring and management information systems provide the board and management with an effective method for evaluating risk exposures and adjusting the behavior of the organization to stay within its risk parameters. Comprehensive internal controls, including policies, procedures, and operating processes ensure that the residual risk is being managed and that the organization is compliant with applicable laws and regulations. The compliance monitoring process identifies issues requiring corrective action...and the process begins again.

The Compliance Risk Assessment Process

Assessing the compliance risk of an institution’s products and services is the beginning of the compliance risk management process. It is important to have a cohesive and well documented analysis of the inherent risk for each product and/or service offered and the mitigating internal controls which have been adopted by the company to manage that risk. This assessment process should be formalized, documented and revisited on at least an annual basis, but more frequently when key risk or performance indicators signal a potential change in risk resulting from an internal or external event, such as the identification of issues in the monitoring process, changes in the products/services provided, amendments to regulations, or an increase in related regulatory enforcement actions. As noted in SR 08-8, compliance risk, unlike credit or market risk, does not lend itself to quantitative measures. Therefore, each institution must make its own assessment of the inherent compliance risk of offering its products and services so that, after considering the controls which mitigate that risk, the overall appetite for risk defined by the board of directors can be a governing factor in deciding to offer such products/services. Many institutions assign broad risk measurements such as “low”, “medium” or “high”. Alternatively, a numeric scale – say one to ten – may be of greater value in reflecting more discrete movements of risk levels while still relating easily to this broader measurement. For example: an institution might consider values of one through three to be “low” risk; four to six to be “medium” risk; and seven to ten to be “high” risk.

Assessing the Inherent Risk of a Product or Service

The assessment of the inherent risk associated with each product or service should consider at least the following four factors:

- Complexity of the product or service;
- Operational risk associated with the product or service;
- Regulatory compliance risk associated with the product or service; and
- Legal and reputational risk associated with the product or service.
Regulatory comments concerning the analysis of these risk areas are general in nature and, yet, call for significant granularity in the analysis. For instance, in terms of the complexity of the product or service, the analysis should consider the level of judgment, academic or technical skill, and technology required to provide and support the product or service, the “newness” of the product/service, the interdependency between this and other products/services, and the number and complexity of regulations to which the product/service is subjected.

The analysis of operational risk must take into consideration issues such as the frequency of transactions and the aggregate number and dollar value of such transactions. The relative stability of the workforce and the total level of resources needed to support the product or service as well as the geographical dispersion of the product/service should also be considered. The level of risk from fraud, errors, or processing disruptions given the complexity and state of the company’s systems relative to the product/service is also important to quantify.

An evaluation of regulatory compliance risk is equally essential to the assessment. The level of regulatory focus and scrutiny evidenced by recent examination results and/or enforcement actions related to the product/service is important to the analysis. Changes in regulation, lack of clarity or official guidance surrounding the legal/regulatory requirements will impact the analysis as does the level of risk associated with internally identified violations or exceptions (as measured by their number or seriousness) relating to the product or service. The analysis of these factors, together with the level of risk stemming from the institution’s compliance examination rating, are key ingredients in determining the inherent risk associated with the product or service.

Finally, the legal and reputational risk associated with the product or service should be assessed. The level of potential regulatory fines, penalties and/or restitution related to the product or service must be identified. Clearly, products/services with significant levels of potential damages, settlements, legal and other fees arising from litigation are inherently riskier.
Also, the level of risk associated with the volume of customer complaints related to the product/service should be assessed. The likelihood of adverse publicity from a regulatory enforcement action or from adverse attention from consumer advocates and other special interest groups is another important consideration.

After making the initial assessment of the inherent risk related to a product or service, it is important to consider the trend in the risks identified when it is time to reassess the inherent risk. Incorporating the risk trend, identified as “stable”, “increasing” or “decreasing,” adds another layer of accuracy to the ongoing risk assessment of the product or service. The analyses related to the basic factors – together with the assessment of the trends in the risks – should be thoroughly documented.

The end result of the process is a quantification of the inherent risk associated with offering the product or service. Obviously the inherent risk of a particular product or service may differ between financial organizations – dependent upon the factors related to the product or service discussed above and the characteristics of the organization itself. But, such an analysis – when combined with an analysis of the mitigating internal controls and related factors – defines the expected compliance risk and gives management an approach to evaluate the risk against the institution’s defined risk appetite at any given point in time.

