208 - Challenges Faced When Establishing an Enterprise-wide Compliance Risk Management Program

John Beccia III
Senior Vice President and Assistant General Counsel
Boston Private Financial Holdings, Inc.

Steven Lauer
Corporate Counsel
Global Compliance Services

Paul Matecki
Senior Vice President, General Counsel
Raymond James Financial, Inc.

Michele Nicholas
Corporate Counsel & Assistant Secretary
Armstrong World Industries, Inc.

Faculty Biographies

John Beccia III

John A. Beccia, III is senior vice president and assistant general counsel for Boston Private Financial Holdings, Inc. in Boston. He is responsible for enterprise-wide regulatory matters and ensuring affiliates' compliance with governing laws and regulations. Mr. Beccia is a Certified Anti-Money Laundering Specialist (CAMS) and serves as the anti- money laundering compliance officer and the privacy officer for the bank holding company.

Mr. Beccia was previously assistant general counsel for Investors Bank & Trust Company. He also served as chief regulatory counsel and research director for The Financial Services Roundtable in Washington, DC, where he coordinated regulatory affairs and assisted with the Roundtable's legislative efforts. While at the Roundtable, Mr. Beccia served on the financial crimes enforcement network's bank secrecy act advisory group. Mr. Beccia was also an attorney with the law firm of Perkins Smith & Cohen LLP and John Hancock Financial Services in Boston.

Mr. Beccia is currently co-chairperson of the ACC's Bank Secrecy Act/Anti-Money Laundering Subcommittee and co-chairperson of the Boston Bar Association's corporate counsel committee. He is also an active participant in the banking law committee of the ABA. He is vice chairperson for the compliance, examination, and audit subcommittee and served as a liaison to the ABA's presidential task force on the attorney-client privilege.

A graduate of Providence College, Mr. Beccia earned his J.D. from Roger Williams University School of Law and a LL.M. from Boston University School of Law's Morin Center.

Steven Lauer

Steven A. Lauer is corporate counsel for Global Compliance Services in Charlotte, North Carolina.

Previously, he served as director of integrity research for Integrity Interactive Corporation. He also consulted with corporate law departments and law firms on issues relative to how in-house and outside counsel work together. He worked as an in-house attorney in law departments as the sole in-house attorney for an organization. Mr. Lauer also has served as executive vice president, deputy editor, and deputy publisher of The Metropolitan Corporate Counsel, a monthly journal for in-house attorneys. Prior to becoming an in-house attorney, he was in private practice. Mr. Lauer was an assistant general counsel for The Prudential Insurance Company of America. He was project director for the Prudential law departmentï¿_s outside counsel utilization task force. Mr. Lauer was the in-house environmental attorney in the Prudential law departmentï¿_s real estate section. He was responsible for management of all litigation for those real estate units. Mr. Lauer represented Prudential in industry groups. In his consulting practice, Mr. Lauer conducted benchmarking research for clients, designed evaluation processes for counsel selection, researched and designed a case-evaluation methodology, and created a manual for outside counsel, among other projects. He has worked with law firms to better understand the changing expectations of corporate clients.

He has authored numerous articles on compliance, the relations between in-house and outside attorneys, the selection of counsel by corporate clients, the evaluation of legal service, litigation management, and other topics relevant to corporate compliance programs and corporate legal service.

He received a B.A. from the State University of New York at Buffalo and a J.D. from Georgetown University Law Center.

Paul Matecki
Senior Vice President, General Counsel
Raymond James Financial, Inc.

Michele Nicholas
Corporate Counsel & Assistant Secretary
Armstrong World Industries, Inc.

Agenda

- Enterprise Risk Management
- Creating an Ethics and Compliance Program to Address Risks
- Case Studies and Challenges in Implementation

Enterprise Risk Management

Michele Monaghan Nicholas
Prepared by M. M. Nicholas and Walter T. Gangl

ACC's 2007 Annual Meeting:
Enjoying the Ride on the Track to Success
October 29-31, Hyatt Regency Chicago

What is ERM?

***Enterprise Risk Management*: a "systematic and disciplined" set of policies, processes and practices, as well as a structure, that enables ongoing:**

- Identification, assessment, and prioritization of the major risks associated with the Company's key business objectives;
- Development, implementation, and monitoring of risk mitigation strategies; and
- Independent and objective evaluations *(by management, board and external audiences)* of risk mitigation strategies.

A working definition per COSO (Commission on Sponsoring Organizations of the Treadway Commission). COSO issued an ERM framework in 2004. It has been endorsed by the Securities Exchange Commission and professional auditing and management bodies and has become a standard for risk management methodologies.

Risk Assessment

Why?

- For securities reporting purposes.
- For Board reporting purposes.
- To identify and mitigate risks that could significantly affect the Company's ability to achieve its strategic and financial objectives or that could harm employees, customers, stakeholders or communities.

Risk Management Objectives

- Actively monitor, assess and prioritize.
- Mitigate risks that can significantly affect the Company's ability to achieve its strategic and financial objectives or that can harm employees, customers, stakeholders or communities.
- Communicate about risks in a systematic process that includes management and board oversight.
- Use foresight to better plan forward strategy, operations, capital plans and investment.

Key Definitions

Risk

- Any event or circumstance which could impact the achievement of business objectives.

Inherent Risk

- Exposure to a risk that is intrinsic to the business in the current environment before the consideration of risk mitigation and control activities that have been designed and implemented to address a given risk.

Residual Risk

- Exposure to a risk remaining after considering the effect of mitigation through risk management and control activities.

Key Definitions

Contributing Factors

- Causal drivers of risk that affect either the probability of occurrence or the severity of impact of the event or circumstance.

Risk Management and Control Activities

- The means to mitigate the harm and/or the likelihood of a risk; such as policies, procedures and guidelines, designed to control process or reduce the likelihood and/or impact of a risk.

Types of Risk

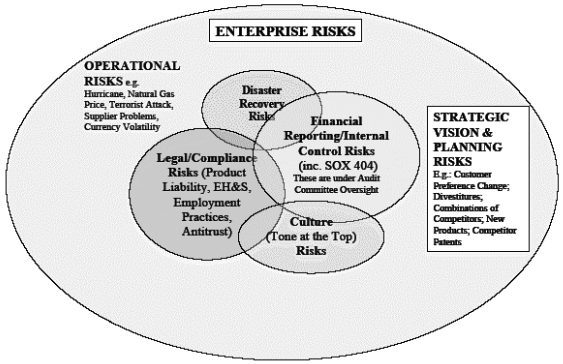
ERM says we should identify and evaluate all types of risks:

- Operational
- Strategic
- Execution
- Controls
- Compliance
- Corporate culture

ACC's 2007 Annual Meeting:
Enjoying the Ride on the Track to Success
October 29-31, Hyatt Regency Chicago

Our Universe of Risks

All types of risks are to be included in the Risk Assessment. This diagram illustrates different categories of risks, and the fact that there are many overlaps. For our Risk Assessment, take as broad a perspective as possible to capture all significant risks to your business operation.



Risk Assessment

An intuitively important business management skill. Companies practice elements of risk management all of the time (hurricane response preparation, business downturn, IT protocols). Risk assessment should be thoughtful and strategic plan-based and should:

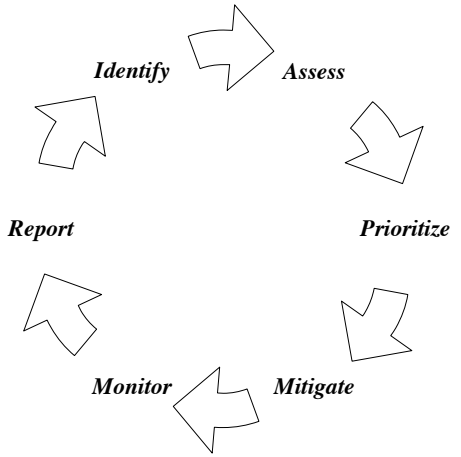
- Identify
- Assess probability and impact
- Prioritize and define major risks

ACC's 2007 Annual Meeting:
Enjoying the Ride on the Track to Success
October 29-31, Hyatt Regency Chicago

Risk Assessment Process

- **Identify** matters that create risk to achieving our business plans.
- **Assess** the risks by considering the likelihood and impact.
- **Prioritize** risks, start with major risks.
- **Mitigate** risks through improved processes or procedures or other action.
- **Monitor** risks to address whether mitigation is effective.
- **Report** risks to management and board.

Risk Assessment Process



ACC's 2007 Annual Meeting:
Enjoying the Ride on the Track to Success
October 29-31, Hyatt Regency Chicago

Risk Matrix and Risk List

Promotes the use of common nomenclature and common "scales" and allows us:

- To assess the likelihood and impact of risks.
- To compare and generate a composite enterprise-wide risk matrix.
- To compare notes and discuss how different business units and corporate departments look at risks.

Risk Prioritization Using a Risk Matrix

Severity of Impact	Rare (Less than 2%)	Unlikely (Less than 15%)	Possible (15-50%)	Probable (>50%)	Almost Certain (>90%)
Massive over $20 M					
Major ($2 to $20 Million)					
Moderate ($250,000 to $2 million)					
Minor (Up to $250,000)					

Impact/ Probability of occurrence

Probability of Occurrence

ACC's 2007 Annual Meeting:
Enjoying the Ride on the Track to Success
October 29-31, Hyatt Regency Chicago

Risk List

POLITICAL & SOCIAL ENVIRONMENT
1= Unstable government or legal system
2=Terrorism or war
3= Regulatory/ environment issues hamper business
MARKET CONDITIONS
4 = Consumer Confidence
5 = Government budgets
6 = Construction activity
7 = Changes in consumer preference
8 = Lower cost imports/competitors with lower cost
9 = Developing market low end products/margins
COMPETITIVE ENVIRONMENT
10 = Price pressure/inability to cover inflation
11= Patents: protection, loss, or competitor blocks
12 = New competitor products
13 = Combination of competitors
PRODUCTION ISSUES
14 = Production quality and efficiency/scrap
15 = Plant capacity/consolidations/closing/divestiture
16 = Productivity and automation
SUPPLY CHAIN/DISTRIBUTION/MKTG
17 = Dependence on supplier/supplier consolidation
18 = Raw material/energy cost and availability
19 = Dependence on distributors
20 = Transportation costs/issues
PRODUCT ISSUES
21 = Product line gaps or development failure
22 = Failure in new product introduction or marketing
23 = Warranty claims/recalls/product safety issues
CUSTOMER ISSUES
24 = Dependence on or loss of key customers
25 = Alliances among customers
26 = Retailer consolidation or changes in policies
27 = Collection issues in declining economy

INFORMATION TECHNOLOGY
28 = IT systems interruptions/data loss
29 = Loss of Data Center function
30 = Loss of IT Connectivity >24 hours
31 = Security weakness/data theft
TREASURERS
32 = Natural disasters
33 = Ability to comply with credit covenants
34 = Credit covenants limit operating/financial flexibility
35 =Availability of financing
36 = Changes in exchange rates
37 = Changes in interest rates
38 = Repatriation hard due to tax laws/exchange controls
TAX
39 = Adverse tax adjustment imposed
40 = Tax rates increase
41 = Double taxation from transfer pricing adjustments
42 = Antiboycott violations – tax penalty
CONTROLLERS/CORPORATE FINANCE
43 = Changes in accounting standards
44 = Changes in value of balance sheet assets
HUMAN RESOURCES
45 = Wages and compensation cost
46 = Employee/retiree benefits
47 = Recruitment and retention/loss of key personnel
48 = Possible work stoppages
49 = Employment practices compliance
ENV HEALTH AND SAFETY
50 = Plant compliance with environmental regulations
51 = Fire and safety compliance
52 =Product safety liability claims (w/legal)
53 = Product labeling regulations compliance
LEGAL
54 = Antitrust practices compliance
55 = Size of liabilities

Art vs. Science

Subjective bias and true differences of opinion exist, but you can minimize their effect by:

- Getting good data/information for risks where it is reasonably available and
- Encouraging discussion:
  - among your team,
  - with colleagues in other businesses and
  - with management

Risk Assessment

Establish "Ownership"

- Assign ownership of significant risks to people qualified to monitor them.
- Owners are responsible for proposing assessment updates and effective mitigation measures.
- Risks owned by a business unit should be discussed internally, with management and with other business units when it adds value.
- Co-owned risks (business units and/or corporate departments) still need a designated owner.

Reporting

Management's Role

- Explain the processes used to identify events or matters that create risk to achieving company objectives.
- Explain the processes used to assess likelihood and impact of the risks and prioritize them.
- Identify major inherent risks, including definition of major.
- Identify owner – who is responsible for mitigation and monitoring major risks?

Oversight

Board's Role

- Advise whether they are comfortable with Company's processes to identify and assess risks.
- Advise whether they agree with our identification, assessment and mitigation measures.
- Advise whether they view the ERM processes as effective.
- Advise whether they confer with the level of residual risk accepted by management.
- Make any suggestions or recommendations they have relative to the ERM processes, including identification, assessment and mitigation plans.

Challenges

- Making risk management a standard part of strategic planning and business activities.
- Ensuring the proper level of resources and attention to the process.
- Qualitative rating of some risks is unavoidable. There may be little or no data to support qualitative or quantitative measures.
- The cost-benefit equation of further investment of time and money needs to be balanced.
- Is it worth the trouble? Work to minimize the burden and maximize the value. We can capture value if we improve the way we detect, understand, prepare for and deal with risks.

Risk Management – Take Aways:

Identify, assess, prioritize and mitigate all types of risks.

- Start analyses by rating inherent risk, evaluate the effect of your mitigation measures, and compute the residual risk remaining.
- Integrate risk assessment with strategic planning.
- Designate risk "owners."
- Get good data to support analysis of quantitative risks.

Risk Management – Take Aways:

- Get good experience and judgment to assess qualitative risks.
- Make risk management discussions a regular part of business discussions and processes.
- Integrate quarterly reporting with those discussions.
- Test conclusions in discussions with in-house and outside sources, such as industry peers.
- Share learning and benefits with other corporate departments and business units.

ACC's 2007 Annual Meeting:
Enjoying the Ride on the Track to Success
October 29-31, Hyatt Regency Chicago

Creating an Ethics and Compliance Program to Address Risks

John A. Beccia, III

Why Focus on Compliance?

- Companies face additional regulatory scrutiny, consumer skepticism and litigation
- Compliance breakdowns can be costly and damage a company's reputation and brand
- Recent sanctions against corporations are the result of governance and testing failures
- Compliance is no longer a cost center - investing in compliance can reduce risks and add value

Guidance on Compliance Function

- Federal Sentencing Guidelines (2004) – Chapter 8 – Part B
  - Corporations should exercise due diligence to prevent and detect criminal conduct
  - Corporations should promote a culture that encourages ethical conduct and a commitment to compliance with the law
- Dept. of Justice - McNulty Memorandum (December 2006)
  - Compliance programs should be sufficiently implemented
  - Prosecutorial decisions are based on the effectiveness of the program, not just single instances or violations of the law

Guidance on Compliance Function

- Enterprise Risk Management – compliance as a risk management function
  - Committee of Sponsoring Organizations of the Treadway Commission (COSO)
- Other Areas of Guidance
  - Regulations and interpretive guidance
  - Litigation and enforcement actions
  - Speeches

ACC's 2007 Annual Meeting:
Enjoying the Ride on the Track to Success
October 29-31, Hyatt Regency Chicago

Elements of an Effective Compliance Program

1. Culture of compliance: Tone at the top
2. Structure: Proper authority, reporting lines, and independence
3. Clearly defined objectives, policies and procedures
4. Comprehensive risk assessment processes
5. Strong validation and independent testing
6. Monitoring and reporting process with performance indicators
7. Adequate compliance training programs
8. Well defined escalation procedures
9. Ongoing communication with regulatory agencies
10. Adequate resources to implement program

Creating a Compliance Culture

- Integrity and ethical values
- Commitment to compliance - board of directors and senior management set the tone at the top
- Compliance woven into business areas
- Assignment of authority and responsibility for oversight
- Accountability within the organization
- Hire the right people

Organizational Structure

- Reporting lines - no one size fits all approach
  - Compliance must be independent from the business units
  - Reporting high in the organization
- Business lines are responsible for compliance
- Appropriate level and amount of resources are needed

Developing Policies and Procedures

- Set the tone – code of conduct policies
- Roadmap for policies – business unit and regulatory compliance matrices of laws and regulations
- Establish enterprise-wide policies
- Board review and approval of policies
- Supporting business unit procedures
- Annual review and update of compliance policies and procedures
- Ongoing tracking of laws and regulations
- Communication of policies through training, committees, etc.

Risk Assessment Process

- Compliance matrices (business unit, overall regulatory risk, and vendor risk)
- Review risks associated with all new customers & products:
  - Customer and product profiles
  - Transaction volume and trends
  - Define "high risk" customers and transactions
- Evaluation of internal controls based on risk ratings:
  - Adequacy of policies and procedures, and current controls
  - Internal and external testing results
  - Ongoing training of staff

Testing Program

- "Three-pronged" testing program
  - Business unit self-assessments
  - Compliance monitoring and testing
  - Internal and external audit testing
- Annual compliance testing plan and programs
- Continuous Monitoring
  - Identification and escalation of key risk indicators
- Validation of corrective actions
- Board and senior management reporting

ACC's 2007 Annual Meeting:
Enjoying the Ride on the Track to Success
October 29-31, Hyatt Regency Chicago

Independent Testing

- Testing should be independent of business lines and compliance
- Scope of testing
  - Evaluate compliance with laws, industry best practices, ongoing compliance monitoring, and adequacy of training
  - Scope must be appropriate to company's size and risk profile
- Testing Results
  - Review of testing results by senior management
  - Escalation to the board of directors when appropriate
  - Prompt corrective action by senior management
  - The testing must be adequately documented (*i.e.* work papers)

Monitoring and Reporting

- Develop metrics of what is a successful compliance program
- Conduct periodic reviews
- Prepare scorecards or heatmaps outlining performance and areas of concern
- Report results to management and the board on an ongoing basis
- Compliance as part of performance reviews

ACC's 2007 Annual Meeting:
Enjoying the Ride on the Track to Success
October 29-31, Hyatt Regency Chicago

Training Programs

- Policies are not effective if not communicated
- Identify specific topics to be covered based on risk assessments
- Annual training for key compliance areas
- Update programs based on regulatory and business changes
- Include in corporate orientation
- Online and web-based training
- Tailored training at business unit level
- Intranet communications, newsletters
- Ongoing communications (committee meetings, etc.)
- Record and track training

Risk Escalation Procedures

- Institute formal procedures for internal issues and customer complaints
- Utilize an ethics hotline with anonymous reporting
- Escalate issues as soon as possible
- Conduct a detailed investigation
- Develop and document prompt corrective actions
- Communicate with regulators when necessary

ACC's 2007 Annual Meeting:
Enjoying the Ride on the Track to Success
October 29-31, Hyatt Regency Chicago

Communications with Regulators

- Maintain ongoing communication with regulators and other government agencies with supervisory authority
- Be proactive in reporting issues
- Demonstrate commitment to compliance
- Don't wait for examinations to review program and business unit areas – create "regulatory goodwill"
- Manage the regulatory examination process

Staffing and Use of Technology

- Management must be committed to assigning the resources needed to implement the compliance program
- Staffing
  - Hire the right people
  - Background checks and other due diligence
  - Training
- Use of technology
  - Can be used to track trends or create databases
  - Requires expertise and IT support

ACC's 2007 Annual Meeting:
Enjoying the Ride on the Track to Success
October 29-31, Hyatt Regency Chicago

Key Challenges

- Creating the culture of compliance
- Acquiring adequate resources (personnel, technology, etc.)
- Managing compliance costs
- Being proactive and anticipating regulatory expectations and next "hot topics"
- Continually updating and enhancing compliance program
  - Incorporate lessons learned
  - Get feedback from business units, audit, human resources, finance, etc.

Case Study #1
Hotlines in Europe:
Varying standards, varying challenges

Steven A. Lauer

ACC's 2007 Annual Meeting:
Enjoying the Ride on the Track to Success
October 29-31, Hyatt Regency Chicago

EU data privacy directive

- Directive 95/46/EC
  - Provides for countries in the European Union to enact statutes that implement "fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, and in the general principles of Community law"

Data privacy directive - principles

- Legitimacy
- Data quality
- Proportionality
- Rights of the "incriminated person"
- Security of operations

ACC's 2007 Annual Meeting:
Enjoying the Ride on the Track to Success
October 29-31, Hyatt Regency Chicago

First Principle - Legitimacy

- Compliance with a legal obligation
- A legal obligation imposed by an EU member (Sarbanes-Oxley not legitimate)
- Accounting, internal accounting controls, auditing matters and combating bribery, banking and financial crime are legitimate concerns
- Necessary for purposes of a legitimate interest of the "data controller"

Second principle – data quality

- Objective data rather than subjective judgments
- Data must be kept only so long as needed for the purpose(s) for which collected

Third principle - proportionality

- How many individuals might be subject to having their personal data collected?
- How many individuals might have access to the personal data?

Fourth principle – rights of incriminated individuals

- Right to be notified that his/her personal data have been collected
- Right of access to his/her personal data collected and processed in a system
- Right of rectification of inaccurate data
- Right to erasure of inaccurate or dated data
- Right of opposition

Fifth principle - security

- "The company or organisation responsible for a whistleblowing scheme shall take all reasonable technical and organisational precautions to preserve the security of the data when it is gathered"
- "Confidentiality of reports is an essential requirement"
- "A specific organisation must be set up within the company"
- "Specially trained and dedicated people, limited in number and contractually bound by specific confidentiality obligations"
- "Strictly separated from other departments"
- "The information collected and processed shall be exclusively transmitted to those persons who are specifically responsible … for the investigation or for taking the required measures to follow up the facts reported"

EU member states and hotlines

- Here are a few examples of the variation among the laws and guidelines pertinent to corporate hotlines that have emerged from EU member states' data protection authorities recently

EU member state - France

- "a whistleblowing system may only be considered as legitimate if it is necessary to comply with a legal obligation … or if it is necessary for the purposes of realizing the legitimate interest [of] the date controller … and its realization does not imply to 'override the interests or the fundamental rights and freedoms of the data subjects"
- "data controllers must clearly indicate that these systems are strictly reserved for such areas, and must refrain from investigating reports related to other areas."
- Registration required

EU member state - Germany

- "The goal of ensuring financial security in international financial markets and in particular the prevention of fraud and misconduct with respect to accounting, internal accounting controls, auditing matters, as well as the fight against bribery, banking and financial crime or insider trading, appears to be a legitimate interest of the employer"
- "conduct which adversely affects company ethics" does not outweigh "the legitimate interests of the data subjects" which "are compelling"
- Registration not required "if the controller has appointed a data protection official"

EU member state - Spain

- Allegations submitted to hotline must be "limited to reports involving internal or external topics or rules, the violation of which could have an actual impact on the maintenance of the contractual relationship between the company and the person incriminated"
- "it must be required that the system accepts the filing of whistleblower complaints in which the whistleblower is identified"

Some suggestions

- Treat operations in any EU member country distinctly from those in other countries
- Adapt the operation of the hotline in each country to the requirements of that country (separate phone line, awareness campaign, phone or online greeting, permissible allegations, security of data, routing of reports, etc.)
- Observe requirements vis-à-vis transfers to the US or other non-EU countries (use EU-approved contract clauses, US Safe Harbour firms, etc.)

Case Study #2
Cross Border Transfer of Personal Data

Paul Matecki

U.S. vs. European Approach

- U.S.- Privacy of personal information is a priority of federal and state government as well as consumers.
  - Sectoral approach
    - Legislation, regulation and self-regulation
- EU- Protection of information privacy is a fundamental, human right.
  - Comprehensive approach
    - EU Directive on Data Privacy

ACC's 2007 Annual Meeting:
Enjoying the Ride on the Track to Success
October 29-31, Hyatt Regency Chicago

EU Directive Overview

- No personal data can, subject to limited exception, be transferred to a country outside the EU unless that country ensures an adequate level of protection of the data.
- The U.S. is deemed not to offer an adequate level of protection unless the recipient company is a participant in the Safe Harbour Principles.