Assessing the Internal Control Factors Mitigating the Inherent Risk

Once the inherent risk related to a product or service has been determined – and the rationale for that inherent risk assessment documented – the mitigating factors or internal controls established to manage the risk should be assessed. Again, a framework for such assessment should consider at least four broad categories of controls:
- Product, service or process controls;
- Behavioral controls;
- Management controls; and
- Diagnostic controls.

In assessing the impact of the internal controls to mitigate the inherent risk of a product or service, each of these broad categories of controls should be analyzed. The evaluation of product, service or process controls will include a determination of the effectiveness of the institution’s change management process – that process which is applied to the introduction of new products, services, strategic initiatives or acquisitions. Regulatory guidance relating to change management is available in OCC Bulletin 2004-20. Additional elements to be considered in the evaluation of this control category include the level of self-monitoring performed to identify weaknesses in operating processes, information systems and controls, the level of automation, and the degree of centralization related to the product or service.

Evaluating behavioral controls is another important aspect of determining the mitigating factors. This category considers the effectiveness of the training programs as well as the level of compliance-related resources associated with the product or service. It also incorporates an assessment of the organization’s control culture, including the level to which compliance management and information systems are sound and the extent to which policies and procedures are drafted, implemented, maintained and disseminated throughout the organization. The final element to be evaluated in this category is the level to which authority and accountability for compliance are defined and enforced with respect to the product or service.

Management controls must also be assessed for each product or service in determining the risk which remains after application of the mitigating factors. Several factors are analyzed to
complete the assessment of this control category including the level of director oversight and management’s understanding of and commitment to compliance with respect to the product or service. Management reporting and information systems concerning the product or service and the level of management responsiveness to complaints from customers or employees relating to the product or service are important mitigating factors. The level of management’s implementation of corrective action when deficiencies are identified is also vital to measuring the impact of mitigating factors on the inherent risk and thus calculating the residual risk for each product and service.

Finally, the level and effectiveness of diagnostic controls should be considered. For example, the level to which controls and systems are implemented to identify compliance problems and assess performance should be considered, as should the extent to which changes in regulations or the regulatory environment are communicated to all affected personnel with respect to the particular product or service being assessed. The degree of consistency of findings identified by compliance monitoring, audit and regulatory examinations is another important mitigating factor which will be considered in evaluating this control category.

The analysis system should rate the strength of each of these mitigating factors – using a scale commensurate with that used for quantifying inherent risk rating (e.g., a one to ten scale) – and then apply the resultant level of combined control (using a weighted average) against the inherent risk of the product or service to calculate the residual risk associated with each product/service. This performance “scorecard” alerts management to those areas where the residual risk exceeds the pre-defined, board approved risk parameters thus requiring further analysis of the risk element and its associated control categories to determine the necessary actions to adjust the residual risk to an acceptable level. The adoption of a systematic risk assessment process supported by appropriate technology and integrated with a comprehensive risk-based compliance monitoring process provides a strong foundation for a cohesive and efficient enterprise-wide compliance risk management program.

The Compliance Monitoring Process

The compliance monitoring process is a critical element of an effective enterprise-wide compliance risk management program. “Compliance testing is necessary to validate that key assumptions, data sources, and procedures utilized in measuring and monitoring compliance risk can be relied upon on an ongoing basis and, in the case of transaction testing, that controls are working as intended. The testing of controls and remediation of deficiencies identified as a result of testing activities are essential to maintaining an effective control framework.”

A properly defined risk-based compliance monitoring process increases efficiency and effectiveness. A risk-based compliance monitoring process contemplates that the institution has
verified that all of the institution’s legal entities, lines of business, products, and services were considered and related compliance requirements were identified in the risk assessment process. And, when monitoring activities are completed, the results are then integrated into the risk assessment process to update the institution’s risk profile.

The scope and frequency of compliance monitoring activities is determined based on the results of the institution’s risk assessment. Utilizing risk-based scheduling deploys resources to those areas exhibiting the highest risk to the institution. Further, defining the scope of the testing based on your risk assessment provides a similar efficiency in resource deployment. Monitoring activities should be designed to identify deviation from prescribed regulatory practices and should include reviews of policies, procedures, forms, disclosures, and transactions. Lower risk areas are reviewed either with less frequency or in less detail or in some combination thereof.

The compliance monitoring process should establish documentation standards. Reviews conducted under the compliance monitoring process should be evidenced by detailed workpapers including documentation of the procedures performed, the sampling methods employed, and the universe tested. Deficiencies identified during the process should be clearly documented and retained with supporting documentation. Conclusions drawn should be fully supported by the documentation retained and plans for corrective action should be documented, implemented, and tracked to completion.

Regularly scheduled periodic reports relating to the compliance monitoring process should be provided to senior management and the board of directors. The reports should refer to the compliance risk assessment that has taken place during the reporting period, including any changes in the compliance risk profile based on relevant measurements such as performance indicators, summarize any identified breaches and/or deficiencies, the corrective measures recommended to address them, and report on corrective measures already taken.  

The Challenge

The separate development of a risk assessment program to identify, measure, and assess compliance risk and of a compliance monitoring process to monitor, test, and report the results of compliance testing is easily accomplished. Integration and management of the two processes, however, is much more difficult. While, as noted in the Deloitte Study, many institutions simply “throw personnel resources” at the process, the challenge we face is to implement a systematic approach that not only protects the institution, but also uses resources effectively.
The CompliancePro Enhanced Risk Management System

CompliancePro is a comprehensive browser-based compliance management system which integrates risk assessment and compliance monitoring procedures, designed to meet regulatory expectations that institutions identify, measure, and assess compliance risk; as well as monitor, test, and report the results of compliance testing. CompliancePro’s automated approach is a sophisticated and effective way of meeting regulatory expectations and mandates in this important managerial arena.

The following diagram outlines CompliancePro’s capabilities to provide “state-of-the-art” compliance risk management which is designed to achieve a “firmwide” compliance risk management system. CompliancePro’s database is the “heart” of the enterprise compliance risk management system. It contains approximately 14,000 procedures which mirror regulatory examination procedures for evaluating the organization’s compliance with federal consumer regulations and other key laws/regulations with which financial institutions must comply.

CompliancePro’s four libraries -- bank, thrift, trust and internal audit/internal controls -- are specifically designed to support each institution’s particular charter. The system’s risk assessment module leads the institution’s compliance or risk manager through, and documents, an analysis and assessment of the inherent risks and associated internal controls for each product/service type within each line of business. The resultant residual risk of the product or service type is mapped to the related monitoring activities via the procedures contained in the CompliancePro database.

While compliance risk assessment and monitoring activities are the two primary functions of the system designed to identify, measure, monitor and control the compliance risk of the enterprise, CompliancePro’s additional basic functional workflow capabilities displayed in the graphic are:
The *calendar and workbook* creation system used to prepare workbooks, make monitoring assignments, monitor the status of the workbooks assigned and document the monitoring activities.

The *compliance issue management* functionality used in documenting the compliance issues identified in each workbook monitoring activity, the corrective action planned, the responsibility assignment and the date due. Progress and completion can be tracked from this capability.

The *risk action plan management* capability (which functions like the compliance issue management capability) used to document risk issues and related risk action plans, along with responsibility for completion and the date due. Progress and completion can be tracked.

*Employee knowledge testing* which is designed to be used, not as a training device, but to identify risk with respect to training needs within the institution and/or department regarding specific knowledge requirements.

*The Policy module* used by clients as an on-line receptacle for the institution’s policies and procedures and other important information which may be related to compliance.

CompliancePro’s reporting system is an important functional capability for clients. The following highlights the system’s reporting capacities:

- Examiner/audit “*snapshots*” are used to generate on CD-ROM or other electronic media copies of CompliancePro workbooks, transactional reviews and related electronic attachments for use off-site by regulatory examiners and independent auditors. This function simplifies the client’s preparation time and effort for regulatory examinations.

- A comprehensive library of *board and management reports*, enabling client selection of breadth and depth of reporting, is available to support the Compliance Officer’s reporting to management and directors.

- *Risk Dashboard Reports* displays, in one screen, the important risk management factors for the institution, organized by both lines of business and/or organizational units.
The CompliancePro Risk Assessment Process

Risk assessment is an important part of the overall risk management process expected – and demanded – by regulators. The CompliancePro system is designed to lead a client through the maze of activities which are needed to assess risk in a comprehensive manner. The system takes the client through an analysis of the inherent risk factors by each product/service within a line of business. The individual assigned the task of preparing the inherent risk analysis responds to a series of pre-defined inherent risk factors (presented as questions) and may document the associated rationale for the level of risk relating to each of these factors. This analysis is then released to the designated supervisor for approval. Similarly, an associate (who may or may not be the same person who completed the inherent risk questionnaire) completes a series of pre-defined mitigating risk factors questions. The assessment of these factors reduces the level of inherent risk for the particular product being considered to produce the expected residual risk. The system’s pre-defined inherent and mitigating risk analysis factors may be customized with unique client based factors.