EU Directive Overview

- Other methods to achieve adequate protection
  - Model Contractual Clauses
  - Binding Corporate Rules

ACC's 2007 Annual Meeting:
Enjoying the Ride on the Track to Success
October 29-31, Hyatt Regency Chicago

Risk Analysis

- Risks are serious
- Data transfers are lifeblood of many organizations and the underpinning of all electronic commerce
- The information can be simple (personal telephone directories) to highly sensitive (credit card information)

Enterprise Policy

- Principles-Based Approach
  - Essential to achieve enterprise-wide coverage
- Additional Guidance
  - Essential to ensure compliance with multitude of regulations and data types
- Basic Tenets to Any Policy
  - "Know What you Do"
  - "Say What You Do"
  - "Do What You Say"

ACC's 2007 Annual Meeting:
Enjoying the Ride on the Track to Success
October 29-31, Hyatt Regency Chicago

SWIFT Decision

- First decision which examines in detail the issue of cross-border data flows.
- SWIFT attempted to rely on exemptions which were rejected.
- SWIFT and all of the financial institutions which utilized it were found to have "failed to respect the provisions of the directive.

Useful Links

- www.export.gov/safeharbor/
- www.eur-lex.europa.eu/en/index_cnt.html
- SWIFT decision:
  - www.ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_en.pdf
- Example Policies:
  - www.telekom.com/dtag/cms/contentblob/dt/en/51858/blobBinary/privacy-code-of- conduct.pdf
  - www.unisys.com/about__unisys/copyright/privacy__policy.htm
  - www.jnj.com/privacy_safeharbor/

ACC's 2007 Annual Meeting:
Enjoying the Ride on the Track to Success
October 29-31, Hyatt Regency Chicago

2. EFFECTIVE COMPLIANCE AND ETHICS PROGRAM

Historical Note: Effective November 1, 2004 (see Appendix C, amendment 673).

§8B2.1. Effective Compliance and Ethics Program

(a) To have an effective compliance and ethics program, for purposes of subsection (f) of §8C2.5 (Culpability Score) and subsection (c)(1) of §8D1.4 (Recommended Conditions of Probation - Organizations), an organization shall—

(1) exercise due diligence to prevent and detect criminal conduct; and

(2) otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

Such compliance and ethics program shall be reasonably designed, implemented, and enforced so that the program is generally effective in preventing and detecting criminal conduct. The failure to prevent or detect the instant offense does not necessarily mean that the program is not generally effective in preventing and detecting criminal conduct.

(b) Due diligence and the promotion of an organizational culture that encourages ethical conduct and a commitment to compliance with the law within the meaning of subsection (a) minimally require the following:

(1) The organization shall establish standards and procedures to prevent and detect criminal conduct.

(2) (A) The organization's governing authority shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight with respect to the implementation and effectiveness of the compliance and ethics program.

(B) High-level personnel of the organization shall ensure that the organization has an effective compliance and ethics program, as described in this guideline. Specific individual(s) within high-level personnel shall be assigned overall responsibility for the compliance and ethics program.

(C) Specific individual(s) within the organization shall be delegated day-to-day operational responsibility for the compliance and ethics program. Individual(s) with operational responsibility shall report periodically to high-level personnel and, as appropriate, to the governing authority, or an appropriate subgroup of the governing authority, on the effectiveness of the compliance and ethics program. To carry out such operational responsibility, such individual(s) shall be given adequate resources, appropriate authority, and direct access to the governing authority or an appropriate subgroup of the governing authority.

(3) The organization shall use reasonable efforts not to include within the substantial authority personnel of the organization any individual whom the organization knew, or should have known through the exercise of due diligence, has engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program.

(4) (A) The organization shall take reasonable steps to communicate periodically and in a practical manner its standards and procedures, and other aspects of the compliance and ethics program, to the individuals referred to in subdivision (B) by conducting effective training programs and otherwise disseminating information appropriate to such individuals' respective roles and responsibilities.

(B) The individuals referred to in subdivision (A) are the members of the governing authority, high-level personnel, substantial authority personnel, the organization's employees, and, as appropriate, the organization's agents.

(5) The organization shall take reasonable steps—

(A) to ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct;

(B) to evaluate periodically the effectiveness of the organization's compliance and ethics program; and

(C) to have and publicize a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization's employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation.

(6) The organization's compliance and ethics program shall be promoted and enforced consistently throughout the organization through (A) appropriate incentives to perform in accordance with the compliance and ethics program; and (B) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct.

(7) After criminal conduct has been detected, the organization shall take reasonable steps to respond appropriately to the criminal conduct and to prevent further similar criminal conduct, including making any necessary modifications to the organization's compliance and ethics program.

(c) In implementing subsection (b), the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement set forth in subsection (b) to reduce the risk of criminal conduct identified through this process.

Commentary

Application Notes:

1. Definitions.—For purposes of this guideline:

"Compliance and ethics program" means a program designed to prevent and detect criminal conduct.

"Governing authority" means the (A) the Board of Directors; or (B) if the organization does not have a Board of Directors, the highest-level governing body of the organization.

"High-level personnel of the organization" and "substantial authority personnel" have the meaning given those terms in the Commentary to §8A1.2 (Application Instructions - Organizations).

"Standards and procedures" means standards of conduct and internal controls that are reasonably capable of reducing the likelihood of criminal conduct.

2. Factors to Consider in Meeting Requirements of this Guideline.—

(A) In General.—Each of the requirements set forth in this guideline shall be met by an organization; however, in determining what specific actions are necessary to meet those requirements, factors that shall be considered include: (i) applicable industry practice or the standards called for by any applicable governmental regulation; (ii) the size of the organization; and (iii) similar misconduct.

(B) Applicable Governmental Regulation and Industry Practice.—An organization's failure to incorporate and follow applicable industry practice or the standards called for by any applicable governmental regulation weighs against a finding of an effective compliance and ethics program.

(C) The Size of the Organization.—

(i) In General.—The formality and scope of actions that an organization shall take to meet the requirements of this guideline, including the necessary features of the organization's standards and procedures, depend on the size of the organization.

(ii) Large Organizations.—A large organization generally shall devote more formal operations and greater resources in meeting the requirements of this guideline than shall a small organization. As appropriate, a large organization should encourage small organizations (especially those that have, or seek to have, a business relationship with the large organization) to implement effective compliance and ethics programs.

(iii) Small Organizations.—In meeting the requirements of this guideline, small organizations shall demonstrate the same degree of commitment to ethical conduct and compliance with the law as large organizations. However, a small organization may meet the requirements of this guideline with less formality and fewer resources than would be expected of large organizations. In appropriate circumstances, reliance on existing resources and simple systems can demonstrate a degree of commitment that, for a large organization, would only be demonstrated through more formally planned and implemented systems.

Examples of the informality and use of fewer resources with which a small organization may meet the requirements of this guideline include the following: (I) the governing authority's discharge of its responsibility for oversight of the compliance and ethics program by directly managing the organization's compliance and ethics efforts; (II) training employees through informal staff meetings, and monitoring through regular "walk-arounds" or continuous observation while managing the organization; (III) using available personnel, rather than employing separate staff, to carry out the compliance and ethics program; and (IV) modeling its own compliance and ethics program on existing, well-regarded compliance and ethics programs and best practices of other similar organizations.

(D) Recurrence of Similar Misconduct.—Recurrence of similar misconduct creates doubt regarding whether the organization took reasonable steps to meet the requirements of this guideline. For purposes of this subdivision, "similar misconduct" has the meaning given that term in the Commentary to §8A1.2 (Application Instructions - Organizations).

3. Application of Subsection (b)(2).—High-level personnel and substantial authority personnel of the organization shall be knowledgeable about the content and operation of the compliance and ethics program, shall perform their assigned duties consistent with the exercise of due diligence, and shall promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

If the specific individual(s) assigned overall responsibility for the compliance and ethics program does not have day-to-day operational responsibility for the program, then the individual(s) with day-to-day operational responsibility for the program typically should, no less than annually, give the governing authority or an appropriate subgroup thereof information on the implementation and effectiveness of the compliance and ethics program.

4. Application of Subsection (b)(3).—

(A) Consistency with Other Law.—Nothing in subsection (b)(3) is intended to require conduct inconsistent with any Federal, State, or local law, including any law governing employment or hiring practices.

(B) Implementation.—In implementing subsection (b)(3), the organization shall hire and promote individuals so as to ensure that all individuals within the high-level personnel and substantial authority personnel of the organization will perform their assigned duties in a manner consistent with the exercise of due diligence and the promotion of an organizational culture that encourages ethical conduct and a commitment to compliance with the law under subsection (a). With respect to the hiring or promotion of such individuals, an organization shall consider the relatedness of the individual's illegal activities and other misconduct (i.e., other conduct inconsistent with an effective compliance and ethics program) to the specific responsibilities the individual is anticipated to be assigned and other factors such as: (i) the recency of the individual's illegal activities and other misconduct; and (ii) whether the individual has engaged in other such illegal activities and other such misconduct.

5. Application of Subsection (b)(6).—Adequate discipline of individuals responsible for an offense is a necessary component of enforcement; however, the form of discipline that will be appropriate will be case specific.

6. Application of Subsection (c).—To meet the requirements of subsection (c), an organization shall:

(A) Assess periodically the risk that criminal conduct will occur, including assessing the following:

(i) The nature and seriousness of such criminal conduct.

(ii) The likelihood that certain criminal conduct may occur because of the nature of the organization's business. If, because of the nature of an organization's business, there is a substantial risk that certain types of criminal conduct may occur, the organization shall take reasonable steps to prevent and detect that type of criminal conduct. For example, an organization that, due to the nature of its business, employs sales personnel who have flexibility to set prices shall establish standards and procedures designed to prevent and detect price-fixing. An organization that, due to the nature of its business, employs sales personnel who have flexibility to represent the material characteristics of a product shall establish standards and procedures designed to prevent and detect fraud.

(iii) The prior history of the organization. The prior history of an organization may indicate types of criminal conduct that it shall take actions to prevent and detect.

(B) Prioritize periodically, as appropriate, the actions taken pursuant to any requirement set forth in subsection (b), in order to focus on preventing and detecting the criminal conduct identified under subdivision (A) of this note as most serious, and most likely, to occur.

(C) Modify, as appropriate, the actions taken pursuant to any requirement set forth in subsection (b) to reduce the risk of criminal conduct identified under subdivision (A) of this note as most serious, and most likely, to occur.

Background: This section sets forth the requirements for an effective compliance and ethics program. This section responds to section 805(a)(2)(5) of the Sarbanes-Oxley Act of 2002, Public Law 107–204, which directed the Commission to review and amend, as appropriate, the guidelines and related policy statements to ensure that the guidelines that apply to organizations in this chapter "are sufficient to deter and punish organizational criminal misconduct."

The requirements set forth in this guideline are intended to achieve reasonable prevention and detection of criminal conduct for which the organization would be vicariously liable. The prior diligence of an organization in seeking to prevent and detect criminal conduct has a direct bearing on the appropriate penalties and probation terms for the organization if it is convicted and sentenced for a criminal offense.

Historical Note: Effective November 1, 2004 (see Appendix C, amendment 673).

The Metropolitan Corporate Counsel®

www.metrocorpcounsel.com

Volume 14, No. 10 © 2006 The Metropolitan Corporate Counsel, Inc. October 2006

Compliance Readiness – Legal Service Providers

A General Counsel And His Experts Tackle Risk Assessments

By John M. Spinnato, Debra Sabatini Hennelly and Steven A. Lauer

The corporate ethics and compliance practice and the compliance profession arose after two noteworty events. First, scandals involving activity in the electrical industry in the 1950s and '60s that violated the antitrust laws led to prison terms for some corporate executives. Later, the scandals that centered on the bribery of foreign government officials in the 1970s led to the enactment of the Foreign Corrupt Practices Act. The United States Sentencing Commission ("Commission") issued Sentencing Guidelines for Organizational Defendants (the "Guidelines") in 1991, which articulated the concept of a corporate compliance program as a means of qualifying for a reduced sentence in the (unlikely) event that a business suffers conviction for a federal crime. The following year, twelve corporate ethics officers formed the Ethics Officer Association (now called the Ethics & Compliance Officer Association) to "[b]e … the leading provider of ethics, compliance, and corporate governance resources to ethics and compliance professionals worldwide." (See www.theecoa.org/AboutECOA.asp#mv v.) ECOA's membership now numbers over 1,000 and other associations have grown up over the last few years, all evidence of the growing acceptance and maturation of the ethics and compliance practice.

The profession has matured to a greater degree than has the practice itself. To some extent, there is less consensus on what constitutes "best," "leading edge" or "best existing" practices in corporate compliance than on the attributes of a chief compliance officer position or that of an ethics officer. ECOA has published a list of those attributes that reflects recent changes to the Guidelines. See www.theecoa.org/ Whatis.asp. (Whether those two roles – ethics officer and compliance officer – ought to constitute distinct positions or represent simultaneous roles of one corporate officer constitutes an issue beyond the scope of this article.) We have achieved, however, broad agreement that an effective compliance program is a comprehensive system of policies and procedures designed to prevent – or, if they occur, to detect and correct – violations of law or company policy.

The changes to the Guidelines adopted by the Commission that became effective as of November 1, 2004, introduced a new element to the constellation of compliance practices. Among other things, the Commission enunciated a requirement that companies develop their compliance and ethics programs after conducting risk assessments and that they use such tools periodically to assess the effectiveness of those programs. A risk assessment thus now occupies a central and strategic position in the compliance universe.

Despite introducing the risk assessment into the calculus of compliance program design and the management of such a program, the Commission offered little guidance as to how an organization might conduct one. It listed in its commentary to the Guidelines the following criteria that such assessments should take into account, but it did not advise companies how to do so:

1. The nature and seriousness of possible criminal conduct that might occur in the business;
2. The likelihood that criminal conduct might occur in the course of the business operation, and
3. The prior history of the organization in respect of past criminal conduct.

How might or should a company conduct a risk assessment as described by the Commission? Would a risk assessment for purposes of designing a compliance program differ from a risk assessment conducted to evaluate a program's ongoing effectiveness? If so, how would they differ? These issues are the focus of ongoing discussion in the profession.

An assessment, whether conducted prior to organizing a compliance regimen or as part of the periodic evaluation and improvement of an existing one, should serve the same ultimate purpose: determining whether the business operations violate, or present a substantial risk of violating, external or internal requirements or standards. (Though an organization needs to worry only about external standards that define criminality for purposes of the Guidelines, an understanding of other behavioral expectations, such as civil statutes and other standards, may be important enough to qualify for consideration in this regard.) To the extent that the assessment uncovers such violations or risk of violations, it should proceed to specify the type of violation or quantify the potential impact and likelihood of risk so represented. Having established these parameters, the organization may more effectively correct violations and mitigate potential risks.

You should plan your risk assessment with the following goals in mind:

- To enhance the organization's ethics and compliance program to meet expectations and "best practices;"
- To coordinate methodology and scheduling, as appropriate, with the organization's existing enterprise risk assessment procedures;
- To identify and prioritize significant legal and ethical (or reputational) risks;
- To identify means by which to mitigate the most significant risks so identified by means of new or existing compliance program elements, and
- To establish a basis for continual improvement to the organization's risk management, synchronized with the organization's budgetary cycle.

Those goals will provide touchstones by which to measure your progress in conducting the risk assessment and, later, designing and implementing or improving an ethics and compliance program that will serve the organization's interests well. Those goals also lead you to a means by which that program will support the company's business goals and assist to establish support for the program (a "business case") that transcends its "compliance" nature.

Conducting A Risk Assessment

The Guidelines provide that a corporate compliance and ethics program "shall be reasonably designed, implemented, and enforced so that the program is generally effective in preventing and detecting criminal conduct." The group that the Commission had charged with reviewing the first ten years of the Guidelines' operation had expressed the view that "risk assessments need to be made at all stages of the development, testing, and implementation of a compliance program to ensure that compliance efforts are properly focused and effective." Report of the Ad Hoc Advisory Group on the Organizational Sentencing Guidelines (October 7, 2003), p. 87. The Guidelines as adopted by the Commission, however, "are clear about the role of risk assessment in compliance, [but] they are conspicuously thin on *how* one goes about doing a risk assessment." McGreal, "Legal Risk Assessment After the Amended Sentencing Guidelines: The Challenge for Small Organizations" *Corporate Counsel Review* (January 19, 2005), pp. 101, 115.

Before even beginning the formal risk assessment, one must gain a thorough understanding of the company's self assessment of its risk tolerance. This is the most daunting challenge and must start with an analysis of the firm's compliance and litigation history. Have there been numerous investigations, either by governmental agencies or internal auditors due to violations of law or policy? Is the business in an area that is highly regulated or under intense public scrutiny? Has the company been involved in litigation that could have been avoided by better internal controls? Is the organization under some sort of consent decree? Given that many compliance standards are not necessarily crystal clear, it is critical for the organization to evaluate how strictly it is willing or comfortable it is to operate within a "gray zone." The strictness of the application of compliance standards when so much is gray will depend on the responses to the questions raised above.

Having achieved an understanding of itself and its tolerance for risk, how does a company conduct a risk assessment with the goals listed above in mind? Begin with a clear action plan. Treat the effort to develop and implement a risk assessment as a project and apply project-management tools. You should begin with a "toolkit" – a methodology, task list, timeline – and a cast of players with clear ownership of various responsibilities before, during and in response to the risk assessment.

The toolkit need not have a lot of "bells and whistles" to be effective in identifying current or potential violations or risks of violations. In fact, it might only include:

- a methodology for identifying the external and internal requirements that apply to the organization (including an understanding of the various jurisdictions in which the organization operates);
- a methodology for identifying whether and how the organization's activities could violate those requirements;
- a methodology for addressing the findings of actual or potential violations (prioritizing, developing and implementing mitigating activities) (a risk assessment conducted to meet the Guidelines' standards may not necessarily qualify as "attorney work product" or even come within the attorney/client privilege, so consider carefully the privilege issues attendant to such an exercise; this issue is beyond the scope of this article), and
- a system for documenting the assessment's activities and their owners, the assessment findings, and then for tracking the mitigating activities that result (tasks, owners, timelines, etc.).

Numerous firms offer software and other tools for risk assessment, but be a cautious consumer. Most such software has been developed to serve the "enterprise risk management" requirements in the financial accounting field, particularly after enactment of the Sarbanes-Oxley Act, and may not be helpful in –

John M. Spinnato is vice president-general counsel, pharmaceutical operations, at sanofi-aventis in New Jersey. Debra Sabatini Hennelly is founder and president of Compliance & Ethics Solutions LLC, a consulting team bringing decades of in-house and outside experience to helping companies manage legal and reputational risk, building sustainable compliance programs and cultures of integrity. Information about the team is available at www.callces. com. Steven A. Lauer, who previously worked as in-house counsel, is director of Integrity Research, a division of Integrity Interactive Corporation of Waltham, MA, a provider of Web-based corporate ethics and compliance services to Global 2000 companies.

Please email Steven A. Lauer at slauer@i2c.com with questions about this article.

Volume 14, No. 10 © 2006 The Metropolitan Corporate Counsel, Inc. October 2006

Volume 14, No. 10 © 2006 The Metropolitan Corporate Counsel, Inc. October 2006

Volume 14, No. 10 © 2006 The Metropolitan Corporate Counsel, Inc. October 2006

or easily adapted to address – the non-financial, more intangible issues that arise in other regulatory areas or in the ethics arena. It may be more cost-effective to invest some time in reviewing the principles of the widely-regarded standard for enterprise risk management outlined in *Internal Control – Integrated Framework* developed by the Committee of Sponsoring Organizations of the Treadway Commission, as it contains much that can be extrapolated into the compliance and ethics risk assessment methodology. (See www.coso.org/.)

Outside experts, law firms and consultants can help in establishing risk assessment methodologies or managing this project, but the long-term sustainability of meeting the goals articulated above (as with the compliance program as a whole) relies on the assimilation of compliance and ethics risk mitigation into the day-to-day operations of the business. Accordingly, that might be achieved most effectively when the assessment is "home-grown," rather than having the look-and-feel of an outside audit. If required to choose between committing resources for acquiring sophisticated software or tools or freeing up internal personnel to contribute to the assessment, the latter may be the better choice.

Critical factors in assessing the organization's risk profile will be the participants and their roles. Regardless of the tools employed, an effective assessment will always require a broad understanding of the company's operations and a clear understanding of the regulatory schemes that apply across those operations and across the organization's locations. (For this purpose, you may need to involve several internal business people, subject matter experts and in-house counsel may yield some considerable tangible and intangible benefits, such as:

- gaining "buy-in" for the goals of the risk assessment and ownership among the business leaders for the related mitigation activities;
- educating business people about potential risks in their operations and activities;
- positioning in-house counsel and subject matter experts as the "go-to" resources for addressing the risks that are identified, and
- building traction for incorporating the mitigating behaviors and tasks into the day-to-day operations.

Having prepared your toolkit and identified your team, make sure that your methodology includes at least three basic steps. The first step entails an analysis of the business operations against applicable laws and requirements. A review of how the business operation meshes against the behavioral expectations of various external and internal audiences requires a detailed look at the activities of employees and agents of the business and how they interact with others, such as competitors, government officials, customers and suppliers.

You must understand whether and, if so, the extent to which the business operates in one or more regulated industries. While activities of all business entities must comply with certain government mandates, such as anti-discrimination requirements in the employment law arena and requirements for the proper disposal of hazardous substances, some industries are wholly or mostly regulated by the government. The development, manufacture, sale and marketing of pharmaceuticals, for example, must satisfy a host of regulations adopted by the federal Food and Drug Administration. Radio and television broadcasters must comply with those of the Federal Communications Commission.

In addition to the government's mandates, you should review other behavioral or operational standards that do or might apply to the business operations. A company whose stock is publicly traded on the New York Stock Exchange or through the channels of Nasdaq must satisfy the listing standards of the NYSE or Nasdaq, respectively. Industry standards, usually voluntary, may also be incorporated into market expectations or customer specifications such that their violation could affect the company's reputation. Many consumer products companies apply the product standards identified by the "UL" label or the "Energy Star" rating. Many global companies try to satisfy the United Nation's Declaration of Human Rights.

The company's own, expressed policies, procedures and external commitments can provide fodder for the company's critics and, for that reason, probably should also animate the analysis of possible risk. Those policies and procedures reflect a company's risk tolerance profile as they embody its own understanding and application of laws and regulations. The development of policies is the initial task that will most reflect the corporate commitment to compliance and its own understanding of the risks associated with its business. Benchmarking of industry standards in various industries almost always shows a wide variety of interpretations of the laws or regulations that give rise to the policy need. These differences reflect the varying cultures and histories of different organizations, though they may not reflect each organization's commitment to compliance or high ethical standards.

The Commission determined in 2004 that the Guidelines should cover actions that constitute criminal activity only, rather than "'violations of any law, whether criminal or noncriminal, (including a regulation), for which the organization is, or would be, liable...'" Such a broader scope had been recommended by the group to which the Commission delegated the task of reviewing the then-existing Guidelines and recommending any possible changes in light of then-extant experience. Those extra-legal standards of behavior often represent or influence the opinions and decisions of creditors, insurers, potential board members, current or future employees, jurors, investors and others whose judgments can impact the reputations or fortunes of businesses. Thus, they might merit attention in the assessment process.

With these considerations in mind, your risk assessment should examine current (and planned) operations against the external and internal standards you've identified in all of the jurisdictions in which you do, or expect to do, business. (A particularly problematic subject is that of a joint venture by two companies. Should the venture adopt the two companies' compliance and ethics policies or adopt its own, distinct ones? These questions are beyond the scope of this article, but worthy of consideration.) Document your approach and findings so that you can maintain a record of your activities and also drive improvements in how the organization addresses its compliance obligations and ethical commitments.

The expression, "you can't boil the ocean," bears some consideration in the context of risk assessment. The Guidelines provide that a corporate compliance and ethics program "shall be ***reasonably*** designed, implemented, and enforced so that the program is ***generally effective*** in preventing and detecting criminal conduct." (Emphasis added.) It would be unreasonable to expect a risk assessment to address all potential risk areas across all operations in all jurisdictions during its first run-through. Only a rare organization could sustain such activities while still attending to its regular business.

For this reason, the second step should include prioritizing the identified risks so that the company can address the most significant risks first. To do otherwise might squander scarce resources by allowing for limited employee focus on minor risks (those with very low potential impacts or those only remotely likely to occur). Such "low-hanging fruit" might seem easy to address and tick off the list – or might be in the bailiwick of an enthusiastic subject matter expert who proactively addresses that risk area – but focusing resources and attention on these activities could distract the company from identifying and mitigating more significant risks. During each cycle through the risk assessment, the organization can measure its progress in mitigating those more significant risks and then move down the risk inventory toward the lower-priority risks in order of lessening priority.