CompliancePro automatically maps the residual risk for each product or service within a line of business to the appropriate area and subarea within the system’s monitoring database and then continuously updates the risk level reflected in the monitoring activity procedures. To the extent that compliance issues are identified, the residual risk is elevated and corrective action is requested. The system’s risk management module tracks the identified risk, associated documented risk action plans, including responsibility for completion and due dates. The system’s compliance risk dashboard displays the results of the risk assessment by the client’s choice of specific product/service, line of business, or the whole institution.
The CompliancePro Monitoring Process

The foundation of the enterprise risk management system provided by CompliancePro lies in its monitoring process. CompliancePro’s extensive database of procedures – some 14,000 in all (counting all the separate procedures identified by each appropriate regulator) – are available to the compliance officer when creating workbooks to monitor the compliance of the organization with specific laws/regulations which are applicable to a specific area or subarea (for example, real estate lending or Bank Secrecy Act). The institution’s CompliancePro system administrator schedules monitoring activity in the calendar module and CompliancePro technology populates the workbook with the appropriate procedures to monitor compliance. The administrator assigns the workbook for completion by designating the due date and individual responsible for completion.

Workbooks include procedures, questionnaires, and file reviews (if transactional testing is needed) associated with the scheduled monitoring activity. When issues are identified, the system records those issues, supporting details and corrective action, including accountability and timeframe. The workbook user can attach workpapers electronically to the workbook to support the monitoring activity.

The calendar/workbook creation process is facilitated with a 12-month calendar – three months that have already elapsed, the current month in the fourth column and eight months into the future. Workbooks which have been assigned by area/subarea are displayed and their status is reflected as either (a) scheduled, (b) past due, (c) completed, or (d) virtually scheduled (that is, to be periodically repeated in the future at a user-defined frequency).

As the user completes the workbook, the system “alerts” the user to any previous issues which may have been identified for a particular procedure in the workbook so that the “corporate history” of the particular monitoring activity is always available to the compliance monitoring staff. Issues identified by regulatory examination or internal/external auditors may also be entered into CompliancePro’s database at the procedure level which corresponds to the regulatory citation where the compliance issue occurred. In this way, the client can monitor previous issues to avoid the potential of the dreaded “repeat violation.”

Compliance Issue Management

CompliancePro provides for compliance issue management – complete with corrective action assignments, due dates, progress reporting and documented action which is recorded and maintained in the historical database. The issue management tab contains summary information of issues in the system-defined areas/subareas within user-specified timeframes and entities and/or departments. The user can see “at-a-glance” where issues have been identified: issues
which have been identified by “internal” monitoring activities and those which have been identified by “external” audit activities, whether by regulatory examination and/or auditors.

The user can view issue details, including the organizational unit or “center”, the status, the creator, the occurrence date, the area and/or subarea, the type of issue (internally discovered or externally identified) and the risk rating related to the issue. The procedure text relating to the issue is also displayed. When a file review sample contains an issue, the system displays the subject of the file review, the client name on the file, the identification number and the date the review record was created. The issue details will display full detail of the documented cause of the issue. Prior corrective actions are also maintained by the system and reported on the issue management screen. This capability provides a complete history of current and prior corrective actions related to the issue.

The issue history screen displays the record of action, status, the history of revisions, and the date of entry. Finally, the issue attachments capability provides links to scanned documentation, if any, relating to the issue.

Documentation Integrity

Using spreadsheet or word processing programs to document risk assessments, compliance monitoring programs, and related action plans expose institutions to the risk that documented information may be corrupted, modified, or deleted. CompliancePro’s secure system minimizes this risk, providing high data integrity, data protection, and secure documentation retention. All user entries and attached documents are automatically protected and archived inside CompliancePro’s database.

The Policy Module

The CompliancePro system provides an on-line repository for a client’s policies and procedures if such capability is not otherwise available. Clients may place their policy information in CompliancePro for reference by users.