The third step involves systematically developing mitigating activities or tasks to address the prioritized risks previously identified. Each task must have an owner and a commitment for a time-frame for its completion. The prioritization approach of the second step, if addressed in a timely manner by this third step, can deliver important early successes, which will not only reduce the company's risk profile cost-effectively, but also help secure "buy-in" from the business people who are asked to own parts of the exercise. This step should also include procedures for reporting violations internally and, as required, externally, instituting internal investigations as necessary, and then tracking progress of correcting violations or mitigating potential risks.

Finally, an effective compliance and ethics program includes a commitment to continual improvement. With regard to the risk assessment, this means committing to on-going tracking of the implementation of the mitigating activities and a periodic (annual?) renewal of the risk assessment process, being sure to include new or revised requirements (external or internal) as well as reflecting any changes in the organization's operations or footprint locally or globally. Risk assessment is arguably the most difficult task in the development of an effective compliance and ethics program, given that it is necessarily subjective and requires not only a thorough understanding of the laws and regulations that affect the industry in question, but an understanding of the corporate culture by the compliance officer as well as the company itself. If well done, though, a risk assessment can lead to reduced risk and even operational improvements.

FOR METRO AREA IN-HOUSE COUNSEL

ALM

GC New York

MAY 9, 2005

The Big Picture

Compliance and knowledge management in today's law department.

BY JOHN M. SPINNATO AND STEVEN A. LAUER

IN THIS post-Sarbanes-Oxley world, corporate law departments no longer simply manage and provide legal services. Many corporate counsel are also responsible for their companies' corporate compliance programs. While the compliance-related responsibilities present demands that are distinct from — or even conflict with — those that flow from the legal-service role, they both require the creation, organization and reference to information and knowledge. Because some of that information arises outside of the organization, and sometimes the organization itself generates the relevant information, the department must know and understand the relationships among disparate information and data in order to successfully apply old information to new situations or new knowledge to old problems.

With what sorts of information and data must an organization's compliance program contend? Any information that will or might affect the firm's business operations presents sufficient value (positive or negative) for the firm that the compliance program should at least review that information in some fashion. That externally generated information includes the following: existing and new laws and regulations; interpretations promulgated by governmental administrative agencies; procedures and policies issued by various associations and standard-setting organizations; court decisions; and even news reports.

Ultimately, a company's compliance with law and practice depends on its employees and agents. If their day-to-day activities conform to those requirements and expectations, then the organization is in compliance; if those actions violate one or more of those standards, the firm is out of compliance. (The degree to which it is out of compliance — and the legal and other consequences that might flow from that noncompliance — will, of course, vary.) Providing all those employees and agents with the information by which they can know (1) what is expected of them and (2) how they should act so as to comply with those expectations, constitutes the core of a compliance program.

Vital to a law department's success in either role is its recognition that the same data can have differing significance in varying contexts. For example, in an environmental context, a specific level of contamination in a well, even a short-term reading, might represent a violation of law absent a prior permit from regulators allowing a heightened level during maintenance; knowledge of the existence and terms of that permit represents an important compliance knowledge requirement. How can an organization effectively assess a situation, which might require an investigation that could lead to the finding of a compliance violation, without knowing of the history and past practice of the firm and without having the tools to access information about that history and practice in order to apply that to the new compliance issue at hand?

To achieve success in either the law or compliance, then, the practitioner must create processes by which he or she maintains supremacy over the information that can so easily overwhelm people and organizations. In other words, knowledge management represents the key to a viable approach to the provision of legal service and to the assurance of compliance.

Adequate Information Is Crucial

Information and data that the organization creates itself represents a considerable amount and variety of material. That material could include at least the following types of information:

- the organization's basic ethical code of conduct (an essential, internally generated document);
- policies on various areas of concern, such as environmental or personnel policies;
- the delegation of authority to various employees to make specified types of decisions on behalf of the firm;
- procedures by which employees should address various types of issues;
- forms developed or used in specific transactions that might serve as templates for future matters;
- contracts and other documents relative to relationships between the firm and other organizations;
- correspondence with government officials;
- documents related to litigation; and
- internal correspondence (much of which likely exists only electronically).

Why does all that information matter in the context of compliance? Most directly, any of that information might relate to whether and how the organization complies with applicable standards of behavior.

Sometimes, compliance is measured against legal standards, as those contained in a law or a government regulation. Failure to satisfy those standards can lead to investigation by the government or even, in a worst-case situation, criminal proceedings. (If a compliance failure triggers criminal proceedings, of course, the role of a compliance program becomes much more important, since it can affect the sentence that a federal court applies to the firm.)

More frequently, though, a firm will find itself judged, in terms of its adherence to internal or external standards of behavior by other private parties. Private party disputes, if they proceed to litigation, generally will be adjudicated in court or a court-like proceeding, such as mediation or arbitration. The importance of compliance standards continues to grow in significance in these private party proceedings as they do in the governmental arena. This makes the urgency of developing appropriate compliance standards more critical than ever.

The inadequacy of information available to a business' employees can lead to compliance failures. Sometimes that information is the external type, as was the case in the situation that led to the jury verdict in New Jersey earlier this year against the concessionaire at a professional football game because an employee of that concessionaire had sold several beers to a fan at a game despite stadium rules against such a sale. The jury awarded punitive damages in favor of a child who was permanently disabled in an accident caused by that fan who was driving after the game while under the influence of alcohol. A situation of this type obviously calls into question the necessity of an adequate training program as an essential part of good compliance practice.

Internal policies as well as applicable laws and regulations must be adequately communicated to all employees and agents who in one respect or another represent an organization to the public. Recently, a family announced its intention to sue a major hotel chain, based in the United States, on account of the death of a child in a swimming pool at one of the chain's facilities in Southeast Asia. According to the family's announcement, they had selected the hotel overseas on account of the chain's reputation in this country, but the local hotel had not managed the swimming pool to the same standard of care as they had expected based on that reputation. Were the employees at that local hotel familiar with the hotel chain's policies and procedures vis-à-vis swimming pool maintenance and management? Were local laws and regulations followed? If not, how might the local hotel or the chain have better apprised the employees of the issues?

The Bandwidth Dilemma

While the deluge of information from outside the organization presents considerable challenges, the other sources of data and knowledge generate their own difficulties. Every firm creates data as it follows its business practices. Moreover, each employee generates information and also creates knowledge.[1]

One can quickly appreciate that the sheer volume of information to which a company's employees must have access will present possibly overwhelming challenges. While they must cope with that volume, however, businesses face the additional test of identifying which data elements present a sufficient basis for action or inaction. Differently stated, employees must separate the "wheat" from the "chaff" among the myriad pieces of information that flood their in boxes so as not to find themselves frozen into inaction on account of an overwhelming "data dump."

Data and information in electronic form, of course, present enormous issues in the litigation context, where discovery requests for such documents and electronic data can place huge burdens on companies dealing with the complexities of data storage for purposes of compliance with document-retention policies. Once they have organized the available data, employees must apply their knowledge of the business operation and its operational environment to identify those requirements that must be followed. In other words, they need to prioritize their activities. To do that, they must be conversant with the compliance standards as well as the information bombarding them.

The General Counsel Roundtable described the dilemma in a recent report. "The greatest challenge in identifying critical legal risks is limited bandwidth — legal departments lack the time and resources to process and prioritize an overwhelming quantity of risk-related information, while the business as a whole lacks the capacity to act on the prioritized risks effectively."[2]

The inability to focus on the highest-priority risks results from one or more of three causes: the excessive volume of information coming in; a failure to take advantage of knowledge already possessed by the organization; and a failure to communicate risk-related information to the business in a form comprehensible by that audience.[3] Effective management of risk requires effective management of data. Take, for example, the audit requirements of any good compliance program. An effective audit, even outside the traditional financial audit, which is essential to identify and quantify risks, cannot be conducted adequately without the ability to review data, which must be accessible — or in other words, managed.

While the influx of data presents challenges, once an organization has accumulated that information, it faces another high hurdle — rendering that information available to those who might make valuable use of it on behalf of the company: its employees and agents. In that regard, the bigger challenge for a compliance program constitutes communicating to each employee the information that will enable that individual to more effectively perform the duties of his or her job in order to meet the expectations — both internal and external — that concern the company from a compliance perspective. Knowledge management, alone and in a vacuum, does not suffice. Effective compliance is impossible without systems and processes that ensure that employees are educated and trained about that knowledge and how to use it.

Conclusion

Knowledge management represents a core competency of an organization. It can serve as the foundation for a comprehensive and effective compliance program. Fortunately, though, a functional knowledge management system serves other purposes also — purposes that directly support a business' operational and revenue-enhancing goals. The ability to access institutional knowledge and reuse or adapt it to the circumstances of a current operation can be a strategic advantage today by enabling the company to respond to market conditions faster.

By designing an effective knowledge-management protocol — a means for capturing, indexing and accessing data and knowledge — for its compliance efforts, then, a company will simultaneously enhance its business operations for other purposes. The compliance program should not represent a goal divorced from day-to-day business efforts. Rather, the two should exist in a symbiotic relationship supporting each other.

In any event, given the number of recent compliance- and ethics-related scandals, one can no longer hold any doubt as to the validity of the proposition that "good business and good ethics go hand-in-hand."

John M. Spinnato *is vice president-general counsel, pharmaceutical operations, at sanofi-aventis in New Jersey.* **Steven A. Lauer** *is director of Integrity Research, a division of Integrity Interactive Corp. of Waltham, Mass., a provider of Web-based corporate ethics and compliance services to Global 2000 companies. Mr. Lauer, who is based in Matthews, N.C., has previously worked as in-house counsel.*

1. Whereas the basic facts that they encounter while performing their jobs constitute "data," the understanding that employees develop in the course of their jobs equals "knowledge." Knowledge thus represents the ability of employees, agents and others — and ultimately the organization — to "make sense" of all the data that they encounter.

2. "Safeguarding the Corporation: Engaging the Enterprise in Compliance and Risk Management" ((c)2003, Corporate Executive Board, Washington, D.C.), p. 20.

3. "Safeguarding the Corporation," at 21.

BUSINESS ETHICS AND COMPLIANCE – ESTABLISHING AN EFFECTIVE PROGRAM*

David G. LaJoie and Steven A. Lauer**

Business ethics and compliance. It's a topic on the minds of many -- if not most or all -- corporate executives. It looms large in the awareness of the chief legal officer of virtually every corporation. It's a primary goal of ethics officers in corporate America. Given the recent business scandals, it is even on the minds of shareholders.

For many, compliance occupies that position of interest because of government scrutiny. Government agencies such as the Securities and Exchange Commission, the federal Health and Human Services Administration and, most significantly, the U.S. Sentencing Commission have indicated the benefits that a company might enjoy as a result of having a comprehensive, effective ethics and compliance program in place.

Will a program that focuses on compliance, but not ethics, suffice? What is the difference? Many companies have established compliance programs and identified compliance officers. What do those programs lack, if anything?

From the perspective of assuring that the company's activities conform to the legal mandates of the government, compliance provides some assurance of meeting that standard, if the program is effective. From a broader perspective, however, that approach may serve the company's interests only partially. In reality, compliance with applicable law and regulation merely defines the floor for the acceptable behavior of the company and its employees and agents. A comprehensive ethics and compliance program, on the other hand, attempts to challenge the organization continually to embrace true integrity and do what is right, not only what the law requires.

Further, a program designed to address the standards set by the government will be compliant only so long as those standards remain static. When government agencies revise their expectations, the compliance program must adapt, often under less-than-helpful time constraints. A program that incorporates ethical approaches, on the other hand, likelier will satisfy more than those agencies' currently expressed standards. If those standards become more demanding, the company will need to change its internal processes less dramatically than a company with a compliance-only approach.

While the establishment of an effective ethics and compliance process conveys very sound business benefits, other forces have brought this subject to the fore from a more mandatory perspective. In July 2002, Congress enacted the Sarbanes-Oxley Act of 2002 in an effort to eliminate at least some of the causes of corporate scandals of the past few years. Among other subjects, that new law enacted a requirement that an issuer of securities disclose whether it has enacted a "code of ethics" that applies to its principal executive officer and several other identified corporate executive positions. If a company has not adopted such a code, it must disclose that fact and an explanation of why it has not done so. The statute defines a "code of ethics" very specifically, and its definition does not cover a code that applies to all employees of a company. A code of ethics that satisfies that definition, however, might be part of a broader code that covers all employees.[1] The requirement that the existence of a code of ethics be disclosed to investors certainly increases the benefits gained by implementation of an effective ethics and compliance program.

The statute also mandates that the SEC adopt rules to require companies to disclose waivers granted to senior financial officers of the requirements of their ethics codes.[2] Congress intended, through that mandate in the Sarbanes-Oxley Act, to reduce the likelihood that corporate boards of directors would routinely waive ethics requirements for senior officers of their companies, as happened at Enron. See Pittman & Navran, "Corporate Codes of Ethics and Sarbanes-Oxley," Wall St. Law., July 2003, at 1, 3. The possibility of public scrutiny of such decisions by a board of directors certainly provides considerable incentive to grant such waivers much more judiciously than might otherwise pertain.

Another provision of the Sarbanes-Oxley Act pertains to this discussion. Section 301 of the law requires that the audit committee of a publicly held company "establish procedures for … (A) the receipt, retention, and treatment of complaints received by the issuer regarding accounting, internal accounting controls, or auditing matters; and (B) the confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters." The SEC issued final rules to implement that provision in the statute[3] and to provide some flexibility for companies in satisfying the law's mandate.[4] A hotline by which employees can report ethical lapses has constituted an element of an ethics program for some time though, and one that clearly constitutes the process that § 301 envisions.[5]

The existence of such mandates in the Sarbanes-Oxley Act certainly provides considerable reason to review your company's means of assuring compliance with the developing standards of corporate governance. Identifying what other statutes and regulations might relate to your company's operations would require, of course, a company-by-company analysis.[6]

If you accept the proposition that it is good to have a corporate business ethics and compliance process in your company, then you may ask the following: How do you put

---

[1] See Griffith, "Recent Developments under the Sarbanes-Oxley Act of 2002," *Lawyer's Brief*, Mar. 31, 2003, at 2, 10-11.

[2] See § 406(b) of the Sarbanes-Oxley Act. The SEC issued rules to implement that requirement on January 23, 2003. See "Final Rule: Disclosure Required by Sections 406 and 407 of the Sarbanes-Oxley Act of 2002," SEC File S7-40-04, Rel. No. 33-8177, adding § 229.406(d) to its rules. That release appears at www.sec.gov/rules/final/33-8177.htm.

[3] See www.sec.gov/rules/final/33-8220.htm#procedures.

[4] The SEC noted that "[w]e do not believe that a 'one-size-fits-all' approach would be appropriate. As noted in the Proposing Release, we expect each audit committee to develop procedures that work best consistent with its company's individual circumstances to meet the requirements in the final rule. Similarly, we are not adopting the suggestion of a few commenters that, despite the statutory language, the requirement should be limited to only employees in the financial reporting area."

[5] Whether a hotline that predated the Sarbanes-Oxley Act satisfies all of the requirements of that law should be carefully reviewed. For example, among other things, the statute requires that the audit committee develop procedures for the "receipt, retention, and treatment of complaints received by the [company] regarding accounting, internal accounting controls, or auditing matters; and the confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters." See § 301 of that law, adding § 10A (m) (4) to the Securities Exchange Act of 1934.

[6] The Sarbanes-Oxley Act applies to companies the shares or securities of which are traded publicly and that are required to file various reports with the SEC. The extent to which privately held companies must or should satisfy that statute's mandates may depend on future developments.

one together? Where do I start? How do I use limited resources to assure and document that the corporation is compliant with the numerous government requirements that apply? Which areas merit attention? What does an effective program look like? Of what does a compliance program consist?

Determining the scope of an ethics and compliance program is the first phase of the process. That scope depends on several factors. Some of those factors flow from the laws, regulations, and court decisions issued at various levels of government. What kind of industry are you in? Is it heavily regulated? What are the business risks? Are your employees aware of these risks? What potential impacts do its operations have? Who might be impacted by those operations (particularly if those operations do not proceed in accordance with law or other applicable requirements)? How significant (i.e., harmful) might those impacts be?

After you've determined what substantive and operational areas merit attention, the next phase is to design a program that's appropriate to satisfy those compliance needs. That program should reflect the legal and operational challenges of your business (those identified in the first phase). You must understand those business operations well and determine the most effective means of assuring compliance with the applicable laws and other requirements and of ameliorating the potential adverse effects of those operations.

Let's explore that analysis in a hypothetical, but realistic, context. Assume that a company invests in real estate in a variety of ways. It purchases and sells improved real property (i.e., it's an equity investor); it purchases property (either undeveloped or developed by former owners) and improves that land by constructing, improving, or renovating improvements on that property (housing, office buildings, or another type of structure); it lends money to others who own real estate, with repayment secured by a lien on the borrower's property; and it manages real estate owned by others. What compliance issues does that company face?

There are at least four primary purposes of an ethics and compliance program for such a company:

1. to achieve conformity with legal and regulatory requirements;
2. to achieve conformity with behavioral and values expectations expressed within the company;
3. to achieve consistency in its treatment of similar issues and similarly situated persons; and
4. to achieve full, careful responses to government inquiries.[7]

How do those purposes animate the process of designing an appropriate ethics and compliance program for a company with the above-described activities? You canvas the laws and regulations that apply (or might apply) to those activities. As examples:

1. The lending activities may require licensure in one or more jurisdictions. They may be subject to certain behavioral constraints such as usury laws.
2. The ownership and management of real estate may trigger obligations vis-à-vis the physical safety of guests and licensees.
3. The sale of property may trigger obligations of disclosure (to purchasers and potential purchasers) and even of nondiscriminatory treatment (fair housing laws).
4. To develop unimproved real estate, one must be mindful of laws and rules that relate to navigable water (the need for permits to accomplish certain things), wetlands (the obligation to preserve, and in some cases restore, any such habitats that might be adversely impacted by the development), and other concerns.

Nearly deserving of separate, complete treatment are environmental responsibilities attendant to the real estate activities described above. The scope of environmental regulation by government at all levels[8] is very significant. The regulations are often detailed.

So, what would a real estate-related compliance program include? First, you must investigate for any applicable requirements among laws and regulations. Second, if any of the company's activities require that the company hold government-issued permits or licenses, establish a mechanism for securing and maintaining those permits or licenses. An ethics and compliance program requires that business activities be controlled in order that activities that require a license not be undertaken without a license, or that, if such activities are undertaken without permission, the company can secure a license in timely fashion, and that, if the license is held by the company, activities are conducted in accordance with terms of that license.

A company must be able to detect its own violations of applicable requirements (whether internally or externally generated). Any violations so discovered must be corrected and perhaps even disclosed.[9]

An effective record-keeping system is an important -- and often overlooked -- element of a comprehensive ethics and compliance program. If a company has complied with all applicable requirements fully -- it has appropriate licenses, its decisions and actions accord with law, etc. -- would it be able to establish that conformity if a government agency inquired? Every company should assure that its record- keeping procedures satisfy both external and internal requirements.

A mechanism by which a company can audit its operations for legal conformity is another critical component of a compliance program. Not only does a good audit function help to ensure substantive compliance with the law, but it can be particularly helpful in any dealings with government agencies. The more government officials believe that they can rely on a company's auditing and investigative functions to identify examples of

[7] At first blush, this fourth purpose may seem to replicate the first (conformity with legal requirements), but we use the phrase to suggest a broader goal. A credible, effective compliance program is not only a significant factor in determining what penalty the government might apply when a company is found to have violated the law (see the discussion of the Sentencing Guidelines below), but it can affect the length, detail, scope, and seriousness of an investigation (or preliminary inquiry) by a government agency, even an investigation or inquiry that never results in sentencing under those guidelines.

[8] While the federal government's regulatory enactments are best known (e.g., the Clean Air Act, the Clean Water Act, Superfund), state and local laws, ordinances, and regulations have proliferated since 1970. Many of the requirements of the latter jurisdictions' enactments are even more stringent than those of federal agencies. Sometimes they are to some degree inconsistent. That they are not to be ignored is the salient point.

[9] Whether and, if so, how to report violations to a government agency is a separate subject that is beyond the scope of this article. The considerations involved in making that determination can be numerous and complex.

noncompliance, the more likely they are to accept a company's representations in the course of an investigation.

Training is an important element of any ethics and compliance program. Inasmuch as such a program will be judged by its effectiveness, the degree to which its substantive terms inform the day-to-day actions of a company's employees might provide the critical difference between constituting an effective program and an ineffective one.[10]

Having identified the necessary components of a company's ethics and compliance program, you must create them. In doing so, you must take into account more than legal issues. Operational factors demand consideration. An ethics and compliance program that imposes on a business unattainable behavioral standards is not only doomed to fail, it may create liability beyond that of the substantive legal requirements.

This is particularly true in situations to which the Federal Sentencing Guidelines apply. Those guidelines provide for beneficial treatment of a company that has an "effective" compliance program. Thus, an ethics and compliance program that, while well designed (intellectually, that is), cannot be satisfied by the operations to which it applies, will serve to highlight lapses more than it can eliminate them.

The more you can design ethics and compliance-related activities that build off activities that have independent, business-oriented purposes, the more successful that compliance program will be. For example, requiring that a duplicate copy of a document that is already prepared as part of a transaction be filed in a compliance-related repository is far better than expecting that the business personnel will prepare an additional document solely for compliance purposes.

In other words, design your ethics and compliance program so that its elements represent the least additional burden for the company that you can. Creating more bureaucracy should never be a goal. Try to integrate these activities into existing processes as much as possible, rather than erecting a separate ethics and compliance-oriented process solely.

** David G. LaJoie is the Director of Business Ethics and Compliance for the Integrated Defense Systems business of Raytheon Company, Tewksbury, Massachusetts. Steven A. Lauer is Director, Integrity Research, Integrity Interactive Corporation, Maplewood, New Jersey (e- mail slauer@i2c.com).

[10] The Office of the Inspector General of the U.S. Department of Health and Human Services and the American Health Lawyers Association jointly developed a document entitled "Corporate Responsibility and Corporate Compliance: A Resource for Health Care Boards of Directors," on page 8 of which they said as follows: "A critical element of an effective compliance program is a system of effective organization-wide training on compliance standards and procedures. In addition, there should be specific training on identified risk areas, such as claims development and submission, and marketing practices." That document is posted at http://oig.hhs.gov/fraud/docs/complianceguidance/040203CorpRespRsceGuide.pdf.

the GLOBAL COMPLIANCE LANDSCAPE:

A Resource File

If you're the chief compliance officer, you know how important it is to keep the company's ethics and compliance program current with the law, including the recent changes in the United States Sentencing Guidelines for Organizational Defendants (the "Guidelines"). But if your company is a multinational, it isn't enough just to keep up with US law—you also need to know how developments in other countries affect your compliance program.

And international compliance is a big issue. Compliance is difficult enough when a company operates in just one country. Keeping up with the myriad of laws, regulations, and industry-specific standards is a significant ongoing burden, as is keeping your employees up-to-date about changes in your firm's compliance policies. But the difficulties become much greater when a company does business in multiple countries. For instance, acts that might violate the laws of one country might be accepted or even preferred behavior in another.

In this article, we examine some of the challenges facing multinational firms in developing and implementing global ethics and compliance policies and offer you resource files on the following topics:

- Developments around the world affecting corporate compliance and ethics programs in certain (but by no means all) countries of particular current interest to global compliance officers. (See "Mapping Global Compliance Developments," on p. 44.)
- Two hot topics: efforts to eliminate corruption in business dealings and the use of hotlines to enable whistleblowers to report questionable business activities. (See "International Anticorruption" on p. 42 and "Whistleblower Hotlines" on p. 36)
- Creating an effective global compliance program that supports your company's business goals. (See "Tips for Global Compliance Programs," on p. 40.)

The business case for compliance is a strong one. Even given the complexities it involves, global compliance is good business. It will keep your company out of hot water—and more than that, it can provide your company with a competitive advantage in the market.

By Alan Greenwood and Steven Lauer

Alan Greenwood is ethics & compliance officer at Dow Corning Corporation. He is currently based in Belgium; his previous work as corporate lawyer has included stints in Shanghai, Tokyo, and Michigan. He can be reached at alan.greenwood@dowcorning.com.

Steven Lauer is director, Integrity Research, at Integrity Interactive Corporation, a company based in Waltham, Massachusetts, that offers a unique combination of best-practice ethics and compliance expertise, effective employee-training courses, and a defensible delivery process that together comprise a comprehensive solution for companies' compliance-training needs. He can be reached at slauer@i2c.com.

THE FORCES DRIVING GLOBAL COMPLIANCE STANDARDS

Until recently, the US government followed a laissez-faire approach to business, and the EU countries similarly trusted companies to act responsibly. Recent events, however, have exposed the vulnerabilities of these approaches. In the United States, scandals at Enron, WorldCom, Adelphia, and other corporations over the past five years have proved to many that business does not deserve unquestioning trust. More recent corporate scandals involving European companies, such as Parmalat, Ahold, Royal Dutch Shell, and Adecco, have increased pressures on regulators in the EU countries to be more active in monitoring and regulating corporate conduct.

In parallel with this growing international concern over corporate behavior, the integration of global capital markets has fueled a growing international consensus that companies need well-defined governance practices. Every country with a stock market—including China, Mexico, and Zimbabwe—has adopted corporate governance codes in which codes of ethics and/or compliance programs for the board and members of the organization are either explicitly mandated or strongly recommended as a central component of good governance. Supranational entities such as the OECD (Organization for Economic Co-operation and Development) and OAS (Organization of American States), together with a variety of nongovernmental organizations (NGOs), including Transparency International and the Fair Labor Association, monitor the activities of governments and private business and highlight failures to adhere to governance and compliance standards. (See "Look Who's Watching You Now," on this page.)

The internationalization of compliance standards has also been fueled by recent globalization. If a company is subject to the compliance rules of a government or supragovernmental organization, the company is usually expected to satisfy these standards in all of its locations throughout the world. Business leaders have generally supported these trends because they tend to promote similar standards and values and thus avoid confusion about what behavior is expected of employees no matter where they are working.

US government agencies have played a key role in this internationalization of standards. The Guidelines, promulgated by the United States Sentencing Commission in 1991 and modified greatly in 2004, have served as one of the primary catalysts for the development and increasing maturity of corporate ethics and compliance programs. Because the Guidelines apply to organizations based in the United States and so many of the world's largest companies are domiciled there, the Guidelines have had a huge impact on corporate ethics and compliance programs worldwide,

(continued on page 38)

LOOK WHO'S WATCHING YOU NOW

- Transparency International and Amnesty International each monitor private actors in the international arena.
- Worldwide Responsible Apparel Production describes itself as "an independent, non-profit corporation dedicated to the certification of lawful, humane and ethical manufacturing throughout the world."
- The Fair Labor Association works "to promote adherence to international labor standards and improve working conditions worldwide."
- The International Council of Toy Industries has developed ethics guidelines intended to ensure safe and humane workplace environments for all workers in toy factories.

WHISTLEBLOWER HOTLINES

YOU KNOW HOW TO WHISTLE, DON'T YOU?

The United States leads the way in the use of hotlines and similar mechanisms to promote whistleblowing, but over the past dozen years, there has been a growing international trend towards protecting whistleblowers. Nearly all common law countries, including Australia, Canada, New Zealand, South Africa, and the United Kingdom, have adopted national or local rules that protect whistleblowers in many parts of society. "Whistleblower protections are also gaining ground in Europe, Asia, and Latin America. Several international instruments, including multilateral treaties, institutional regulations and codes of conduct now include protections for whistleblowers."[1]

COUNTRY	STATUTE	DESCRIPTION
Australia	Workplace Relations Act of 1996 (as amended) §170CK Available at *www.austlii.edu.au/au/legis/cth/consol%5fact/wra1996220/s170ck.html*	Protects a worker from termination of employment that is based, at least in part, on the employee's having filed "a complaint, or . . . participat[ed] in proceedings, against an employer involving alleged violation of laws or regulations or recourse to competent administrative authorities." Provides remedies in the event of a retaliatory discharge, an administrative process for the issuance of implementing regulations, and a judicial process by which terminated employees might seek redress for violations of the statute.
New Zealand	New Zealand's Protected Disclosures Act of 2000 §§ 6(1)–9 Available at *www.legislation.govt.nz/browse_vw.asp?content-set=pal_statutes*	Provides that an employee may disclose information in the manner provided by the Act if (a) the information is about serious wrongdoing in or by that organization; and (b) the employee believes on reasonable grounds that the information is true or likely to be true; and (c) the employee wishes to disclose the information so that the serious wrongdoing can be investigated; and (d) the employee wishes the disclosure to be protected. Requires that the disclosure be made according to the organization's internal procedures "for receiving and dealing with information about serious wrongdoing." However, disclosure may be made to "an appropriate [governmental] authority" if the employee believes that "the head of the organization is or may be involved" in the wrongdoing, that exceptional circumstances require immediate reference to an appropriate authority, or no response to an earlier disclosure has occurred and at least twenty days have passed.

And of course in the United States, Sarbanes-Oxley has had an effect. A survey conducted in July 2003 (one year after the enactment of the statute) found that 79.2 percent of the responding companies had established some type of hotline that enabled employees to anonymously raise ethics or compliance issues.[ii] Moreover, the 2004 changes to the Guidelines have created an additional incentive for companies to encourage whistleblowing. The Guidelines (§8B2.1 (b)(5)(C)) provide that a company's sentence can be reduced if it has established a method that lets the organization's employees and agents anonymously "report or seek guidance regarding potential or actual criminal conduct without fear of retaliation."

COUNTRY	STATUTE	DESCRIPTION
South Africa	The Protected Disclosures Act, 2000 §3	An employee is guarded against "occupational detriment" on account of having made a protected disclosure. Such a protected disclosure can be, in certain enumerated circumstances, a revelation to someone other than that employee's employer, such as a public official or a third party. The term "occupational detriment" covers discipline, transfer, suspension, harassment, intimidation, and other types of harmful actions.
United Kingdom	Public Interest Disclosure Act of 1998 Available at *www.opsi.gov.uk/acts/acts1998/80023—b.htm#2*	Any worker is protected who makes a "qualifying disclosure" in good faith to his or her employer, or in certain situations to another person, about a crime or a failure to satisfy a legal obligation, among other subjects. The worker is protected against "any detriment by any act" so long as his "qualifying disclosures" are made in the manner prescribed by the law.
United States	The Sarbanes-Oxley Act of 2002 15 U.S.C. §78f(m)(4), as added by §301 of the Sarbanes-Oxley Act of 2002, Pub. L. 107-204. Congress had earlier adopted the Whistleblower Protection Act of 1989, but that statute protects only federal employees, not employees in private industry. See 5 USC §§1201–1222.	Audit committees of publicly traded companies must "establish procedures for . . . the receipt, retention, and treatment of complaints received by the [company] regarding accounting, internal accounting controls, or auditing matters; and . . . the confidential, anonymous submission by employees of the [company] of concerns regarding questionable accounting or auditing matters." These mandated procedures are largely intended to encourage whistleblowing.

WHISTLEBLOWER HOTLINES

NOTES

i. R. Vaughn, T. Devine, and K. Henderson, *The Whistleblower Statute Prepared for the Organization of American States and the Global Legal Revolution Protecting Whistleblowers*, 35 GEO. WASH. INT'L L. REV. 857, 861 (2003) (footnotes omitted).

ii. "Business Ethics and Compliance in the Sarbanes-Oxley Era: A Survey by Deloitte and Corporate Board Member Magazine," available at *www.deloitte.com/dtt/cda/doc/content/us_assur_ethicsCompliance%281%29.pdf*.

(continued from page 34)

and have become a de facto global standard. To the extent that there is an EU approach to this issue, it has been much less up-front and less legalistic: The EU Commission actively supports the development of CSR (Corporate Social Responsibility), but it has stopped short of promoting compliance programs.

The definition provided by the Guidelines of when an ethics and compliance program can be called "effective" has animated many countries' efforts to elevate corporate behavior. In some countries, the authorities have not adopted any of the Guidelines per se, but have just suggested or strongly recommended that business organizations adopt higher standards of conduct through better ethics and compliance programs. The specifics of how to achieve this goal are left to businesses, with the expectation that those businesses will use the Guidelines as a template.

THE BUSINESS CASE FOR COMPLIANCE

Compliance programs can serve a variety of business purposes. For instance, the training that your company provides for compliance purposes should help employees perform their jobs, and should not focus merely on satisfying their compliance responsibilities.

Quality control. Information gleaned from hotline submissions can help improve business operations. As one prominent consultant has noted, organizations "are making greater efforts to listen for feedback and signs of trouble, just as one might monitor quality on a production line."[1] Since the quality of a business process that consists entirely, or almost entirely, of a service can be difficult to measure (unlike the output of a production line), a hotline might in fact serve as the best means of assuring such quality.

Risk management. The same prominent consultant has also observed that "[o]verall, existing business ethics activities are perceived to improve business performance, *not* hinder it." Business ethics protect companies from risks involved in violating the law, legal regulations, or company policies—including the risk of damage to a company's reputation. Business ethics can thus even help to create competitive advantage.[2]

Stock performance. There is also evidence that good corporate governance procedures are strongly correlated with above-average stock returns. A study of stock prices in the 1990s found that

> [a]n investment strategy that purchased shares in the lowest-*G* firms ("Democracy" firms with strong shareholder rights) and sold shares in the highest-*G* firms ("Dictatorship" firms with weak shareholder rights) earned abnormal returns of 8.5 percent per year… The results for both stock returns and firm value are economically large and are robust to many controls and other firm characteristics.[3]

The self-interest of corporations thus counsels a strategy that takes ethical concerns into account in their business activities.

Stakeholder expectations. Finally, compliance programs also serve companies' broader interests by helping them meet the expectations of internal and external stakeholders. Whether those stakeholders are the company's employees, shareholders, government agencies, extranational organizations, or NGOs, a business that incorporates certain behavioral norms into its day-to-day operations will fare far better. With fewer concerns for adverse publicity on account of ethical lapses and a deeper fund of societal goodwill to draw from, such a business should enjoy a smoother journey.

Register for session *509: A Comparative Review of Multinational Compliance Programs* at ACC's Annual Meeting, October 17–19, in Washington, DC. In this session you will learn how to help your company use compliance as a competitive advantage internationally. This program will examine leading multinational compliance programs, including a discussion about the tensions between compliance and decentralized international management structures, types of international risks, and tools that are available to assist you.

For more information and to register for the meeting, visit *www.acca.com/am/05*.

A WORLD OF COMPLIANCE

As chief compliance officer, how should you

(continued on page 49)

TIPS FOR GLOBAL COMPLIANCE PROGRAMS

Seven Ways to Improve Your Global Program

Be globally conscious. When implementing a compliance program or developing compliance policies and procedures covering multiple countries, make sure to remember your company's international status. Avoid policies focused on the United States that ignore the needs and practices of other countries where your company does business. Company encouragement for whistleblowers, for instance, is widely accepted in the United States and other common law countries, but it is looked upon with great suspicion in France and Italy, where people have unpleasant memories of collaborators during World War II. For example, in June 2005, McDonald's was told by La Commission Nationale de l'Informatique et des Libertés of France that it must excise from its code of conduct references to its reporting hotline, which the French government would not allow. East Europeans are even more hostile to the idea of anonymous reporting because of their recent experiences of life under a spying, totalitarian system.

Create consensus. Create a consensus throughout your company on the goals for the compliance effort and take the time to gain understanding and support for your program, especially in countries with works councils and labor unions. Some of these bodies may consider whistleblower and hotline procedures as infringing on bargained-for grievance procedures and may raise issues such as those raised in the Wal-Mart case cited below. (And see "Mapping Global Compliance Developments," on p. 44.) One useful approach is to form a group whose mission is to provide direction for the program. The group should include personnel from multiple countries and business units, to better reflect the interests of all significant parts of the company.

Identify shared values. With the assistance of a multinational coordinating employee group, identify the ways in which all employees share values. Make sure to highlight these shared values in the ethics and compliance program. This helps foster a greater sense of community among your far-flung employees, helping them to focus on what they have in common, rather than their differences.

Emphasize resource diversity. Distribute your company's ethics and compliance resources throughout various countries where your company does business. This helps ensure that your compliance procedures are sensitive to local needs. For the same reason, ethics and compliance positions should be staffed by people from a variety of countries.

Translate carefully. Make compliance and ethics materials available in multiple languages. But be aware that terms commonly used in the United States, such as "ethics," may not readily translate into some other languages. As one commentator notes, because the term "ethics" often does not translate well, some organizations reframe the concept through other terms such as integrity, business practices, or responsible business conduct. (See Nathan Hurst on Corporate Ethics, as cited in "From this point on," on p. 48.) All translations should appropriately reflect the vocabulary and idioms used by local people. This might require translation into a locally used dialect or language. For example, the Spanish spoken in some countries in South America varies from Castilian Spanish.

Train. Do not simply distribute the code of conduct and expect all employees to properly follow its rules. Particularly in light of linguistic complexities, some training and assistance must accompany the code.

Publicize the benefits. Business units often resent new initiatives that emanate from corporate with little apparent regard for the exigencies of the operating businesses. Hostility can be even more pronounced when initiatives from the company's headquarters affect employees in a distant country that has a very different social milieu. (Such resentment may have fueled the opposition to Wal-Mart's implementation of its corporate code of conduct. See *www.dw-world.de/dw/article/0,1564,1519102,00.html.*) To minimize such resistance to compliance rules, show the employees that compliance rules help your company's business and are not just another time-wasting corporate exercise. Make sure that the business units have an investment in the program and that they recognize the benefits they will gain from an effective compliance effort.

INTERNATIONAL ANTICORRUTION

The Growing Global Effort Against Corruption

Many countries have adopted anticorruption legislation in accordance with a growing international effort to eliminate corruption. (For more information, see "From this point on," on p. 48.) Those laws usually make it a criminal offense to accept bribes, but fail to punish those who give bribes. But there is growing demand for stronger anticorruption compliance policies.

Entity	Convention or Law	Description
EU	1998 Joint Action on corruption in the private sector, arts. 2.1 and 3.1 Available at *http://europa.eu.int/eur-lex/pri/en/oj/dat/1998/l_358/l_3581998l231en00020004.pdf*	Criminalizes both active and passive corruption conducted "in the course of business activities," even if no public figure or government action is involved. "Passive" corruption is (generally speaking—see the Joint Action definition) violating a duty by requesting or receiving an undue advantage in exchange for performing (or not performing) an act, whereas "active" corruption is offering or giving such an undue advantage.
OAS	The Inter-American Convention Against Corruption in 1996 (art. III, §10) Available at *www.oas.org/main/main.asp?sLang=E&sLink=http://www.oas.org/juridico/english/fightcur.html*	Includes identified "mechanisms to ensure that publicly held companies and other types of associations maintain books and records which, in reasonable detail, accurately reflect the acquisition and disposition of assets, and have sufficient internal controls to enable their officers to detect corrupt acts."
OECD	Convention on Combating Bribery of Foreign Officials in International Business Transactions, Art. 1, §1 Available at *www.oecd.org/document/21/0,2340,en_2649_34859_2017813_1_1_1_1,00.html#text*	The contracting nations agree to criminalize giving "any undue pecuniary or other advantage. . . to a foreign public official. . . in order that the official act or refrain from acting in relation to the performance of official duties," in order to gain improper advantage in the conduct of international business.
UN	The United Nations Declaration against Corruption and Bribery in International Commercial Transactions, adopted by the General Assembly in 1996	Covers both the private and public sectors. This document, more of a political commitment by the voting nations than a legal one, is part of an international effort to promote transparency in business transactions.
US	Foreign Corrupt Practices Act (FCPA), 15 U.S.C. §78dd-3	Prohibits firms that are registered in the United States and foreign corporations the shares of which are traded on United States stock exchanges from offering or giving anything of value to foreign officials or other specified persons, except for certain types of payments.

MAPPING GLOBAL COMPLIANCE DEVELOPMENTS

Six Compliance Hotspots

CHINA

Some might be surprised to learn that in China, certain types of compliance programs have entered the landscape, in spite of—or in the absence of—any lead from the state. The chief drivers have been the compliance certification programs of the global business supply chain in the industries where China is playing an increasingly dominant role, such as textiles and garments.

For the central government, the task of combating corruption remains the primary focus. Thousands of officials are prosecuted each year for corruption, but the problem remains massive, because the number of officials employed by all levels of government in China exceeds the populations of many countries.

Another government priority—induced by China's accession to the WTO in 2001—has been to abolish more than 2,600 laws and regulations and, in a number of areas, to publish new laws providing for greater transparency. China's commitments to the WTO include opening its capital markets to foreign competition by 2007, which serves as a powerful stimulant for further regulatory transparency.

Even though (with the exception of the annual anticorruption drives) there is no prospect of any domestically sponsored initiative to promote compliance programs, China is no stranger to focused compliance programs, certifications, and audits, many driven, as stated above, by the global supply chains of industries in which China now plays such an important role. The standards endorsed by international NGOs have therefore been introduced into a number of industries, such as clothing and garments.

EUROPE

United States and European multinationals have served as active propagators of codes of conduct in many countries. Such efforts often are driven by nonlegal factors, particularly the desire to create a common set of values throughout the organization. The deployment of such codes is not always smooth sailing, however, especially in civil law countries. France and Germany, for example, have strong traditions of labor contracts and collective agreements. Wal-Mart, which operates more than 90 stores in Germany, recently discovered this in the venue of the Labor Court (Arbeitsgericht) of Wuppertal. The Arbeitsgericht Wuppertal is reported to have recently granted an injunction filed by the group works council of Wal-Mart against parts of Wal-Mart's Code of Conduct for employees. The court said in its decision that certain guidelines (concerning the love life of employees or the telephone ethics hotline which employees are asked to use to report code violations) contradict German labor law. It ordered the company to delete from its Code guidelines relative to relationships between coworkers that prohibited "any kind of communication that could be interpreted as sexual." (The Arbeitsgericht Wuppertal has yet to issue a written decision, and this description is based on various newswire reports. See, for example, *www.indexonline.org/en/indexindex/articles/2005/2/germany-wal-mart-ethics-code-blocked-by-cour.shtml.*)

IRELAND

Ireland has become an increasingly attractive location for corporations in the United States that wish to enter the EU market, because Ireland is the EU member closest to the United States geographically and shares many attributes with the United States. In December 2004, Ireland's Office of the Director of Corporate Enforcement (ODCE) issued regulations of great potential interest to such companies. These regulations are designed to help companies comply with the Companies (Auditing and Accounting) Act of 2003.

Section 45 of the Companies (Auditing and Accounting) Act of 2003 requires company directors (a title that applies to corporate officers who would be considered senior management in the United States) to prepare a "compliance statement" that specifies the company's "(a)…policies respecting compliance with its relevant obligations; (b) its internal financial and other procedures for securing compliance with its relevant obligations; (c) its arrangements for implementing and reviewing the effectiveness of the policies and procedures referred to in paragraphs (a) and (b)." (See *www.oireachtas. ie/documents/bills28/acts/2003/a4403.pdf.*) The ODCE guidance—much like SEC pronouncements on securities statutes in the United States—provides guidance to companies subject to the statute on how to prepare the required statements. (It can be found at *www.odce.ie/_fileupload/publications/Revised_ Guidance_on_Directors_Compliance_Statements_Final.doc.*)

The statute also requires company directors to issue an annual statement in which they affirm the ongoing effectiveness of the procedures for assurance of compliance. The annual statement seems to resemble the certification required by § 302 of Sarbanes-Oxley.

MAPPING GLOBAL COMPLIANCE DEVELOPMENTS

Compliance Hotspots (Cont'd)

JAPAN

Japanese society has long frowned on those who expose unpleasant facts, and Japanese business has a long tradition of sweeping corporate misconduct under the rug. In 1998, for instance, a bond trader at Daiwa Bank incurred $1.1 billion in losses, but the bank's directors withheld disclosure of the losses from US bank regulators until the directors had completed their own internal assessment. The bank was later required to shut down its US banking operations.

After lengthy deliberations, the Japanese Diet in March 2004 enacted the Whistleblower Protection Act (law No. 122 of 2004). This law does not come into effect until April 2006 and is reported to have been substantially inspired by and modeled on the UK Public Interest Disclosure Act (1998). In contrast to some of the many other countries with whistleblower laws, including Ghana, Israel, and Australia, the Japanese law applies to disclosures in the private as well as public sectors.

In another interesting private sector development, the Japanese Pharmaceutical Manufacturers Association (JPMA) has expanded on its Charter for Good Corporate Conduct by issuing the JPMA Compliance Program Guidelines. These 2001 guidelines provide guidance for JPMA members on how to meet appropriately high ethical standards of behavior. According to these guidelines, the compliance programs of all JPMA member companies should at minimum satisfy the eight requirements for an effective compliance program set out in the US Guidelines. (Available online at *www.jpma.or.jp/12english/publications/guide/02.html.*)

KOREA

Since the Korea Independent Commission Against Corruption (KICAC) began operating in 2003, this government-established organization has been working to protect whistleblowers and to encourage their activities by providing "appropriate rewards." The KICAC has had reasonable success in uncovering corruption. In one case, for instance, a high official of IBM Korea Inc. was prosecuted for offering bribes to government officials and illegally colluding with competitors in order to obtain government contracts worth 66 billion won (approximately $55 million).

UNITED KINGDOM

Corporate failures in the 1980s led the UK government to establish a series of groups to study business governance and other issues. Those groups issued reports that recommended a variety of corporate reforms. (One such report, which proved very influential, is known as the Cadbury Report. It is available online at *http://rru.worldbank.org/Documents/PapersLinks/1253.pdf.*) The government responded by issuing the Combined Code, which incorporates the reports' recommendations on corporate governance and internal control. (The Combined Code is available online at *www.fsa.gov.uk/pubs/ukla/lr_comcode.pdf.*)

Among other things, the Combined Code "contains the corporate governance principles and code provisions applicable to all listed companies incorporated in the United Kingdom." In addition to setting out specific best practices, the Combined Code contains principles that underlie those practices, so as to provide guidance for situations for which specific answers might not exist in the Combined Code itself.

From this point on . . .
Explore information related to this topic.

ACC RESOURCES ON INTERNATIONAL COMPLIANCE

ACC's committees, such as the International Legal Affairs Committee, are excellent knowledge networks and have listservs to join and other benefits. Contact information for ACC committee chairs appears in each issue of the *ACC Docket*, or you can contact Staff Attorney and Committees Manager Jacqueline Windley at 202.293.4103, ext. 314, or *windley@acca.com* or visit ACC Online℠ at *www.acca.com/networks/committee.php*.

- *Doing Business Internationally*, an ACC InfoPAK℠, available on ACC Online at *www.acca.com/infopaks/intbus.html*.
- E. Scott Gilbert, *603: Globalized Risk: Internal Investigations Outside the US*, ACC 2004 Annual Meeting course material, available on ACC Online at *www.acca.com/am/04/cm/603.pdf*.
- *The Global Law Department*, an ACC InfoPAK, available on ACC Online at *www.acca.com/infopaks/global.html*.
- Leading Practices in Global Law Department Design and Service Models: What Companies Are Doing, an ACC Leading Practices Profile, available on ACC Online at *www.acca.com/protected/article/international/lead_globallaw.pdf*.
- Richard Mosher and Owen Warnock, *"All For One and One for All: Navigating Trade Unions and Work Councils in Europe"* ACC Docket 23, no. 2 (February 2005): 48–67, available on ACC Online at *www.acca.com/protected/pubs/docket/feb05/union.pdf*.
- Lori Shapiro and Philip Weis, *803: Codes of Conduct for Multinational Corporations*, ACC 2004 Annual Meeting course material, available on ACC Online at *www.acca.com/am/04/cm/803.pdf*.

If you like the resources listed here, visit ACC's Virtual Library℠ on ACC Online℠ at www.acca.com/resources/vl.php. Our library is stocked with information provided by ACC members and others.

If you have questions or need assistance in accessing this information, please contact Senior Staff Attorney and Legal Resources Manager Karen Palmer at 202.293.4103, ext. 342, or palmer@acca.com. If you have resources, including redacted documents, that you are willing to share, email electronic documents to Julienne Bramesco, director of Legal Resources, bramesco@acca.com.