Conclusion

Regulatory burdens and regulator expectations continue to increase while the resources available to meet those expectations and requirements are constrained by market, industry, and institution forces. CompliancePro’s comprehensive system streamlines your compliance risk management and monitoring activities, providing an integrated end-to-end system for identifying, measuring, monitoring, and managing your institution’s compliance risk on a continual rather than annual basis. The system’s flexibility and scalability ensure a perfect fit for
any size institution. CompliancePro fulfills the *Compliance Paper’s* related principles, achieves the “firmwide” approach called for in the Federal Reserve Supervisory Letter SR 08-8, and implements a systemized program integrating compliance management and risk management.

CompliancePro automation eliminates time- and paper-intensive processes; provides high quality, standardized monitoring workpapers; allows at-a-glance status of monitoring activities, corrective action and risk action plans; reduces redundancies associated with maintaining separate monitoring and risk assessment systems; minimizes board and management report preparation time; protects against issues “falling through the cracks”; and, reduces time spent preparing for examinations and audits. The efficiencies you’ll gain by automating your compliance solutions will make it seem like you’ve increased staff but without hiring more people!

Notes:

3. Ibid, p. 16.
CompliancePro’s Cadre of Experts

CompliancePro is kept current with regulatory changes by a cadre of compliance experts who are also available for help with your compliance questions. Customer Care provides 24/7 high-touch technical and usage support.

James W. Bruce, Jr – Chairman of American Bank Systems, Inc. and its subsidiaries.

Mr. Bruce began his banking career with Liberty National Bank and Trust Company of Oklahoma City in 1965. During his 25 year tenure at Liberty, Mr. Bruce was responsible for launching the state’s first credit card program and developing the Bank’s planning and capital markets functions. In his capacity as Chief Financial Officer, he was responsible for raising approximately $175 million in new equity and debt capital. Mr. Bruce was the principal executive officer responsible for the development and execution of the comprehensive financial restructuring of the parent company in 1988 — the only major banking company in the Southwest to recapitalize privately without federal assistance during the region’s severe economic downturn in the late 1980’s.

In 1990, Mr. Bruce formed JW Bruce & Associates to provide consulting services to the financial industry and subsequently acquired controlling interest in American Bank Systems in 1993. Mr. Bruce is a graduate of the University of Oklahoma and the Harvard Graduate School of Business Administration. He is Director of American Bank & Trust Company of Tulsa Oklahoma and InvesTrust, NA of Oklahoma City. He is a member of the Executive Boards of Oklahoma City University’s Meinders School of Business and the Wanda L. Bass School of Music. Mr. Bruce is a former member of the Board of Trustees of Austin Presbyterian Theological Seminary and the Board of Trustees of the Texas Presbyterian Foundation. He co-authored a chapter in The Loan Officer’s Handbook concerning the relationship of asset-liability management to loan policy and also has served on the faculty of the American Bankers Association’s National Commercial Lending Graduate School and several other banking schools.

James W. (Jay) Bruce, III – Executive Vice President and General Counsel of American Bank Systems and its operating subsidiaries.

Mr. Bruce has been with the company since 1999. Prior to joining the company, Mr. Bruce was an associate with the law firm of Phillips, McFall, McCaffrey, McVey and Murrah and before that with the law firm of Kornfeld & Franklin, both of Oklahoma City. Mr. Bruce received his education at Oklahoma State University (B.S., Accounting, 1983) and the University of Oklahoma (J.D., 1989). He is a member of the Oklahoma Bar Association, is admitted to practice before all Oklahoma Courts, the United States Tax Court and the United States Court
of Appeals, Tenth Circuit, and served as a judicial clerk for Justice Marian Opala of the Oklahoma Supreme Court (1987). Mr. Bruce is also a Certified Public Accountant (licensed in 1985).

**Elva Coffey-Sears**, CRCM and CRP - Vice President and Compliance Consultant for ABS Proactive, LLC and ABS Consulting Services, LLC

Ms. Coffey-Sears joined the Company in March 2008. She began her banking career in 1978 on the operations-side of the bank, switching to a compliance focus in 1989. She has had responsibility for compliance for three Chicagoland banks, including chief compliance officer for a $75-billion, multi-state, multi-bank holding company. She has served as an examiner with the Office of the Comptroller of the Currency. In her tenure as a compliance consultant, she has assisted financial institutions with regulatory remediation involving BSA/AML, conducted diagnostic compliance and BSA/AML reviews, and provided regulatory compliance and compliance risk management training. She holds a bachelors degree in Economics from Loyola University of Chicago, and is a Certified Regulatory Compliance Manager and a Certified Risk Professional.