FOR ADDITIONAL INFORMATION

- Anticorruption Resources
  - Anticorruption efforts in countries belonging to the Anti-Corruption Gateway for Europe and Eurasia, available at *www.nobribes.org/en/country_information/default.asp*.
  - "Combating Corruption: OGP Progress Report," Report No. 1.21/334 (December 2002), p. 7, issued by the International Association of Oil and Gas Producers, available at *www.ogp.org.uk/pubs/334.pdf*.
  - "First to Know: Robust Internal Reporting Programs," by Trace International, ISIS Asset Management, and The International Business Leader Forum (2004), available at *www.isisam.com/uploadfiles/co_gsri_first_to_know_jul_2004.pdf*
- T. Dworkin, *Whistleblowing, MNCs and Peace*, 35 Vanderbilt J. of Transnat'l L. 457, 461 (2002).
- Nathan Hurst, *Corporate Ethics, Governance and Social Responsibility: Comparing European Business Practices to Those in the United States*, The Markkula Center for Applied Ethics, Santa Clara University, Spring 2004, p. 6, available at *www.scu.edu/ethics/publications/submitted/hurst/comparitive_study.pdf*.
- R. Vaughn, T. Devine, and K. Henderson, *The Whistleblower Statute Prepared for the Organization of American States and the Global Legal Revolution Protecting Whistleblowers*, 35 Geo. Wash. Int'l L. Rev. 857, 861 (2003).

(continued from page 38)

approach your company's international compliance procedures? You should start by closely reviewing recent compliance-related developments in those countries where your company either does business or contemplates doing business in the near future.

Once you have digested that information, you should outline the international trends that you have identified in ethics and compliance programs. You should highlight how these growing expectations are already satisfied by your company's program. To the extent your program doesn't fully meet these emerging standards, you should determine how to revise the program in the near future. You will also need to be prepared for foreseeable future developments that might create new challenges for the company's compliance rules.

With all that done, you'll be on top of the international compliance issues that face your company, including the issues that arise under the Sarbanes-Oxley Act and the revised Guidelines. Finally, you'll be able to sit back and relax, and enjoy your view of the global compliance landscape.

Notes

1. *Ethical concerns and reputation risk management,* Arthur Andersen and London Business School, 1999, p. 12, available at *www.globalethics.org/andersonrpt.pdf*.
2. *Id.*
3. Paul Gompers, Joy Ishii, and Andrew Metrick, Corporate Governance and Equity Prices, Quarterly J. of Econ. 118(1) (Feb. 2003): 107, available at *http://finance.wharton.upenn.edu/%7emetrick/gov.pdf*.

THE FINANCIAL SERVICES ROUNDTABLE
Impacting Policy. Impacting People.

The Compliance Function in Diversified Financial Institutions

Harmonizing the Regulatory Environment for Financial Services Firms

CORNELIUS HURLEY
JOHN A. BECCIA, III

BU LAW Morin Center

JULY 2007
SPONSORED BY THE ANTHONY T. CLUFF RESEARCH FUND OF THE FINANCIAL SERVICES ROUNDTABLE

Table of Contents

Message from Cluff Fund Chairman Patrick B. Frost, Chairman, Cullen/Frost

On behalf of the Anthony T. Cluff Research Fund of The Financial Services Roundtable, I am pleased to present this study, *The Compliance Function in Diversified Financial Institutions: Harmonizing the Regulatory Environment for Financial Services Firms.*

The events of September 11, 2001, the collapse of WorldCom and Enron, and several trading scandals have placed legislators and regulators in a reactionary mode. In their efforts to keep Americans safe and the economy sound, government officials have enacted laws and regulations that often are unclear. In addition, the enforcement of these guidelines has at times been inconsistent and without coordination among key federal and state agencies.

As a result of this uncertain regulatory environment, financial services firms have struggled with how to structure compliance functions within their organizations. These efforts have been costly in terms of time and resources. Some have posited that the current regulatory structure has negatively impacted the United States' competitive position in the world marketplace.

It is clear that laws and regulations are necessary to ensure the safety and soundness of financial services institutions and promote the integrity of the U.S. financial markets. The regulatory structure in the U.S. has long been heralded as one of the premier systems in the world. However, because of the vast number of new regulations and the rapidly changing regulatory and business environment, lawmakers, regulators, and industry officials should continually review the effectiveness of the system.

To facilitate this process, the authors of this study make a number of recommendations in areas where positive changes can be made. It is our hope that these recommendations will lead to the harmonization of missions of regulators, a review of enforcement practices at both the state and federal level, bridging the gap between regulator and industry approaches to compliance, and a commitment by financial institutions to promote ethics and integrity beyond what is legally required.

On behalf of the Trustees, I thank the authors of this study, Cornelius Hurley, of the Morin Center for Banking and Financial Law, Boston University School of Law, and John A. Beccia, III, of Boston Private Financial Holdings, Inc. I also heartily thank the many regulators and industry representatives who so generously donated their time and expertise for this report. Without their help, this study would not have been possible.

Should you have any questions about this study, please do not hesitate to contact Richard M. Whiting, General Counsel and Executive Director for the Roundtable, at 202.289.4322.

Sincerely,

Patrick B. Frost
Chairman, Anthony T. Cluff Fund
Chairman, Cullen/Frost Bankers, Inc.

The Anthony T. Cluff Research Fund designs, approves, and funds research on issues affecting the financial services industry and related public policy. The results of these studies advance the policies of the Roundtable, and inform and educate opinion leaders and policymakers.

Collaborators

John A. Beccia, III
Boston Private Financial Holdings, Inc.

Michael Bleier
Reed Smith LLP

Stephen Cesso
Computershare, Ltd.

Thomas Cimeno

Tamar Frankel
Boston University School of Law

Cornelius Hurley
Morin Center for Banking and Financial Law
Boston University School of Law

Paul L. Lee
Debevoise & Plimpton LLP

Gary M. Welsh
PricewaterhouseCoopers

Student and Professional Contributors

Greg Dekermenjian

Jonathan Feiler

Samson Huang

Austin Kim

Martin Lacdao
Morin Center for Banking and Financial Law, Boston University School of Law

Jeremy McLeod

Kevin E. Thorn
Caplan and Drysdale

Jon Trotter

Joseph V. Zujkowski
Annual Review of Banking and Financial Law, Boston University School of Law

Executive Summary

Background

Financial services institutions in the United States are subject to a multi-layered regulatory regime. There have been several factors in the last few years that have led to more stringent regulations and supervisory scrutiny for financial services firms. In particular, new laws on anti-money laundering after the events of September 11, 2001; new financial accounting/corporate governance rules following the Enron and WorldCom failures; and late trading/market timing and other scandals. Regulatory changes have been underscored by significant enforcement actions brought by the federal financial regulators; the Securities Exchange Commission (SEC), the Department of Justice (DOJ), and state attorneys general which resulted in large monetary fines and penalties.

The legal, reputational, and financial risks associated with the current regulatory and enforcement environment are negatively impacting financial services institutions. On a larger scale, some have argued that the current regulatory environment is too severe and is damaging U.S. financial institutions' competitive position in the world marketplace. On a more practical scale, business planning, acquisition strategy, and daily operations are being affected by additional regulatory scrutiny. It is difficult for compliance functions to adapt to this rapidly changing environment, unclear standards and regulatory expectations, and a lack of coordination among regulators, which often results in supervisory overlap or duplication. These challenges are magnified in larger, more complex financial institutions.

Compliance Functions in Diversified Financial Institutions

"Compliance" as a mission critical function is a relatively recent phenomenon. In diversified financial services institutions, entire departments dedicated to compliance have been created in response to the current regulatory and enforcement environment. Financial services institutions are challenged by increasing compliance costs and the heightened risks of noncompliance, including legal and reputational risk.

The basic goal of today's compliance department is to develop policies and procedures and other compliance program elements needed to conform to relevant laws and regulations.

In recent years, financial services regulators, self-regulatory organizations (SROs), and various international supervisory bodies have issued guidelines on how the compliance function should be structured. These guidelines have not always been consistent. As a result, the financial services industry has developed its own best practices on how compliance should operate within diversified financial services institutions. Compliance departments have become more formal and tend to operate as an independent function that reviews risks on an enterprise-wide basis. As the risks of non-compliance have increased, the position of the compliance officer has gained status, and is now critical to the success of the firm.

The basic goal of today's compliance department is to develop policies and procedures and other compliance program elements needed to conform to relevant laws and regulations. This goal is accomplished in many ways. The compliance function must oversee, monitor, test, and validate key aspects of a financial institution's business and compliance program. Senior management and the board of directors must oversee these efforts and assess the effectiveness of the compliance program. Adequate resources, including people and systems, must be allocated for compliance to achieve its goals. Compliance staff must possess the necessary expertise. Due to

the rapidly changing environment, the compliance function must stay abreast of developments while being proactive and anticipating future risks. One way to be proactive is to build a strong rapport with regulators and communicate with regulatory officials on an ongoing basis. Assuming all compliance functions are implemented effectively, institutions still run significant compliance risks due to disparate approaches and expectations of different financial regulators toward compliance. Until this regulatory structure is harmonized, any strides industry makes to improve compliance structures may be inadequate. The recommendations in this report are intended to promote such regulatory harmony.

Summary of Recommendations

Following are several actions that may be taken to address the current regulatory challenges and bolster compliance functions within diversified financial services institutions.

1. Harmonize the Missions of All Financial Services Regulators

Strong regulatory oversight and transparency are critical for the success of financial services institutions and the capital markets in general. However, it is essential to strike the correct balance to ensure that regulations are effective and achieve their stated purposes. Duplicative and unclear regulatory guidance can place a strain on the compliance function within diversified financial services institutions. Therefore, it is important that government officials continue to review the U.S. regulatory structure for possible enhancements.

- To the extent possible, the government should harmonize the missions of the multiple state and federal financial services regulators. This includes establishing high level principles which operate as a framework for regulatory supervision, and provide institutions the flexibility to build effective compliance programs instead of having to take a "check the box" approach to compliance.
- The membership of the Federal Financial Institutions Examinations Council (FFIEC), which currently includes the federal bank and credit union regulatory agencies and a State Liaison Committee (composed of five representatives of state supervisory agencies) should be expanded to include the SEC, SROs, the National Association of Insurance Commissioners (NAIC), and other state regulators. The FFIEC should also be given a more direct role in ensuring consistency among all regulators; e.g., it would be charged with reconciling conflicting regulatory actions and establishing uniform national standards where appropriate.
- The President's Working Group on Financial Markets (PWG)[1] should oversee and work with groups such as the FFIEC to help establish high level principles and harmonize the actions of financial regulators.
- More meaningful cost-benefit analysis by legislators and regulators on current and proposed regulations could ensure they are effective and serving their intended purpose.
- Detailed prescriptive rule-making should supplant principles only when needed for clarity or to avoid other risks.
- Congress should consider moving toward a more productive form of federalism which properly balances state and federal interests. Uniform national standards and preemption of state laws should be considered in certain areas in order to allow financial services institutions to operate on an interstate basis without having to comply with multiple, conflicting laws. Any national standard enacted should ensure that consumers are adequately protected.
- Congress should enact an optional federal charter for the insurance industry to give insurance companies the ability to operate more efficiently in all fifty states.

[1] The PWG was created by Executive Order 12631, signed on March 18, 1988 by U.S. President Ronald Reagan. The Working Group includes the Treasury Secretary (Chair), the Chairman of the SEC, the Chairman of the Commodities Futures Trading Commission, and the Chairman of the Board of Governors of the Federal Reserve System, with the Comptroller of the Currency and the Director of Office of Thrift Supervision as ex-officio members.

2. Review Enforcement Practices of State and Federal Authorities

In this regulatory environment, legal risks are extreme. It is important that financial institutions have proper governance and compliance controls in place. It is also important that government agencies conducting investigations and enforcing regulations be transparent in their actions and exercise their authority discretely, cognizant of the impact of their actions on the U.S. capital markets.

- The SEC should consider enhancing nascent efforts to move toward a more prudential approach to regulation and supervision. Prudential regulation has been successful in fostering ongoing communications between banking regulators and their regulated institutions. A prudential approach would require the SEC to focus more resources on examinations relative to enforcement actions.
- Rules should be made through a process of notice and comment and not through enforcement actions. Without losing sight of their investor/consumer protection mandates and their ability to uphold the laws, government officials should cooperate with financial services institutions in a proactive manner rather than waiting to bring an enforcement action.
- The attorney-client privilege must be protected. Financial services institutions have been critical of practices by the DOJ and the SEC, including pressure to waive the attorney-client privilege in the course of investigations. Privileged information shared with the SEC and DOJ should be adequately protected as is the case for information shared with bank examiners. This examination privilege should be extended to the SEC and safe harbors should be considered for other privileged information.
- Federal and state agencies should coordinate investigations and enforcement actions. This includes sharing information and limiting duplicate actions against financial services institutions.

For the most part, state and federal agencies do not have an effective forum to formally coordinate their efforts in relation to their regulated entities.

3. Bridge the Gaps between Regulator and Industry Approach toward Regulation and Compliance

Financial services institutions are subject to myriad regulators and guidelines. As institutions become more complex, regulatory scrutiny increases. For the most part, state and federal agencies do not have an effective forum to formally coordinate their efforts in relation to their regulated entities. This lack of coordination has led to different perspectives on regulations and major hurdles to the effective functioning of compliance departments. Lack of clarity in regulatory guidance has created a divide between regulatory expectations and how compliance departments are operating.

There is a need for greater coordination among U.S. financial services regulators, in particular relating to agencies that supervise large, complex financial services firms on a consolidated basis. Regulators should adopt additional guidance in specific areas to provide clarity on compliance. Some specific areas where more regulatory guidance is necessary include:

1. The role of board of directors in approving policies and procedures
2. The structure of the compliance function
3. The level and type of testing required
4. Proper methods to assess the compliance function
5. Regulators' risk-based supervisory approach.

4. Institutions Should Promote Ethics and Integrity Beyond the Law

Much has been made of the need for "tone at the top" when it comes to inculcating an ethical culture within a financial services firm. The current regulatory environment, however, tends to promote a quantitative versus a qualitative approach to compliance. Regulators should give explicit encouragement to management actions designed to promote a culture of heightened ethical standards.

For their part, financial services institutions have a duty to act as good corporate citizens beyond the law and apply common sense in determining whether conduct or a practice is appropriate. If institutions maintain comprehensive programs and an ethical culture, corporate misconduct should rarely occur.

I. Background

A. Goals and Objectives of the Study

The primary objective of this study is to review the state of compliance within diversified financial services institutions and assess the degree of harmonization between regulators' expectations and industry practices.

This paper will:

- Review the current regulatory environment and determine what external factors have shaped today's compliance departments
- Analyze regulatory guidance that has addressed these subjects, including the emerging concept of enterprise risk management (ERM) and managing compliance risk
- Review how the industry has adapted to regulators' expectations, including creating best practices for the compliance function
- Discuss the elements of an effective compliance program and will theorize on what the future holds for the compliance function

Finally, the recommendations will improve the effectiveness of the compliance function within diversified financial services institutions and allow companies to be more competitive in the global marketplace while continuing to provide innovative products and services to consumers

B. Methodology

The contributors to this study consist of former government officials, industry experts, academicians, and practicing attorneys. In addition to the considerable background of these individuals, interviews were conducted with policymakers at the regulatory agencies and with chief compliance officers at many diversified firms and institutions. Assisting in these interviews were several staff members of the Annual Review of Banking and Financial Law at Boston University's Morin Center.

II. Regulatory Environment

A. Background of U.S. Regulatory Structure for Financial Services Institutions

The financial services industry plays a crucial role in the U.S. economy. In 2005, assets held by the financial services sector totaled almost $49 trillion[2]. Between 2000 and 2005, the financial sector averaged 5.4 percent of the total U.S. private industry employment.[3]

The U.S. financial system and markets are by far the broadest, deepest, and most liquid of any in the world. One of the primary reasons for this condition is the high regard for the rule of law and the efficacy of regulation and supervision. Foreign companies often choose to do business in the U.S. because of the transparency and integrity of the U.S. regulatory structure. In order to achieve this level of integrity, financial services institutions in the United States are subject to a complex, layered regulatory regime.

Banks are regulated by four federal banking agencies; the Board of Governors of the Federal Reserve System (Federal Reserve), the Office of Thrift Supervision (OTS), Office of Comptroller of the Currency (OCC) and the Federal Deposit Insurance Corporation (FDIC), as well as state banking departments. Securities firms are subject to regulation by the U.S.

Securities and Exchange Commission (SEC), self regulatory organizations (SROs) such as the NASD and New York Stock Exchange, as well as state securities regulators. In addition, the Federal Reserve, the OTS and the SEC supervise firms on a consolidated basis at the holding company level (in the case of certain large institutions).

Insurance firms are supervised by state insurance officials in fifty states.

The actions of financial services institutions are also subject to review by the U.S. Department of Justice (DOJ) and state attorneys general.

The financial services industry, and its regulatory structure, changed dramatically with the passage of the Gramm-Leach-Bliley Act of 1999 (GLBA), which permitted a much greater degree of convergence among banking, insurance, and securities activities. As a result, diversified financial services institutions owned by one set of shareholders have the ability to offer a variety of financial products to the consumer via one central source. However, GLBA encouraged innovation, competition, and global expansion as well as significant merger and acquisition activity within the industry as new types of financial services institutions developed. GLBA established a system of functional regulation that requires each financial regulator to defer to the regulator primarily responsible for supervising specific activities of regulated entities. Thus, even with the passage of GLBA, diversified financial services institutions remain subject to supervision by multiple regulators.

Regulatory change and regulatory reform in the U.S. has traditionally been reactive in nature and impacted by critical events in history. For example, the National Bank Act creating the Office of the Comptroller of the Currency (OCC) was enacted in 1864 to help finance the Civil War; the Federal Reserve was created in 1913 to act as a central bank as a result of the financial collapse known as the Panic of 1907; and the nation's first securities laws, the Securities Act of 1933 and the Securities Exchange Act of 1934 were enacted to restore confidence in the markets during the Great Depression. Similarly, in 1989, on the heels of the savings and loan crisis in which over 1,000 thrifts failed at a cost of $150 billion, the Office of Thrift Supervision (OTS) was established by Congress as a bureau of the Department of the Treasury as part of the Financial Institutions Reform, Recovery and Enforcement Act of 1989.

[2] Ins. Info. Inst. and The Fin. Services Roundtable, *2007 Financial Services Fact Book*, p. 5 (2007).
[3] Id.

More recently, and following the passage of GLBA in 1999, there occurred a "perfect storm" of events, including the dot-com bust, September 11, 2001, and a series of corporate scandals, all of which prompted re-configuration of the regulatory environment and compliance culture. These events produced legislation such as Sarbanes Oxley and the USA Patriot Act, as well as other changes in practices within the financial services industry. Financial services institutions are now faced with additional regulatory risks and are subject to oversight by a variety of regulators with a diverse set of regulatory missions which they carry out with varying degrees of zeal. In the wings are new regulatory capital standards for financial institutions (Basel II and IA). The marriage of risk based capital standards with compliance risk has forged a major shift in the way firms view compliance. In essence, compliance has gone from being an *ex post* function to an *ex ante* one.

B. How Regulations, Litigation and Enforcement Actions and Preemption Have Shaped Compliance

Significant Regulations

Various external factors have led to the current regulatory environment. The war on terror, massive fraudulent schemes leading to unprecedented bankruptcies, improper and illegal accounting and trading scandals, along with other corrupt practices have contributed to a hyper-conscious compliance climate. These factors have placed additional regulatory emphasis on corporate governance and the need for a strong centralized compliance function within an organization.

Some of the most significant changes over the last five years have taken place in relation to anti-money laundering (AML) efforts. The tragic events of September 11, 2001 underscored the need for additional protections against terrorist financing and money laundering. In the U.S., Congress reacted

Litigation and enforcement actions have resulted in new regulations and laws in other areas.

swiftly by passing the USA Patriot Act of 2001. In addition, organizations around the world, such as Financial Action Task Force (FATF), The Wolfsberg Group, and the Basel Committee on Banking Supervision (Basel Committee), either updated or created new guidelines in this area. Among some of the common themes in these guidelines was the need to create a strong compliance program that included written policies and procedures, risk assessments, monitoring and oversight, board reporting, training, and a comprehensive review by internal audit or another independent party. These principles proposed that financial services institutions appoint a centralized compliance officer to oversee its anti-money laundering program. These AML compliance guidelines have resulted in enhanced scrutiny during the course of regulatory examinations. Several high profile enforcement actions and settlements have underscored the need for strict controls in relation to AML efforts.

The financial accounting scandals associated with Enron, WorldCom, and others prompted Congress to pass the Sarbanes-Oxley Act of 2002 (Sarbanes-Oxley) which placed additional emphasis on corporate governance and controls within corporations. Sarbanes-Oxley changed the accounting practices and financial reporting of public companies and introduced a new regulator, the Public Company Accounting Oversight Board (PCAOB), for auditing firms. The most challenging provision for institutions is Section 404 which requires management to assess the effectiveness of a company's internal controls and requires auditors to attest to the company's

assessment. This provision and the regulatory risks associated with it have prompted organizations' compliance and risk management departments to closely review internal controls and further assess risks on an enterprise-wide basis. Companies continue to struggle with ongoing costs and interpretations of the law. The PCAOB and SEC have attempted to mitigate the impact of Section 404 by their recent changes to Auditing Standard No. 2 and the creation of advisory committees to conduct ongoing reviews of rules. It remains to be seen whether further relief is needed.

Litigation and Enforcement Actions

Enforcement actions have impacted corporate governance and compliance within diversified financial institutions. This is particularly evident in the securities and insurance industries where enforcement actions have brought reforms to certain practices. From 1999 to 2007, New York State Attorney General Eliot Spitzer negotiated more than $7 billion in fines, restitutions, or disgorgements, and another $671 million of pledges to reduce customer fees.[4] Most notably, 14 actions were brought against securities firms related to late trading and market timing, cases against analysts for biased research and conflicts of interest, and charges against insurance companies for bid rigging and fraudulent practices. The SEC brought similar actions during this period. Between 2001 and 2005, the SEC brought 3,604 enforcement actions against securities firms. In 2006, the SEC brought another 574 actions. Although this was a decline from previous years, the SEC completed two of the largest settlements in its history in 2006, which initiated the departure of senior executives and an array of criminal charges.[5]

Litigation and enforcement actions have resulted in new regulations and laws in other areas. One example is the impact of court decisions relating to the retention of documents and other records. In *Zubulake v. UBS Warburg LLC*, 2004 US Dist Lexis 13574 (SDNY), there was a $29 million award ($20 million punitive damages) when a court determined that an employer had willfully deleted emails relevant to the litigation despite contrary court orders. In 2002, the accounting firm of Arthur Andersen was convicted of obstruction of justice for shredding documents related to its audit of Enron.[6] The penalties in both cases were a result of having destroyed documents. The real issue was not that the documents were unavailable, but that they were not destroyed in accordance with an established records management program. For this reason, a negative inference was made against these organizations. As a result of these cases, new compliance programs have been adopted in organizations in relation to record retention. In addition, federal rules have been adopted, such as the new electronic discovery rules which took effect on December 1, 2006.[7] The e-discovery rules remove the ambiguity surrounding electronic records. These rules cover the loss of potential evidence in the course of routine records disposal. Rule 37(f) is a "safe harbor" which states that it is generally acceptable to destroy discoverable evidence if it was done in good faith as part of a record retention program. In this new regulatory environment, there is more scrutiny and accountability for organizations. Records must be properly documented and retained in case questions arise in relation to transactions and company practices.

With the new laws and rules has come a new attitude by enforcement agencies. One example of the new enforcement approach is the treatment of the attorney-client privilege during the course of government investigations. In January 2003, then-Deputy Attorney General Larry Thompson issued a memorandum to U.S. Department of Justice (DOJ) officials (Thompson Memorandum) outlining guidelines for the federal prosecution of business organizations.[8] The Thompson Memorandum set forth nine factors that prosecutors should consider in deciding whether to charge a company and to gauge the level of cooperation provided by business organizations. The failure to waive the attorney-client privilege was one such charging factor.

Some in the industry have argued that waiver of attorney-client privilege is more of a requirement than a factor in determining the level of cooperation in these investigations. In December 2006, the DOJ issued the McNulty Memorandum, which attempted to clarify the circumstances in which prosecutors can seek a waiver. Although the issuance of the McNulty Memorandum was a positive step in protecting attorney-client privilege, there is still significant liability for corporations that are subject to government investigations.

The SEC also has a history of considering the waiver of attorney-client privilege when determining penalties against financial institutions. In October 2001, the SEC released a report explaining why it was not filing charges against the Seaboard Corporation after investigating the company for accounting irregularities.[9] The "Seaboard Report" detailed factors the SEC considers in determining whether, and to what extent, it grants leniency to investigated companies. These so-called "Seaboard" factors include the level of cooperation by institutions and whether institutions waived their privilege.

The industry has criticized the SEC and DOJ because some believe that waiver of attorney-client privilege is forced in order to obtain credit for cooperation in the course of an investigation. The industry is concerned that requiring a waiver may have a chilling effect on communications between management, boards of directors, and their attorneys because of the lingering question about what conversations and work-product is protected.[10] The likelihood that internal communications are not protected can also act as a disincentive for financial institutions to conduct internal investigations. Additional guidance, along with possible safe harbors for sharing of information, is needed.

The general approach to enforcement actions and differences in enforcement attitudes and the way investigations are conducted have impacted compliance departments. In the 2003 SEC Annual Report, then SEC Director of Enforcement Stephen Cutler stated, "These days, the concept of effective enforcement necessarily includes 'seeing around the corner.' What that means to us is identifying trends, practices, and risks within our capital markets that could be exploited to the detriment of investors. Ideally, if we are able to spot these issues in their infancy, we can prevent them from growing into full-fledged, confidence-eroding scandals." Enforcement actions have further defined the expectations of regulators. Regulatory agencies have become more proactive which means compliance must also adapt and do the same. As the industry responds to the changes in the regulatory environment, some financial institutions have been slower to put the proper controls in place and have faced high fines and reputational damages. For the most part, the financial services industry has responded by dedicating substantial resources to compliance and by creating comprehensive programs and systems that monitor and place controls on these practices.

Preemption and Uniform National Standards

The debate over states' rights and national powers has been a long-standing one in the U.S. financial services industry. Both state and federal regulators have a vested interest in retaining regulatory authority over financial services institutions and have acted accordingly. The currently besieged dual banking system offering state and federal charter options exemplifies the ongoing federalism debate. More recently, new regulations by federal regulators preempting state laws and activism within the states to enact their own rules to fill regulatory voids, especially with regard to customer privacy and customer protection, have once again heightened the discourse and impacted compliance functions within diversified financial services institutions.

---

[4] *Spitzer Effect: Tabulating His Prosecutions,* American Banker, Jan. 10, 2007, ***available at*** http://ww.americanbanker.com/article_search.html?articlequeryid=446310666&hitnum=12

[5] Sarah Johnson, *SEC Enforcement Declines 8.9 Percent*", CFO.com, (November 6, 2006), available at http://www.cfo.com/article.cfm/8127167?f=search.

[6] *United States v. Arthur Andersen,* 2002 Extra LEXIS 437 (S.D. Tex. June 15, 2002) (No. H-02-121)

[7] Amendments to the Federal Rules of Civil Procedure Addressing Discovery of Electronically Stored Information. Fed. R. Civ. P. amendments to Rules 16(b), 26(a), 26(b)(2), 26(b)(5), 26(f), 33, 34(a), 34(b), 37(f) and 45, as well as Form 35 (effective December 1, 2006) see http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf for details.

[8] Memorandum by Larry D. Thompson, Deputy Attorney General, U.S. Department of Justice, to Heads of Department Components, United States Attorneys, on Principles of Federal Prosecution of Business Organizations (Jan. 20, 2003)

[9] See Report of Investigation Pursuant to Section 2(a) of the Securities, Exchange Act of 1934 and Commission Release No. 34-44969, (Oct. 23, 2001); Statement on the Relationship of Cooperation to Agency Enforcement Decisions, SEC Release Nos. 34-44969 and. AAER-1470 (October. 23, 2001) (the "Seaboard Report").

[10] Statement of John A. Beccia III on behalf of The Financial Services Roundtable before the American Bar Association's Task Force on the Attorney-Client Privilege, New York, NY (April 2005). Hearing information, hearing information available at http://www.abanet.org/buslaw/attorneyclient/publichearing20050421/schedule.shtml 2004).

In 2004, the OCC issued rulings that preempted various state laws (i.e. those related to parts 7 (deposit-taking) and 34 (real estate lending) of OCC regulations) in relation to national banks.[11] These preemptions included restrictions on the visitorial rights by state attorneys general over national banks and their operating subsidiaries. National banks have argued that this type of preemption makes it easier for them to operate in multiple states rather than being forced to comply with the laws of multiple states and being subject to review by different state attorneys general.

The argument for many institutions is that uniform national standards allow them to operate more efficiently. In the absence of uniform national standards, the main issue for compliance is how to manage institutions that provide services in multiple states and are subject to numerous different rules and regulations. The opponents of preemption argue that allowing states to have jurisdiction over financial institutions creates more checks and balances and provides additional protection for consumers.

There are many examples demonstrating how the lack of national standards challenges compliance departments. One relates to consumer privacy laws and, in particular, data breach notification requirements. Although there are several bills pending in Congress that would create a national standard, financial institutions must comply with more than 30 state data breach notification laws with varying degrees of requirements and complexities. Second, insurance companies are forced to comply with fifty different state laws and licensing requirements. Despite model laws, regulations and guidelines issued by the National Association of Insurance Commissioners (NAIC), insurance compliance professionals must build systems and controls to track all existing and proposed laws, legislation, regulations, and opinions of insurance commissioners and attorneys general for each state where its company does business. Congress has considered creating an optional federal charter for the insurance industry to address these challenges.

C. Impact of Regulations on Capital Markets, Business Planning, and Compliance

Recently, several high profile groups and bipartisan commissions have reviewed the regulatory environment.[12] The reports produced by these groups stress the importance of the U.S. capital markets to the American economy. In particular, the U.S. financial services industry's GDP is well over $1 trillion and is over 8 percent of the U.S. GDP.[13] More Americans are investing in the markets. The mutual fund industry alone currently holds over $11 trillion in assets.[14] Despite being widely regarded as the most transparent and well regulated market in the world, these groups suggest that the U.S. financial services industry's position in the world markets has been compromised due to an inefficient regulatory structure, regulatory enforcement actions, and civil litigation. The papers also criticize what is referred to as a lack of a strategic vision and unified purpose for the financial services industry.

[11] Office of the Comptroller of the Currency; Bank Activities and Operations: Real Estate Lending and Appraisals, Fed. Reg., Vol. 69, No. 8, p. 1904-1917 (January 13,

[12] See Reports and Recommendations of the Commission on the Regulation of U.S. Capital Markets in the 21st Century (March 2007) http://www.capitalmarketscommission.com/portal/capmarkets/default.htm; Interim Report of the Committee on Capital Markets Regulation (December 5, 2006), http://www.capmktsreg.org/index.html; and the report on Sustaining New York and the U.S.'s Global Financial. Services Leadership issued by Mayor Michael Bloomberg and Senator Charles Schumer, http://www.nyc.gov/html/om/pdf/ny_report_final.pdf.

[13] Interim Report of the Committee on Capital Markets Regulation, supra note 12 at p. 23.

[14] Source: Investment Company Institute, http://www.icifactbook.org/fb_sec1.html.

More regulation and more compliance requirements have affected the competitiveness of U.S. financial markets. These recent studies point with alarm at an array of statistics indicating an erosion of U.S. dominance over the global capital markets. We would point out, however, that the maturation of foreign markets is also a contributing factor. Moreover, it is encouraging that many of the governance practices of the U.S., including key elements of Sarbanes-Oxley, are being emulated in other developed economies. Nevertheless, it is apparent that the strain from a regulatory, litigation, and compliance risk perspective has slowed potential growth. Boards of directors and senior management are often overwhelmed by compliance issues, so business decisions are deferred. For these trends to change, businesses need to get more clarity from regulators on compliance rules and procedures.

Along with the sheer volume of rules and regulations, compliance departments must cope with inconsistent interpretations and overlapping supervision.

Impact of Regulations on Compliance

In the current environment, more focus has been placed on corporate governance and compliance. Increasingly, CEOs are engaged on compliance issues and are in constant contact with chief compliance officers on key risk areas. Boards and audit committees are continually updated on these risks. Compliance risks are managed across the organization and are part of all business decisions and discussions. Compliance departments regularly track and monitor developments in this quick moving environment. Institutions' policies, procedures, and controls are continually adjusted as regulations change. Institutions are more proactive and anticipate future risks. Along with the sheer volume of rules and regulations, compliance departments must cope with inconsistent interpretations and overlapping supervision. Compliance departments must also account for regulatory guidance that comes from outside the formal rulemaking process. For example, firms regulated by the SEC are inclined to review speeches by Commissioners and recent enforcement actions since these forms of "rulemaking" are given great weight and authority by SEC examiners and enforcement officials.

D. Attitudes toward Regulation, Supervision, and Enforcement

Several themes were evident when speaking to regulators and industry representatives in the course of preparing this study. Although there appears to be some common ground, there are many areas where regulatory officials believe the industry needs to improve or where industry believes additional regulatory guidance and changes need to be made.

Regulatory Environment

Some of the compliance executives interviewed indicated that a review of current regulatory requirements is necessary on several fronts. First of all, some rules are antiquated and do not align with changes in technology or current practices. For example, the definition of "local community" under the Community Reinvestment Act of 1977 (CRA) does not account for the national scope of business operations today. Federal Reserve Chairman Ben S. Bernanke has stated that "for some institutions the concept of local community is no longer as clear as it was when the CRA was enacted. Today, some institutions are not identified with a particular community but are regional or national in scope, which inevitably makes the definition of the relevant assessment areas somewhat difficult".[15] Second, industry representatives believe regulators have not attempted to perform an adequate cost-benefit analysis to determine the effectiveness of current or proposed regulations. Third, compliance executives expressed concern over the reactionary nature of regulations and the lack of collaboration with the industry in the rulemaking process. In particular, one compliance officer stated that some agencies do not seek meaningful input from the industry prior to proposing a rule. It often appears that regulators prefer to avoid the rulemaking process except when clearly required, relying instead on more subjective

[15] Federal Reserve Chairman Ben S. Bernanke's remarks at the Community Affairs Research Conference, Washington, D.C. (March 30, 2007).

policy statements with limited or no opportunity for public input.

Supervision and Examinations

Most compliance officers and other industry executives interviewed believe there is a need for more coordination and communication among regulators. One compliance executive stated his firm is subject to 45 regulators. In 2006, the firm had 156 regulatory examinations, not including other general inquiries and investigations. This represented a 40% increase over the previous year. The compliance executive noted that there was no effort to streamline or coordinate these reviews. In addition, there are lingering questions on how to interpret rules. Compliance executives noted that different regulators seem to interpret the same regulations in a dissimilar fashion.

One banking official noted that its regulatory agency focuses on risk-based examinations and supervision. In many cases where regulatory sanctions were issued against financial institutions, it was due to the absence of an effective compliance program, not because of an individual occurrence or violation of the law. According to this banking official, an organization's compliance program is reviewed in its entirety and how it operates across the organization. The official indicates that more guidance would provide clarity on this approach.

Enforcement Practices

Industry officials are concerned with the enforcement attitudes of state and federal regulators and prosecutors. There is a belief that the SEC is overly aggressive in investigations and enforcement actions and that a more prudential approach would benefit the industry and investors. Some in the industry believe that the SEC is too broad in its enforcement actions. Industry officials argue that Rule 10b-5, the rule that prohibits any act or omission resulting in fraud or deceit in connection with the purchase or sale of any security including insider trading,[16] is being interpreted too broadly and being used as a "catch all" for actions brought by the SEC and class action lawyers. Industry representatives interviewed also stated that there is a lingering problem with companies being forced to waive attorney-client privilege during the course of investigations.

Industry officials believe there is a lack of coordination between government authorities. And, there is a lack of clarity on compliance standards, which sometimes leads to sanctions. In particular, the SEC's lack of transparency in rulemaking and regulating through enforcement makes it difficult for financial institutions to put proper controls in place.

Regulators interviewed stated that they are adequately fulfilling their obligations under the law, particularly the SEC, which is charged with investor protection. Regulators argue that the ongoing trend of corporate scandals and abusive business practices demonstrates the need for action. Some regulators have noted that the industry's best deterrence for aggressive enforcement is proper compliance. Regulatory officials note that the recent reduction in significant enforcement actions or formal sanctions (especially in the banking industry) in the last year is evidence that financial institutions have bolstered their compliance programs.

Banking regulators have been adamant that their enforcement actions should not be used as guidance for compliance. This differs from the SEC, which often looks at the precedent created by previous actions which in turn result in de facto rules and regulations in relation to certain practices.

One senior official with approximately thirty years as a regulator for a self- regulatory authority in the securities industry commented on the escalation of issues and investigations. This regulator's observation was that regulators in the securities area have been very aggressive in recent years with large fines. As a result, self reporting in the securities industry is declining.

For example, the market timing scandals in the mutual fund industry should have been uncovered via compliance self-reporting as evidenced by the wide-spread nature of the abuses. In fact, the first market timing case arose from an aggrieved employee who reported the violations to a local SEC office. The insurance brokerage industry's "contingent commissions" scandal offers another example of the failure to self-regulate.

Compared to the banking industry, the securities regulators are more aggressive and impose higher fines. The banking industry seems to resolve more compliance problems in-house. The banking regulators have a more collaborative relationship with the banks that they regulate. From time to time, this relationship can become too collaborative, as may have been the case in the Riggs matter. The SEC's aggressive posture, in contrast, deters self-reporting for fear of triggering an enforcement action.

As Treasury Secretary Henry M. Paulson recently stated, "when it comes to regulation, balance is key."

Self-examination by firms is an important tool to ensure compliance during regulatory examinations. In the banking context, self-examination and self-reporting are encouraged by the knowledge that all books and records are available to bank examiners. In the securities context, the access of examiners to the books and records of regulated firms is more limited and often adversarial. This chills the incentive to perform self-testing. Firms do not want to provide SEC with roadmaps for problems.

In some instances, regulators admit that more coordination needs to take place in the course of investigations and enforcement actions; however, regulators also point to successful joint actions taken by multiple agencies, including the DOJ, in relation to money laundering violations, as a model on how the agencies should collaborate. A recent report by the Government Accountability Office (GAO) suggests that the U.S. regulatory system would benefit from collaboration between consolidated and primary bank and functional supervisors in the oversight of the largest, most complex firms and among consolidated supervisors themselves. [17]

Other Compliance Challenges in the Current Environment

Regulators and industry officials agree that updating compliance programs on a continuous basis, and in relation to external events, is difficult. According to regulators, it is a challenge to keep pace in the areas of operations, controls, and training. There is also concern that regulated financial institutions have to compete with unregulated or less regulated entities, such as hedge funds or private equity firms that do not have to comply with regulatory schemes designed for institutions dealing with the general public. The effects of more capital moving to less regulated private markets and the potential impact on the public markets and the financing of the U.S. economy have been queried but not yet studied.

In an attempt to address these concerns, the four federal bank regulators and the SEC recently issued guidance on complex structured finance transactions which outlines best practices for underwriting complex structured finance deals that could pose heightened risks.[18] The guidelines describe the types of internal controls and risk management procedures that should help financial institutions identify and manage legal risks associated with these transactions. These guidelines, although a laudable example of interagency coordination, serve to highlight the divergence of potential consequences which may befall an institution that ignores the guidelines.

Regulators and compliance executives agreed that it is even more challenging to predict future events that may impact compliance. Regulators have made statements that compliance functions must be proactive and perform scenario analysis that will anticipate risks. However, the methodologies and processes to do so are unclear.

[16] Securities Exchange Act of 1934, 48 Stat. 881 (June 6, 1934), codified at 15 U.S.C. § 78a (1934).

[17] Govt. Acct. Office (GAO) Report, Agencies Engaged in Consolidated Supervision Can Strengthen Performance Measurement and Collaboration (March 2007) at p. 12. www.gao.gov/highlights/d07154high.pdf.

[18] Interagency Statement on Sound Practices Concerning Elevated Risk Complex Structured Finance Transactions, Federal Register, Volume 72, Number 7, Page 1372-1380 (January 11, 2007).

E. Future Regulatory Environment and Regulatory Risks

It is difficult to predict the future regulatory environment because most regulations are a reaction to certain external events, such as terrorism, financial market collapses, and improper business conduct. The only control that the government has in this area is to continually assess current conditions to ensure the system is working and regulations are serving their intended purpose. As Treasury Secretary Henry M. Paulson recently stated, "When it comes to regulation, balance is key. Excessive regulation slows innovation, imposes needless costs on investors, and stifles competitiveness and job creation".[19]

There have been some recent indications that adjustments are necessary in order to achieve the proper regulatory balance that will allow U.S. capital markets to thrive. For the most part, regulations are being added while existing regulations are not being reviewed or scaled back. In the years since the passage of GLBA, several events have produced a wave of regulations that has greatly impacted how financial services institutions treat compliance. The passage of the Financial Services Regulatory Relief Act of 2006 did provide some relief in the areas such as GLBA privacy notices, extended cycles on examinations, and protection of attorney-client privilege (in relation to information provided to bank supervisors). However, there is evidence that more radical regulatory relief is needed. Regulatory relief may come in many forms, including legislation and agency action. Regulatory relief can also be achieved through coordination among financial regulators and the industry to review the impact of specific regulations.

Financial services institutions believe that regulations associated with the Bank Secrecy Act and Sarbanes-Oxley is where the most regulatory relief is needed.[20] In relation to AML regulations, banking and other regulatory agencies have been coordinating through the Federal Financial Institutions Examination Council (FFIEC) to reduce redundancies and achieve consistency in examination and supervision. There have been indications that these efforts have made a difference. The 2006 growth rate of suspicious activity reports (SARs) filings from the previous year was well below that of previous years.[21] In addition, significant findings and enforcement actions relating to AML have declined over the past year.

Regarding Sarbanes-Oxley, the PCAOB and the SEC have worked to coordinate with all financial services regulators and reach out to the industry through joint forums and programs. Some of the industry's concerns have resulted in proposed changes to Auditing Standard No. 2, which was proposed by the PCAOB and the SEC in December 2006.[22] The four objectives of Auditing Standard No. 5, which was approved by the PCAOB in May 2007 and will replace Auditing Standard No. 2, are:

1. Promote efficiency by directing auditors to focus on the most important controls. This includes allowing information from internal auditors to be considered by external auditors.
2. Eliminate requirements that are unnecessary to achieve intended benefit. This includes less detailed requirements to evaluate management's own evaluation process and clarifies that the audit does not require an opinion of the adequacy of management's process.
3. Make the audit clearly scalable to fit the size and complexity of any company.
4. Simplify the text of the standard and make it shorter and easier to read.[23]

[19] Remarks by Treasury Secretary Henry M. Paulson, Remarks on the Competitiveness of U.S. Capital Markets, Economic Club, New York, NY (Nov. 20, 2006).
[20] Rob Garver, Charters, Basel, Regulators, Lobbyists, American Banker Executive Forum 2Q '06, American Banker (Aug. 4, 2006) at p. 14, available at www.americanbanker.com.
[21] Cheyenne Hopkins, Defying Forecasts SARs, Filings Didn't Spike, American Banker (January 12, 2007) at p. 1, available at www.americanbanker.com.
[22] PCAOB Release No. 2006-007: Proposed Auditing Standard: An Audit of Internal Control Over Financial Reporting that is Integrated with an Audit of Financial Statements (Dec. 19, 2006) and SEC Release No. 33-8762, Mgmt's Rep. on Internal Control Over Financial Reporting, amending Rule 13a- 15(c) and Rule 15d-15(c) under the Securities Exchange Act of 1934 (December 20, 2006).
[23] Details on Auditing Standard No. 5 and changes that the PCAOB made from its original December proposal are available at http://www.pcaob.org/News_and_Events/News/2007/05-24.aspx.

III. Enterprise Risk Management (ERM): A New Paradigm

A. ERM Process

The emergence of ERM has greatly impacted how organizations manage risk and compliance. ERM is a process of managing risk across business lines and geographic locations rather than within individual business units. The evolution of ERM has created a much broader view of risk management than had previously existed, and compliance risk is an important part of any ERM system.

According to former Federal Reserve Governor Susan Schmidt Bies, ERM is a process that enables management to effectively deal with uncertainty and associated risk and opportunity, enhancing capacity to build stakeholder value. ERM includes:

- Aligning the entity's risk appetite and strategies
- Enhancing the rigor of the entity's risk-response decisions
- Reducing the frequency and severity of operational surprises and losses
- Identifying and managing multiple and cross-enterprise risks
- Proactively seizing on the opportunities presented to the entity
- Improving the effectiveness of the entity's capital deployment. [24]

In today's regulatory environment, organizations have to expand the compliance function and conduct risk assessments on an enterprise-wide basis. As former Federal Reserve Governor Mark W. Olson stated, "the need for an enterprise-wide approach to compliance risk management at larger, more complex firms is suggested by the diversity of laws and regulations that span business lines, legal entities, and geographic boundaries – for example, in the areas of Bank Secrecy Act compliance and anti-money laundering controls, fair lending, information security, privacy, transactions with affiliates (Regulation W), and conflicts of interest."[25] As financial institutions grow, and as technology advances and new products are developed, the compliance function must adjust for additional risk exposures.

The supervision of financial services institutions on a consolidated basis has itself taken on an ERM approach. For years, federal bank regulators, including the Federal Reserve and the OTS, have supervised entities on a consolidated basis by

As the GAO recently stated, consolidated supervision of financial services firms has become more important because firms have grown dramatically and become more complex in terms of the products and services they offer;

examining the safety and soundness of bank holding companies, savings and loan holding companies, their subsidiaries, and affiliates. In addition, under new SEC rules, in order for broker-dealers to take advantage of alternative net capital requirements, they must register as supervised investment bank holding companies.[26] These consolidated supervised entities (CSEs), and their internal risk management control processes, are subject to consolidated supervision by the SEC. New regulations and the emergence of ERM are indicative of a trend of large, complex firms managing risks (and being supervised) on a consolidated enterprise-wide basis. As the GAO recently stated, consolidated supervision of financial

[24] Federal Reserve Governor Susan Schmidt Bies speech to American Bankers Association Convention, Phoenix, Arizona (Oct. 17, 2006). Speech available at http://www.federalreserve.gov/boarddocs/speeches/2006/20061017/default.htm
[25] Federal Reserve Governor Mark W. Olson speech to The Financial Services Roundtable and the Morin Center for Banking and Financial Services Compliance Conference, Washington, D.C. (May 16, 2006). Speech available at http://www.federalreserve.gov/boarddocs/speeches/2006/20060516/default.htm
[26] Alternative Net Capital Requirements for Broker-Dealers that are Part of Consolidated Supervised Entities, 69 Fed. Reg. 34,428 (June 21, 2004); and Supervised Investment Bank Holding Companies, 69 Fed. Reg. 34,472 (June 21, 2004).

services firms has become more important because firms have grown dramatically and become more complex in terms of the products and services they offer; firms increasingly operate on a global basis; and firms manage risk on an enterprise-wide basis.[27]

B. Committee of Sponsoring Organizations of the Treadway Commission (COSO)

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) brought a different approach to risk management.[28] COSO focuses on internal controls, which it defines as "a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations."[29]

Under COSO, internal controls must ensure performance and profit goals, reliable financial reporting, and compliance with applicable law. The COSO framework consists of eight interrelated components, which govern the way risk is managed:

1. Internal environment
2. Objective setting
3. Event identification
4. Risk assessment
5. Risk response
6. Control activities
7. Information and communication
8. Monitoring.

This framework may be applied differently based on the size and type of institution.

COSO provides the framework for the internal control and financial reporting requirements under Section 404 of Sarbanes-Oxley and was also used as a model for similar requirements for banking institutions under Section 112 of the Federal Deposit Insurance Corporation Improvement Act of 1991. Regulators frequently refer to COSO when discussing enterprise risk management and how financial institutions should manage and mitigate risk exposures across an organization.

C. Compliance Risk

Under ERM, financial services institutions review several types of risk across an organization. Financial institutions have long measured credit and market risk. With the dawning of the new Basel II capital standards, operational risks (the risks of people and systems) must also be reviewed and assessed. One crucial type of operational risk is compliance risk. "Compliance risk can be defined as the risk of legal or regulatory sanctions, financial loss, or damage to an organization's reputation, and franchise value".[30] It is axiomatic that the areas with the greatest risk exposure should receive additional attention. Identifying compliance risks and establishing appropriate controls is paramount to mitigating risk exposure. With this in mind, financial institutions carefully evaluate compliance risks, and monitor compliance risks.