**Gina Ellis**, CRCM - Vice President and Managing Compliance Consultant for ABS Consulting Services, LLC

Ms. Ellis has been involved in banking and financial services since 1975, joining ABS in February 2003. She earned the Certified Regulatory Compliance Manager certification and her banking career includes significant experience in operations, accounting, planning/budgeting and internal audit. She has experience as the internal auditor for a multi-bank holding company. Prior to joining American Bank Systems, Ms. Ellis was associated with John M. Floyd and Associates where she was an Engagement Manager. During this time, she managed multiple consulting assignments and projects throughout the United States ranging from assisting financial institutions in the areas of profit improvement, product development and implementation of overdraft privilege programs, development of sales cultures and work simplification and process alternatives. Ms. Ellis attended Phillips University in Enid, Oklahoma and the University of Central Oklahoma in Edmond, Oklahoma where she focused on accounting and auditing.

**Mikel Dunnagan**, J. D. - Vice President and Compliance Consultant for ABS Consulting Services, LLC

Mr. Dunnagan has been involved in banking and financial services since 1985. He joined the Company in 2010 after spending 25 years with Colorado financial institutions during which time he served as a compliance consultant and taught regulatory compliance courses for several training organizations. His banking career includes significant experience in compliance, lending, and operations. Prior to joining American Bank Systems, Mr. Dunnagan was associated with a
Colorado bank holding company where he served as Compliance Officer for the bank and holding company and as Branch President. Mikel earned his Bachelor’s degree from the University of Central Oklahoma in Edmond, Oklahoma, and his Juris Doctorate from the Oklahoma City University School of Law.

**Ernest Springer** – Vice President and Compliance Consultant for ABS Proactive LLC and ABS Consulting Services, LLC

Mr. Springer’s business career has spanned 28 years of diversified financial, operations and management experience. For the past eleven years, he has been involved with the utilization of CompliancePro at Sovereign Bank, Inc. He developed and introduced regulatory compliance monitoring for all lines of business subject to consumer regulations. He was the CompliancePro System Administrator and Trainer for approximately 40 internal users of CompliancePro at Sovereign. During his tenure he managed a new risk assessment project using the Risk Module of CompliancePro. He coordinated the successful multi-year bank-wide implementation of the Fair and Accurate Credit Transactions Act requirement. Mr. Springer has a Bachelors of Science from Drexel University with a major in Accounting.

**Cody Roberts**, CRCM – Assistant Vice President and Compliance Consultant for ABS Proactive, LLC and ABS Consulting Services, LLC

Mr. Roberts is primarily responsible for the development and maintenance of CompliancePro’s extensive libraries of compliance monitoring procedures. Prior to joining ABS in May 2005, Mr. Roberts was in the compliance department of financial institutions for almost eight years including six years as a compliance officer for a chain of community banks. Mr. Roberts’ other duties have included compliance auditing, consulting, and training. His experience includes being a member of the board and officer for an economic development corporation that built low- and moderate-income housing. In addition, Mr. Roberts has been a corporate CRA, BSA, and security officer. Mr. Roberts is a graduate of Oklahoma State University where he earned his Bachelor’s degree in Marketing.

**David Walls** – Assistant Vice President and CompliancePro Product Specialist

Mr. Walls joined the ABS team in 2000 as a member of the Customer Care team and now leads ABS Proactive’s Customer Care related to CompliancePro and its various modules. His responsibilities include consulting with clients on the administrative capabilities and implementation issues related to CompliancePro, quality assurance and continuing customer care in the use of CompliancePro by clients as well as assisting sales staff in providing product demonstrations to potential clientele. He holds a Bachelors degree in Marketing and Advertising from the University of Central Oklahoma.
Kevin Turner, CISA – Information Manager for American Bank Systems and its operating subsidiaries and IT Compliance Consultant for ABS Consulting Services, LLC.

Mr. Turner joined the Company in early 2008 with responsibilities for the Company’s technology infrastructure. He provides IT auditing services to the Company’s client base. Mr. Turner has been an infrastructure technology architect for the last four years, with over ten years of industry experience. He also is involved with the CompliancePro team in the development and maintenance of the CompliancePro internal audit and internal control libraries, including IT monitoring procedures. His audit experience includes FFIEC IT Guidelines, SOX, and SAS70. His education background includes more than a dozen IT related certifications from Microsoft, Cisco, ISACA, (ISC)^2, EC-Council, and CompTIA. He is a member of the Information Systems Audit and Control Association and the Information Systems Security Association.