[27] GAO Report, supra note 17.
[28] Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a U.S. private-sector initiative, formed in 1985. Its major objective is to identify the factors that cause fraudulent financial reporting and to make recommendations to reduce its incidence. COSO has established a common definition of internal controls, standards, and criteria against which companies and organizations can assess their control systems.
[29] See COSO definition of internal controls, www.coso.org available at http://www.coso.org.
[30] Governor Susan Schmidt Bies remarks at the Financial Women's Association Washington Briefing, Washington, D.C. (June 12, 2006), available at http://www.federalreserve.gov/boarddocs/speeches/2006/200606122/default.htm

IV. Compliance Measurements

A. Cost of Compliance

Compliance costs clearly have an effect on a corporation's bottom line, since a significant portion of a company's expenses are earmarked for the compliance function. A Securities Industry and Financial Markets Association (SIFMA) report stated that the securities industry spent $25 billion in compliance in 2005, up from $13 billion in 2002.[31] In a recent American Banker survey, 99% of the respondents stated that the percentage of revenue spent on compliance in the last three years had increased.[32] Both the SIFMA Report and the American Banker survey noted that compliance costs are a significant percentage of total expense. According to the SIFMA Report, much of the increased costs were related to the following: duplication in examinations, regulations and supervisory actions, inconsistencies/lack of harmonization in rules and regulations, ambiguity, and delays in obtaining clear guidance from regulators.

In general, the most expensive compliance line items are people and systems. Expenditures on compliance staff and technology varies significantly depending on a variety of factors, including the qualifications of individuals, training, proper implementation of programs, as well as an ongoing commitment to these resources. Financial services institutions have contracted with vendors and utilized software solutions to meet increasing regulatory requirements. One major global financial institution is spending approximately $250 million annually on technology to address weaknesses cited by regulators.[33] The largest and most complex firms have anywhere from 1,000 to 2,000 employees devoted to compliance worldwide.

Firms either pass on the compliance costs to individual customers, or their shareholders absorb them.

Further, compliance costs associated with new specific regulations have been staggering. The average first year costs per firm of implementing controls associated with Section 404 of the Sarbanes-Oxley Act was $4.36 million.[34] It has been estimated that U.S. banks will spend over $14.7 billion on anti-money laundering compliance between 2005 and 2008.[35] A large portion of these costs are associated with technology. As of 2006, it was reported that 94 percent of large financial institutions in the United States had installed AML software or related technology[36]. Securities firms, which had not been previously subject to AML requirements, spent around $700 million from 2003-2006 on AML software solutions.[37] It is expected that the cost for ongoing systems will grow.

As the SIFMA report suggests, what cannot be easily measured are the opportunity costs. "Every time an employee spends additional time on compliance-related activities instead of developing business,

[31] Stephen L. Carson and Frank A. Fernandez, The Cost of Compliance in the U.S. Securities Industry, Securities Industry Association Research Reports, Vol. 7, No. 2 at p. 3 (February 22, 2006), available at http://www.financialcounsel.com/News/Economics/SIA/2006/SIA-0206.pdf.
[32] See Garver supra note 20.
[33] John Garvey & Miles Everson, Containing the Cost of Compliance: A Major Challenge for Financial Institutions, Bank Accounting & Finance (Aug. 1, 2006).
[34] Interim Rep. of the Committee on Capital Markets Reg. supra note 12 at 5.
[35] Dr. Vasant Godse , White Paper on Anti-Money Laundering, L&T Infotech Confidential, at p. 8, http://www.lntinfotech.com/lntinfotech/WhitePapers/AML%20Whitepaper.pdf
[36] Source: TowerGroup
[37] Id.

opportunity costs are incurred."[38] Firms have also spent considerable time and capital on regulatory and compliance consultants and outside counsel in attempting to manage risks. Firms either pass on the compliance costs to individual customers, or their shareholders absorb them.

The costs of compliance fall most heavily on small firms that cannot spread the expense over a large base. There is ample anecdotal evidence that these costs have been a contributing factor to consolidation within the financial services industry. Of course, in addition to costs causing a company's sale, individual transgressions can occasion a company's sale, as was the case with Riggs Bank.

It is important to note that some of these compliance costs do serve a useful purpose in creating corporate governance and standards that lend integrity to the markets and protect the consumer. However, because of the lack of balance in the regulatory approach, there are excessive costs that outweigh the benefits. It is this disparity that needs to be addressed.

B. Cost of Noncompliance

Regulators have made it clear that compliance should no longer be considered a cost center. Former Federal Reserve Governor Susan Schmidt Bies stated, "In many instances, senior management must move from thinking about compliance as a cost center to considering the benefits of compliance in protecting against legal and reputational risks that can have an impact on the bottom line."[39]

Noncompliance can negatively affect a company's bottom line through fines, penalties, sanctions, legal fees, loss of stock, and brand value. There are multiple reputational and legal risks associated with noncompliance. Legal penalty risks can be easily quantified. In the banking industry, between January 1, 2003 and January 1, 2006, 800 banks paid $492 million in connection with 2,500 publicly announced sanctions.[40] Some of the most notable cases involved high-profile violations of the Bank Secrecy Act. In the insurance industry, significant actions have been brought against companies for bid rigging and fraudulent practices, including an $850 million settlement paid by Marsh & McLennan as a result of an investigation by the New York Attorney General. AIG paid the state of New York $1.64 billion in restitution and fines, and the SEC $800 million to settle claims for fraud/bid-rigging and improper accounting[41]. In addition, pre-GLBA, several class action lawsuits for deceptive sales practices by insurance agents were brought against insurance companies. These included two notable settlements in 1997 involving Prudential Insurance ($410 million) and John Hancock Financial ($471 million).[42] Post-GLBA, securities class action settlement costs have increased from $150 million in 1995 to $3.5 billion in 2005 (excluding the $6.1 billion WorldCom settlement).[43]

Reputational risks are also very costly. As seen in the Arthur Andersen case, a criminal indictment against a company can be a death sentence. In addition, enforcement actions, fines, and sanctions can significantly impact a company's brand value and its attractiveness to analysts and shareholders. Because of the nature of their business, ethics and integrity are vital for financial services institutions. Once a consumer loses faith in an institution, it becomes more difficult to compete with others in the industry.

C. Metrics: How to Measure Costs and Effectiveness

The Role of Capital

The challenge for a financial services institution's board of directors and senior management is to measure the effectiveness of a compliance program and determine whether the money spent on compliance is adequate to efficiently manage risks. There have been attempts to quantify the effectiveness of the compliance function. For example, a General Counsel Roundtable study found that each $1.00 spent on compliance can reduce legal liability by $1.37.[44] A 2006 survey by the Risk Management Association reviewed metrics on more general terms.[45] When asked how institutions currently measure the effectiveness of enterprise risk management, companies stated that the top measurements were:

- Favorably looked upon by regulators and market analysts – 67.7%
- Fewer deviations from compliance – 48.4%
- Improved audit results – 35.5%.

When asked how institutions plan to measure effectiveness over a subsequent 18-24 month period, the top three measurement factors were:

- Improved risk-adjusted profitability – 58.1%
- Improved shareholder value – 41.9%
- Favorably looked upon by regulators and market analysts – 41.9%.

Success of compliance programs can be measured by internal factors, such as self-testing results, risk assessments, compliance reviews, and internal audit findings. Success can also be measured externally though supervisory examinations, external audits, and company market value. In measuring success, auditors and analysts place great value on the ethical culture within a company and the company's overall compliance program.

Empirical data can be used to gauge compliance efficiencies, including the number of customer complaints, internal ethics hotline calls, suspicious activity reports, or other reports of irregular activity. An organization may measure its program by how well it identifies and resolves compliance-related issues, particularly breaches. A company's compliance program may also be measured against events that do not occur, such as enforcement actions, fines, civil litigation, etc.

Success of compliance programs can be measured by internal factors, such as self-testing results, risk assessments, compliance reviews, and internal audit findings.

Under the new Basel II standards, compliance risk is an element of operational risk. In general, firms with the highest compliance risks will be required to hold higher levels of capital while firms with effective compliance programs will be allowed by their regulator to operate with reduced capital. Thus, regulatory guidance as to what constitutes an effective compliance program could have a profound impact on the capital, the profitability, and the competitiveness of all firms.

[38] Securities Industry Association Research Report at p. 8, supra note 31.
[39] Governor Susan Schmidt Bies remarks at the Bond Market Association's Legal and Compliance Conference: Enterprise-Wide Compliance Programs (Feb. 4, 2004), available at http://www.federalreserve.gov/boarddocs/speeches/2004/20040204/default.htm.
[40] Robert Hartheimer, Take a Business Approach to Compliance, American Banker (January 13, 2006).
[41] See Spitzer Effect: Tabulating His Prosecutions, American Banker, Jan. 10, 2007, supra note 4.
[42] In re Prudential Ins. Co. of Am. Sales Practices Litig., 148 F.3d 283, 333-38 (3d Cir. 1998); *Duhaime v. John Hancock Mut. Life Ins. Co.*, 989 F. Supp. 375 (D. Mass. 1997).
[43] Interim Report of the Committee on Capital Markets Regulation supra note 12 at p. 5.
[44] General Counsel Roundtable, Corporate Executive Board, Seizing the Opportunity, Part One Benchmarking Compliance (2003) at p. 27.
[45] Risk Management Association, Enterprise Risk Management Survey (2006), available at http://www.rmahq.org/NR/rdonlyres/B9281EB1-8961-4C5A-B211C0927C870451/0/ERMDistribute2Public.pdf.

V. Summary of Regulatory Guidance on Compliance for Financial Services Institutions

The compliance function in an organization is a product of the current regulatory and enforcement environment. Compliance is also shaped by a company's organic growth and acquisition activity. As a financial institution evolves, it must pay special attention to the rules and regulations on compliance. This guidance may come from several sources. Some regulations, such as those associated with the Bank Secrecy Act, outline how to comply with its requirements. Other guidance, such as the Basel Committee on Banking Supervision's paper on compliance and the Federal Sentencing Guidelines, focus more on the elements of an effective compliance program. There have also been a number of important guidelines on compliance and ERM issued in the last few years, as discussed below.

A. Federal Sentencing Guidelines

The Federal Sentencing Guidelines (2004), Chapter 8, Part B (Sentencing Guidelines) provide a basis for prosecutors charging corporations in deciding what type of penalties to bring against them. There are several mitigating factors in this decision process. One of the factors is whether or not a corporation has an effective compliance and ethics program. The Sentencing Guidelines outline what constitutes an effective compliance program. The Sentencing Guidelines make distinctions for organizations based on the size of the company and industry practices. In relation to all organizations, the Sentencing Guidelines state that each corporation shall:

- Exercise due diligence to prevent and detect criminal conduct. Due diligence means having strong oversight, clearly defined procedures, monitoring and audit processes, and formal training programs.
- Promote a culture that encourages ethical conduct and a commitment to compliance with the law.

On December 12, 2006, the DOJ issued the McNulty Memorandum.[46] The purpose was to update the Thompson Memorandum and discuss the issue of how waiver of attorney-client privilege is used in the course of government investigations. The McNulty Memorandum also updated the Sentencing Guidelines and expanded upon the elements of an effective compliance program. The Memorandum states that compliance programs are established by corporate management to prevent and detect misconduct and to ensure that corporate activities are conducted in accordance with all applicable criminal and civil laws, regulations, and rules.[47] It also emphasizes the importance of maintaining a program and that prosecutorial decisions are based on the effectiveness of the program, not just single instances or violations of the law. In addition, it stresses that compliance guidelines should be sufficiently implemented and not be merely "paper" programs,[48] and lists the following as factors for effective compliance programs:[49]

- Whether the compliance program is well designed to detect misconduct most likely to occur in a particular corporation's line of business
- Whether the compliance program works (is the program effective in preventing or detecting misconduct?)
- Whether the program is adequately designed for maximum effectiveness in prevention and detection of wrongdoing by employees
- Whether corporate management is enforcing the program or tacitly encouraging employees to engage in misconduct to achieve business objectives
- Whether the corporation has established corporate governance mechanisms (for example, do directors exercise independent review of officers' recommendations?; are auditors sufficiently independent?; are management and the board of directors adequately informed?)

B. Banking

Basel Committee on Banking Supervision

The Basel II Capital Accord has created a new paradigm for compliance. Operational risk, defined as the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events, is one of the focuses of Pillar II, the supervisory pillar. Operational risk includes compliance risk (i.e. risk of legal or regulatory sanctions, financial loss, or damage to reputation).

The Basel Committee on Banking Supervision's (Basel Committee) goal is to promote safety and soundness among banking organizations. The Basel Committee issued a paper in April 2005, *Compliance and the compliance function in banks* (Basel Committee Paper).[50] The Basel Committee Paper underscores how organizations should create a culture of compliance that starts at the top of the organization. The paper outlines several key compliance principles, including the structure of a compliance program, the need for an independent compliance function, roles and responsibilities (including those of the board of directors, senior management, and internal audit), how to manage compliance risks, the resources needed to effectively manage compliance, cross-border issues, and the potential outsourcing of risk management functions. The paper discusses the differences in the compliance function depending on the size of the institution. It also touches upon establishing specialized compliance functions in areas such as anti-money laundering and data protection.

Federal Bank Regulators and State Banking Departments

All four federal banking regulators, the Federal Reserve, the Office of the Comptroller of the Currency (OCC), Office of Thrift Supervision (OTS), and the Federal Deposit Insurance Corporation (FDIC) have issued guidance on compliance programs and how to manage compliance risk. State banking departments, as well as their coordinating body, the Conference of State Bank Supervisors (CSBS), have communicated formally and informally about their expectations on compliance. Each agency provides guidance and validation throughout its supervisory reviews of institutions.

[46] Memorandum from Paul J. McNulty, Deputy Attorney General to Heads of Dep't Components and United States Attorneys (Dec. 12, 2006), available at http://www.usdoj.gov/dag/speech/2006/mcnulty_memo.pdf.
[47] Id. at p. 12.
[48] Id. at p. 14.
[49] Id., Part VIII, Charging a Corporation: Corporate Compliance Programs, p. at 12-15.

[50] Source: Basel Committee on Banking Supervision, Compliance and the Compliance Function in Banks (April 2005), available at http://www.bis.org/publ/bcbs113.pdf.

C. Securities

International Organization of Securities Commissions Report on Compliance Functions at Market Intermediaries

The International Organization of Securities Commissions (IOSCO) is an organization of international securities regulators which promotes the development and integrity of capital markets as well as the effective enforcement against violations of securities laws. IOSCO's three main principles are:

1. The protection of investors
2. Ensuring that markets are fair, efficient and transparent
3. The reduction of systemic risk.[51]

In March 2006, the Technical Committee of the International Organization of Securities Commissions (IOSCO Committee)[52] issued a final report on the Compliance Function at Market Intermediaries (IOSCO Report). The purpose of the IOSCO Report was to establish broad international principles in the area of compliance for securities firms. The IOSCO Report discusses how these principles can be implemented by individual firms. The report states that all firms should have a compliance function designed to ensure compliance with securities regulatory requirements although these functions may vary according to a firm's size, the nature of its business, and the risk it undertakes.[53] According to the IOSCO Committee, the role of compliance is to identify, assess, advise, monitor, and report on a market intermediaries' compliance with securities regulatory requirements and the appropriateness of its supervisory procedures on an ongoing basis.[54] In order to achieve this goal, the IOSCO Committee suggests that compliance departments be given the necessary authority and resources to discharge their duties.

The other high level principles outlined in the report include:

1. The role of senior management and the governing authority
2. Independence and the ability to act
3. Qualification of compliance personnel
4. Assessment of the effectiveness of the compliance function
5. Regulators' supervision
6. Cross-border compliance arrangements
7. Outsourcing of the compliance function.

SEC and NASD/NYSE Rules

There are several compliance rules pertaining to investment advisers, broker-dealers, and mutual funds, as explained below.

Rules 206(4) – 7 under the Investment Advisers Act of 1940 and Rule 38a-1 under the Investment Company Act of 1940 require registered investment companies and investment advisers to adopt and implement written policies and procedures designed to prevent the violation of federal securities laws. These policies and procedures must be reviewed annually by the relevant regulators for adequacy and effectiveness. These rules also require a chief compliance officer (CCO) be responsible for administering the policies and procedures.

In the case of the investment companies, Rule 38a-1 requires the chief compliance officers to report directly to the fund's board of directors and the fund's board must approve all compliance policies and procedures. In December 2005, the Investment Company Institute (ICI) published a report which

[51] Int'l Org. of Securities Comm'ns, Objectives and Principles of Securities Regulation (2003), available at http://www.iosco.org/library/pubdocs/pdf/IOSCOPD154.pdf.
[52] Int'l Org. of Securities Comm'ns, Compliance Function at Market Intermediaries (2006), available at http://www.iosco.org/library/pubdocs/pdf/IOSCOPD214.pdf.
[53] Id. at p. 5.
[54] Id. at 7.

provides useful guidelines on how a CCO may assess the effectiveness of a fund's compliance policies and procedures and what type of information should be provided to the fund's board.[55]

NASD Rule IM-3013 and NYSE Rule 342.30(e) require broker-dealers to certify annually that they have processes in place to establish, maintain, and review polices and procedures reasonably designed to achieve compliance with applicable self-regulatory organizations (SRO) rules and federal securities laws and regulations, and to modify such policies and procedures as business, regulatory, and legislative changes and events dictate. These firms must share annual reports of their compliance and supervision programs with regulators. NASD Rule 3012(a)(1) requires broker-dealers to establish principals who will establish, maintain, and enforce a system of supervisory control policies and procedures that tests and verifies a member's supervisory procedures are reasonably designed to comply with applicable securities laws and NASD rules.

D. Insurance Regulations

Although insurance companies often compete with banks and securities firms, they are regulated differently. Compliance in the insurance industry is unique in that the McCarran Ferguson Act, passed in 1945, allows the states to provide exclusive regulatory authority for the insurance industry. Despite efforts to create an optional federal insurance charter, each state insurance department currently has the ability to offer different perspectives on insurance rates, market conduct, solvency, and other practices. There is some level of uniformity offered by the National Association of Insurance Commissioners (NAIC) which drafts model rules and laws. These rules and laws must be passed by state legislatures before being implemented, and having to comply with a wide range of state laws provides many challenges for the insurance compliance professional. Insurers operating on a national level must:

- Be licensed in all states and territories in which they operate
- Obtain separate approvals for each new product in each state and territory in which they operate
- Annually undergo separate market conduct examinations in each state and territory in which they operate
- Meet different sets of administrative and regulatory requirements in each state in which they operate.[56]

Insurance companies' compliance with market conduct and other practices is reviewed through state examinations. In addition, their practices are enforced by attorneys general in each state where a company does business.

The landscape for the insurance industry has changed since the passage of GLBA. With the creation of diversified financial services institutions, banks may sell insurance products. This has created new regulatory and supervisory challenges for bank and other holding company supervisors. Because of the risks associated with bank insurance sales, regulators have stressed that these institutions must focus on compliance with consumer protection regulations. This involves issues of suitability, adequate disclosure, and separation of insurance sales from bank product sales.

[55] Investment Co. Institute, Assessing the Adequacy and Effectiveness of a Fund's Compliance Policies and Procedures (2005), available at http://www.ici.org/pdf/rpt_05_comp.pdf.
[56] American Council of Life Insurers, Optional Federal Charter, information available at http://www.acli.com/ACLI/Issues/40.htm.

E. Other Guidance on Compliance

Speeches

With increasing frequency, regulators have been using informal means to communicate their views on compliance to the industry and to the markets. No longer can firms look solely to rules, interpretations, and other official agency communications for the final word on the regulator's expectations. Rather, speeches, testimony and even interviews contain key "signals" of regulatory attitudes on key compliance issues.

...speeches, testimony and even interviews contain key "signals" of regulatory attitudes on key compliance issues.

Several recent speeches by Federal Reserve Governors, SEC Commissioners, and other officials have discussed the importance of a culture of compliance and the need for a comprehensive program to implement and promote an ethical culture. As one SEC official stated, in accordance with U.S. securities laws, it is necessary to provide for regulation and control in order to protect interstate commerce and ensure the maintenance of fair and honest markets. To achieve this goal it is necessary to maintain comprehensive compliance systems.[57] Clearly, there has been some consumer skepticism and additional regulatory scrutiny in the wake of corporate scandals over the past few years. Government officials' remarks have underscored the role of compliance in maintaining a flourishing financial services industry and integrity within these markets.

Compliance Obligations Embedded in Regulations

In addition to speeches and testimony on compliance, direction on compliance is embedded in many regulations, bulletins, and supervisory letters. For example, AML regulations provide specific guidance on how compliance with these laws should be administered. Moreover, under Sarbanes-Oxley, certain controls must be implemented and the effectiveness of these controls must be attested to by senior executives. Implicit in each regulation is additional guidance and challenges for the compliance professional who must not only understand the black letter of the law, but how it will be implemented and how examiners may choose to interpret subjective areas of the guidance.

Examination Manuals and Handbooks

Guidance for compliance professionals is also provided in examination manuals which outline what examiners are going to inspect when reviewing an organization. For example, the SEC offers an examination brochure to broker-dealers prior to supervisory examinations. These pamphlets outline the examination process and the SEC's expectations. Prior to examinations, examiners discuss the scope of the examination and list particular areas of concern that the SEC has uncovered though prior examinations or industry risk-based investigations (i.e. sweeps). The federal bank regulators have similar supervision manuals for regulated institutions and a manual for expectations at the holding company level. Bank regulators have handbooks addressing certain compliance areas, such as the Federal

[57] Mary Ann Gadziala, SEC, Associate Director, Sec. Exchange Comm'n, Speech at the Compliance Management and Structure Conference, Washington, D.C.: Comprehensive Compliance Examinations for Securities Firms, (May 16, 2006), available at http://ftp.sec.gov/news/speech/2006/spch051606mag.htm.

The federal banking regulators have stressed that its enforcement actions are not akin to a rulemaking and should not be used to create or validate a compliance program.

Reserve's Consumer Compliance Handbook, FDIC's Compliance Examination Handbook, or the OCC's Comptroller's Handbook, which address consumer related regulations and the supervisory guidelines. Some of these manuals are produced jointly by multiple agencies such as the FFIEC's AML/BSA Examination Manual and the FFIECs' Information Technology Examination Handbook which is a guide for conducting information technology examinations at financial institutions and technology service providers. Formerly used primarily as a device for communicating with examiners in the field, these handbooks are now used to communicate agency expectations regarding compliance to regulated firms.

Enforcement Actions

Many SEC and state attorneys general actions in recent years have acted as *de facto* rules in relation to certain practices. Often referred to as "rulemaking by enforcement" these settlements have filled the void in areas where regulators have not written new rules. The SEC Enforcement Division has looked to previous actions and settlements as guidance in pursuing additional actions. The SEC has also delineated various compliance procedures and requirements as part of settlements. For example, in the market timing settlements with mutual funds, the SEC required that firms establish internal controls to review funds' compliance policies and report to the audit committee. Breaches of controls were to be reported by the chief compliance officer.[58] The industry took note and made the necessary changes.

The federal banking regulators have stressed that its enforcement actions are not akin to a rulemaking and should not be used to create or validate a compliance program. In reality, financial institutions can, and do, look to these actions to enhance policies, procedures, and controls and to divine the inclination of their regulators.

[58] See In re Massachusetts Financial Services. Fin. Serv. Co., Investment Advisers Act Release No. 2213, Investment Company Act Release No. 26347 (February. 5, 2004), available at http://www.sec.gov/litigation/admin/ia-2213.htm.

VI. Elements of an Effective Compliance Program: Harmonizing Regulator Views Versus Industry Approach

A. Development of Best Practices

As indicated, the focus on compliance has changed dramatically in the last few years due to increased regulatory scrutiny. Compliance has become a more formalized function. Compliance staffing and resources have been greatly expanded. More resources and technologies have been incorporated. Additional reporting is occurring between compliance, senior management, and the board of directors. Compliance officers frequently report to the CEO, audit committee, and board of directors. Compliance plays a greater role in business decisions and is less likely to be folded into a firm's legal department.

Most regulators agree that there is no standard blueprint for the elements of compliance programs, but have stated that compliance programs should be structured according to the size of the firm and the risks associated with an organization's business model. Programs should include comprehensive policies and procedures and strong independent oversight. Compliance's main function should be to identify, assess, monitor, educate, and support business lines' compliance with relevant laws and regulations. The individual business lines should ultimately own compliance. The corporate compliance function should act as a trusted partner and advisor.

The following outlines some of the key elements that comprise a successful compliance program as gleaned from official pronouncements. These are derived from a combination of written regulatory guidelines as well as interviews with regulators and industry compliance officers that provided insight on the intent of the guidelines and what is needed to create a successful compliance program. As is evident from the discussions of each element, in some areas there is clear harmonization between the regulator's expectations and industry's responses; in other areas, there is discord and a need for additional guidance.

Elements of an Effective Compliance Program

- ☑ Culture of Compliance: Tone at the Top
- ☑ Structure: Roles and Responsibilities
- ☑ Role of Board of Directors and Senior Management
- ☑ Risk Assessments
- ☑ Policies and Procedures
- ☑ Tracking New Regulations and Regulatory Changes
- ☑ Oversight and Monitoring
- ☑ Escalation of Issues and Investigations
- ☑ Testing and Validation
- ☑ Training and Awareness
- ☑ Regulatory Examinations
- ☑ Strong Rapport with Regulators
- ☑ Accountability
- ☑ Adequate Resources and the Use of Technology
- ☑ Staff Expertise

Culture of Compliance: Tone at the Top

Regulators have made it clear that creating a culture of compliance is top priority. Former Federal Reserve Governor Susan Schmidt Bies stated, "A culture of compliance should establish – from the top of the organization – the proper ethical tone that will govern the conduct of business".[59] Mary Ann Gadziala, Associate Director of SEC's Office of Compliance Inspections and Examinations (OCIE) noted that, "a 'culture' of compliance at a firm is an overall environment that fosters ethical behavior and sensitivities to compliance with the law in all decision-making."[60] The goal for firms is to establish parameters of ethical business conduct and have that be a part of every decision that is made throughout the organization. By doing so, an organization is establishing its compliance identity and promoting it across business lines.

[59] Governor Susan Schmidt Bies Remarks at the Bond Market Association's Legal and Compliance Conference, supra note 39.
[60] Mary Ann Gadziala, supra note 57.

There are many ways to establish a culture of compliance within a company. A company's board of directors and senior management set the tone at the top. Companies must ensure that the right individuals are placed in leadership positions and compliance executives are committed to corporate integrity and ethics. The role of senior management is to understand compliance programs and exercise oversight over the implementation of the program. This includes establishing transparency at every level of the organization by clearly defining roles and responsibilities and communicating directly with employees about expectations on business conduct.

An institution establishes an identity in the way it conducts business and its commitment to ethics and integrity. The tone for compliance may be established through a strong compliance charter and mission. Ethical principles may be defined in a comprehensive code of conduct policy. A company may also set the tone for compliance by firmly establishing its risk tolerance and what types of business it is willing to accept.

Ethical standards should be applied consistently throughout the organization, with all employees taking ownership of compliance rather than relying on a centralized oversight of compliance risks. Ethics hotlines and other mechanisms allow employees to report and escalate issues anonymously and without retaliation. Incidents that are escalated should be adequately investigated and wrongdoing addressed swiftly and in accordance with company policy. Employees can be held accountable for their compliance efforts via annual performance reviews. Bonuses and other rewards for adhering to company policy can also add value to compliance efforts. Similarly, compensation plans that provide incentives for questionable behavior should be rejected.

Communication to employees from management is important, whether it is through direct communications or through actions. As one compliance executive stated, compliance needs to be "marketed" to employees and branded. One example of expressly promoting a culture of compliance is management's decision at Bank of America to have all employees' email communications include the message, "compliance is everybody's business at Bank of America". Compliance committees and other working groups involving multiple business lines may be used to create a forum to discuss emerging risk areas and to provide training on compliance-related topics.

As Lori Richards, SEC's OCIE Director recently noted, "at its best, a strong culture of compliance can serve to foster and enhance compliant practices, and, at its worst, it can result in violations of law by firm employees and render efforts by compliance staff meaningless.[61] In order to enhance compliant practices, compliance executives need to continually monitor and update programs to reflect regulatory and business changes. The effectiveness of the compliance program should be assessed at least quarterly and tested by internal and/or external audit.

The role of corporate compliance is to support the business units and to provide monitoring and oversight.

Structure: Roles and Responsibilities

There is no one size fits all approach when it comes to how a compliance department should be organized. A compliance department in a large, diversified

[61] Lori A. Richards, Director, SEC Office of Compliance Inspections and Examinations, The Process of Compliance, National Sec. Exchange Comm'n , Speech at the National Membership Meeting of the National Society of Compliance Professionals, (October: The Process of Compliance (Oct. 19, 2006), available at http://sec.gov/news/speech/2006/spch101906lar.htm.

financial institution will look vastly different than a compliance function within a community bank or small investment advisor. Regulators appreciate these distinctions and have pointed out that smaller firms can require simpler policies and procedures as long as the regulatory objectives are being met. Regulators have warned, however, that as smaller firms grow and develop new products and services, their compliance resources should scale appropriately.[62] There are a variety of factors to be considered by a financial institution when establishing its compliance function, including:

1. The products it offers
2. Its client base
3. The structure and diversity of its operations (including the geographic areas in which it operates and regulatory requirements for its operations)
4. The number of people it engages to conduct its business.[63]

There are several reporting models for compliance. The compliance officer may report to the general counsel, chief risk officer, chief operating officer, or CEO. Traditionally, compliance has reported to a top legal executive. However, with the advent of enterprise risk management, there has been a trend to move the function to the risk management departments. The reason for this change is two-fold. First, it allows compliance to assess risk across the organization and coordinate with the ongoing efforts of a risk officer in measuring operational risk. Second, there are benefits from separating compliance and the legal function. Legal departments can more adequately advise compliance on issues independently, for example. This is especially helpful in the course of internal investigations. In addition to day-to-day reporting, regulators require compliance to report to the board of directors and/or audit committee on an ongoing basis.

It is important that the corporate compliance department, and the compliance officer, remain independent of the business lines. The compliance officer should be given the ability to seek information throughout the organization, review possible breaches, conduct investigations, and report issues directly to senior management, the audit committee, and the board of directors without undue influence. Compliance officers also need adequate resources to carry out their responsibilities. In some organizations, the board and/or audit committee determine compensation for compliance officers to maintain further independence.

The role of corporate compliance is to support the business units and to provide monitoring and oversight. Companies may choose to enhance the compliance function by placing compliance personnel within the business lines. This approach is effective because these individuals will possess first-hand knowledge about customers, products, and other business operations. Compliance professionals within the business lines should report to corporate compliance in some fashion. This may be a formal reporting structure or a "dotted line" to corporate compliance with a direct report to managing directors in the business units. Institutions may consider forming compliance committees and other working groups to ensure that there is proper communication with the business units.

Roles and responsibilities of compliance must be clearly delineated. Regulatory guidance, such as the Basel Committee on Banking Supervision's paper, *Compliance and the Compliance Function in Banks* states that "the Board of Directors should ensure the organization has a top-to-bottom compliance culture that is well communicated by senior management so that all staff members understand their compliance responsibilities. Clear lines of communication and authority help avoid conflicts of interest."[64] Policies and procedures are only effective if personnel understand who is responsible for implementation and who is in charge of monitoring ongoing concerns.

[62] NASD Notice to Members 04-71 (October. 2004), available at http://www.nasd.com/web/groups/rules_regs/documents/notice_to_members/nasdw_011633.pdf.
[63] IOSCO Report on Compliance Function at Market Intermediaries supra note 52 at p. 7.
[64] Basel Paper on the Compliance Function in Banks supra note 50 at p 12.

Role of Board of Directors and Senior Management

The board of directors and senior management may delegate day-to-day compliance operations, but still need to be informed and manage compliance issues. Regulatory guidance states that senior management must oversee the scope and structure of compliance and understand the regulatory and compliance risks impacting the organization. Clear lines of communication among the business units, compliance professionals, and senior management should be established. Ongoing reports and assessments of the program must be provided to senior management and processes to escalate and resolve material issues or breaches must be in place.

Senior executives have numerous responsibilities in relation to compliance. Under acts such as Sarbanes-Oxley, top executives must certify to the accuracy of financial statements and effectiveness of internal controls. The SROs have formalized senior management involvement by requiring that certifications and annual reports on compliance are provided to senior management and the board (See NASD Rules 3012 and 3013, and NYSE Rule 342). Similar regulations in place for broker-dealers require formal interaction between senior management and the chief compliance officer.[65]

Senior executives must account for compliance and legal risks when conducting business operations. As a result, senior management has taken on more responsibility in monitoring the compliance officer and the compliance department. According to an *American Banker* survey, among those firms that have a chief compliance officer, nearly 42% have that individual reporting to the CEO.[66] In addition, an increasing number of compliance officers are reporting directly to the board or the audit committee.

There is some confusion about the level of involvement of the board of directors in the compliance area, especially in terms of what policies and procedures must be approved by the board. Some rules specifically state that a board must approve compliance policies and procedures.[67] However, in other instances, the regulatory guidance is unclear. As a result, many compliance policies and procedures are approved by the board as a defensive measure and not due to regulatory requirements. There appears to be a need for additional regulatory guidance to clarify when board action is required in relation to compliance policies and procedures. According to one former general counsel of a diversified financial institution, there are between 300 and 400 references in the Bank Holding Company Supervision Manual alone that require reports to boards of directors or board approvals of policies and procedures. If boards of directors were held to each one of these requirements, it would have a significant impact on their ability to function. Relevant guidance should be reviewed and updated periodically.

Risk Assessments

Key to an effective compliance program is the identification of compliance risks. Risk assessments and testing ultimately involves more than a checklist approach. A risk assessment is an evaluation of the firm's vulnerability to breaches of legal and regulatory standards. When undertaken for the first time, it involves a painstaking inventory of products, procedures, and policies, department by department, and a mapping of those products, procedures, and policies against their corresponding legal and regulatory requirements. In best-of-breed companies, this process is elevated to include measurement against industry best practices as well.

There are several ways that a financial institution can assess compliance risk across an organization. A financial institution may develop regulatory risk matrices that review what regulations apply to its overall business. Compliance matrices by business line are often used to determine what areas need additional controls and monitoring. These matrices

[65] NASD IM-3013 (applicable to broker-dealers) (November 2004).
[66] See Garver, supra note 20.
[67] E.g., Investment Company Act Rule 38a-1 specifically states that fund boards must approve compliance policies and procedures of each investment adviser, principal underwriter, administrator, and transfer agent of the fund, which approval must be based on a finding by the board that the policies and procedures are reasonably designed to prevent violation of the Federal Securities Laws by the fund.

list the relevant regulations impacting the business and the procedures, controls, and testing needed to handle those risks. Similar matrices may be established for vendors and other third parties with whom firms have business relationships. As a best practice, these matrices rank the risks associated with these activities and an institution will evaluate internal controls, policies and procedures, and testing and training based on risk ratings. Higher risks require additional due diligence, controls, and testing. Gaps in controls are evaluated and addressed on an ongoing basis.

Financial institutions should be diligent when reviewing risks associated with new customers and products. Several factors may be reviewed, such as customer profiles, transaction volumes and trends, product type/complexity, and relevant laws and regulations. Defining high, medium, and low-risk customers and transactions allows institutions to determine what types of controls are required and helps establish an institution's risk appetite when soliciting new clients and products.

Policies and Procedures

Strong policies and procedures set the tone for a compliance program. One of the most important compliance policies is the code of ethics or code of conduct, which outlines the organization's overall attitude toward compliance and makes employees aware of these guidelines. The code of ethics need not reference any specific legal requirements; however, it should be sufficiently specific and exhortatory as to convey the firm's attitude toward compliance and ethical behavior. Compliance policies, in contrast, should include all relevant legal and regulatory requirements. In general, written policies are necessary to outline specific guidelines and ensure that roles, responsibilities, and business rules are transparent. The roadmap for drafting compliance-related polices may come from the business unit and from regulatory risk matrices that outline applicable laws and regulations as well as associated risks and controls. In an enterprise-wide program, regulators stress that policies must be consistent across business lines and geographic jurisdictions (unless otherwise permitted under local laws). All policies should be supported by business unit procedures tailored to the individual functions. Policies need to be continually updated to address changes in regulations and business functions, and to ensure there are no gaps between compliance risks and related controls.

Regulators have stated that a frequent examination finding is that firms have good procedures, but don't follow them.[68] To be effective, policies must be backed up by front line procedures and both must be enforced. Violations of policies and procedures should be quickly identified, investigated, and dealt with appropriately. In addition, exceptions to policies should be weighed carefully against the potential impact on the effectiveness of the policy's intended purpose and results. Institutions should adapt policies to account for changes in the industry, new legislation/regulation, evolving business practices and new customer relationships. According to SEC Director of Enforcement Linda Thomsen, "this task requires constantly looking out for potential conflicts of interest and weak points in your policies and procedures, and exploring ways in which people might try to game the system, subverting the rules and standards to which they are subject. In other words, your program must be proactive, not just reactive."[69]

Tracking New Regulations and Regulatory Changes

Another element of an effective compliance program is the ability to keep abreast of regulations. Regulators have stated that institutions should be proactive and anticipate regulatory expectations and current topics. Former Federal Reserve Governor Susan Schmidt Bies stated that compliance programs should "constantly assess evolving risks when new business lines are added, when existing activities and processes are altered, or when there are regulatory changes."[70] Former Federal Reserve Governor Mark Olson stated, "To prepare for what may be ahead, organizations should not only draw on past experience, but employ quantitative and qualitative scenario analysis and planning."[71] Officials from the SEC agree that "the identification of compliance risks and corresponding changes to the compliance system should be a dynamic process designed to ensure that the firm's compliance controls remain responsive to changes in laws as well as in the activities of the firm."[72]

Former Federal Reserve Governor Mark Olson stated, "To prepare for what may be ahead, organizations should not only draw on past experience, but employ quantitative and qualitative scenario analysis and planning".[71]

In a rapidly changing regulatory environment, financial institutions have a greater need to remain informed in order to ensure compliance policies and procedures are effective. This can be accomplished by creating a system to track regulations in a central database, interpret the impact of these laws, and map them against current policies and procedures to determine if changes are needed. Compliance executives may choose to coordinate with in-house or outside counsel to receive updates and interpretations on new laws. An organization's examiner-in-charge or primary supervisor is another valuable resource for advice and guidance on regulations. Compliance professionals may choose to become engaged in industry trade associations or other groups that provide information and have resources to interpret new rules. This includes becoming involved in the front end of the rulemaking process and offering input on proposed rules as well.

Oversight and Monitoring

Corporate compliance departments are required to have strong oversight and monitoring of the compliance program. This includes reviewing risks associated with all products, customers, and transactions as well as ongoing compliance with policies, procedures, and controls. Compliance best practices require risks to be continually identified and ranked on an ongoing basis and the areas with the highest risk be given the greatest attention. In addition, the compliance function reviews testing results to determine areas of concern.

The goal is to be able to advance business objectives while meeting legal and regulatory requirements. This requires compliance to partner with business and not act as an obstacle to operations. Compliance's role is to advise business supervisors who may need assistance in determining whether or not to effect a transaction. The objective of oversight and monitoring is to identify areas where controls are needed and to promptly identify, escalate issues to senior management, and rectify any areas that may indicate a regulatory breach. Monitoring involves a continuous review of compliance personnel and systems. Compliance professionals and senior management use analyzed data to detect trends and identify areas where additional resources, controls, or training is needed due to systematic weaknesses in the program.

Escalation of Issues and Investigations

The ability to escalate issues to an independent party strikes at the integrity of a compliance program. Firms should have formal procedures for escalating internal compliance issues and customer complaints. Issues are to be escalated as soon as possible. Employees within the business lines must be able to raise issues with an independent compliance

[68] Lori A. Richards, Director, SEC Office of Compliance Inspections and Examinations, remarks before the National Society of Compliance Professionals 2004 National Membership Meeting: Instilling Lasting and Meaningful Changes in Compliance (October 28, 2004), available at http://www.sec.gov/news/speech/spch102804lr.htm

[69] SEC Director of Enforcement Linda Chatman Thomsen remarks before the ALI-ABA Course of Study SEC/NASD Compliance (June 17, 2005), available at http://www.sec.gov/news/speech/spch061705lct.htm

[70] Susan Schmidt Bies Remarks at the Financial Women's Association Washington, D.C. Briefing, supra note 30.

[71] Federal Reserve Governor Mark W. Olson remarks at the Fiduciary and Investment Risk Management Association's Twentieth Anniversary Training Conference, (April 10, 2006), available at http://www.federalreserve.gov/BOARDDOCS/SPEECHES/2006/20060410/default.htm.

[72] See Gadziala, supra note 57.

Audit must operate independently of the business lines and the compliance function.

officer and have the ability to call an anonymous ethics hotline. In turn, the compliance officer must be given authority to report issues directly to the board or audit committee without interference from senior management.[73] If issues are escalated, prompt corrective action should be developed and documented.

Escalation procedures will produce matters deserving further scrutiny. Internal investigations must be thorough and well-documented. It is in the best interest of the compliance function to communicate issues to regulators. As evidenced in the Federal Sentencing Guidelines, the McNulty Memorandum, and the SEC's Seaboard factors, self-reporting and escalation of issues plays a pivotal role in how examiners review an institution's compliance program.

In relation to investigations and inquiries by regulators and other government authorities, compliance departments will often work with the legal department and other groups to investigate the incident and prepare a report for senior management and the regulators (if appropriate). Part of this inquiry could include a review of whether the activity in question was appropriate and whether the policies, procedures, and controls were effective. Compliance may perform some additional testing in these areas or request internal audit to conduct a review to validate systems. Compliance should coordinate providing information related to investigations to regulators and create action plans for prompt corrective action.

Testing and Validation

Testing is necessary to detect and correct compliance weaknesses. Regulators require that all elements of a compliance program, including policies, procedures, systems, and people are tested on an ongoing basis. Testing can occur at a high level, including a review of monitoring and oversight, or can be done on individual transactions. Similar to the examiners' supervisory approach, testing should be risk-based and place additional emphasis on those higher risk areas or areas where unusual activity is detected.

Several layers of testing may exist in any organization. Testing should begin at the business line level with self-testing. Self-testing is a tool to demonstrate the effectiveness of controls and gets each employee to understand these controls and be accountable for the controls' effectiveness. A risk assessment may be performed to rank the risk of each business unit and determine the level and frequency of self-testing. If the risks are high, the scope of testing will be broad and occur more often throughout the year. Self-testing procedures should be consistent across the organization, well documented, and be presented to senior management. Work papers from self-testing (and all testing for that matter) are useful for internal audit and regulators who will subsequently review similar controls within the business unit. The compliance function is responsible for reviewing and validating self-testing. Compliance departments monitor and identify key risk areas that need additional testing either by the business line, compliance, or audit. Compliance validates any corrective actions taken by the business line as a result of the self-testing process.

The role of internal audit in testing compliance risks is crucial. As the Basel Committee stated, "compliance risk should be included in the risk assessment methodology of the internal audit function, and an audit program that covers the adequacy and effectiveness of the bank's compliance function should be established, including testing of controls commensurate with the perceived level of risk."[74] The role of internal audit is similar for any diversified financial institution. Audit must operate independently of the business lines and the compliance function. The scope of testing should be comprehensive and include an evaluation of ongoing compliance with laws, regulations, and applicable industry best practices. The scope should also include a review of the adequacy of policies, procedures, controls, adequacy of training programs, and an analysis of compliance's monitoring of these elements. The scope may be adjusted based on the company's size and risk profile. Internal audit will share its results with senior management, board of directors, and audit committees. The compliance function is responsible for ensuring that corrective actions on audit findings are properly tracked and monitored. Regulatory agencies, such as the SEC and others, review corrective action taken by management on audit findings during the course of their examinations and investigations.

Regulatory examiners often rely on the work of internal audit. For example, in the course of broker-dealer examinations, the SEC has begun a new process of leveraging off internal audit departments when conducting risk management examinations.[75] In gauging the effectiveness of internal audit, the SEC assesses the internal audit charter as well as "qualification and expertise of audit management and staff, the adequacy of resources and systems, the independence and authority of the internal audit department, and the adequacy of audit coverage throughout the organization, with a focus on risk management audits.[76]

In addition to self-testing, compliance testing and internal audit reviews, organizations may wish to use external auditors to further review and validate procedures and controls. Due to limited resources, smaller organizations often outsource the internal audit function.

Training and Awareness

Compliance policies are only effective if properly communicated and understood at the staff level. Training programs may include annual training for key compliance areas as well as additional training for areas with the greatest risk exposure. Regulators require that training programs be reviewed and updated based on regulatory and business changes.

Training can be offered during corporate orientations and via on-line, web-based programs, but must be ongoing as well. Companies may consider utilizing newsletters, intranet communications, distance learning, email, and other forms of communication. Some training programs may be tailored toward the business level to provide additional guidance on the applicability of policies and procedures. All training should be documented and participation tracked accordingly. There is no reason why compliance training and instruction regarding business procedures cannot occur simultaneously so long as appropriate stress is placed on compliance.

Regulatory Examinations

Regulatory examinations are a litmus test for the effectiveness of an organization's controls, at least in relation to a certain point in time. Poor ratings and findings can lead to fines and sanctions. One of the roles of corporate compliance is to prepare business lines for examinations. This can be done throughout the year by implementing the elements of an effective compliance program. Compliance departments need to ensure that business lines have been properly tested prior to examinations; either through self-testing, internal audit, or by the compliance department itself. Any comments from testing, or from prior regulatory examinations, must be addressed and corrective action taken. A gap analysis should be performed to determine if additional action is needed.

The compliance department is the central coordinator during examinations. Compliance schedules meetings and handles requests for information and other inquiries from regulators. Compliance discusses examination findings with management and determines corrective action. All regulatory comments must be tracked in a central database and updated periodically.

[73] Basel Committee on Banking Supervision Paper, supra note 50 at p. 5.
[74] Id at p. 8.

[75] Mary Ann Gadziala, SEC Associate Director, Remarks at the Annual Conference of the Internal Auditors Industry Association: A Regulatory View – Broker-Dealer Internal Audit/Compliance Priorities, 2006 Annual Conference of the Internal Auditors Industry Association, Fort Lauderdale, FL (October 17, 2006), available at http://www.sec.gov/news/speech/2006/spch101706mag.htm
[76] Id..

The perspective of regulatory agencies has changed when it comes to examinations and should be taken into account by compliance departments when preparing for supervisory examinations. Most financial regulators take a risk-based approach during examinations. Regulators either focus on substantive areas that pose the greatest risk for all institutions based on prior experience (i.e. AML, market trading, financial accounting, sales practices, etc.) or examiners review risks across an organization based on factors such as size, customer base, geographic location, and previous regulatory history. In the end, regulators use all examinations as "roadmaps for future exams – focusing on reviews in areas where controls are weak or lacking."[77]

Strong Rapport with Regulators

Ongoing communication with regulatory officials is vital to the success of a compliance program. It is important that regulators understand an organization's business model and compliance program. In turn, compliance officers should fully comprehend regulators' expectations, especially prior to examinations or when there have been significant regulatory changes that may impact a firm's business.

Compliance executives have stated that regulators are a good resource for benchmarking information and other expertise. Compliance officers should therefore be proactive and contact regulators if there is a question prior to conducting a transaction or establishing a new customer relationship. In addition, compliance officers may consider providing periodic reports to supervisory authorities on the compliance program regardless of whether they are required to do so by statute.

One of the compliance function's main duties is to coordinate all information that is provided to regulators as part of investigations, examinations, or routine requests for information. It is also important for compliance executives to promptly self-report any issues identified as a potential problem area and to establish corrective action for regulators. However, it is noted that the culture for self-reporting problems varies with banking being more collaborative *vis-à-vis* its regulators than securities. As the McNulty Memorandum suggests, government officials give positive weight to prompt disclosures of wrongdoing as well as cooperation during government investigations.[78] Compliance departments will often have more difficulty if they do not fully cooperate, or if the issue is not reported but later found during the course of an examination. Maintaining a strong relationship with regulators will give institutions the ability to work through these issues.

Accountability

It is somewhat difficult to measure the effectiveness of compliance programs and determine accountability at the individual and institutional level. On a business line level, regulators have suggested a scorecard approach and periodic reporting to management on how the controls are working. This can be handled through the use of a heat map which includes designations such as red (significant issues that need corrective action), yellow (areas of concern), or green (adequate procedures) respectively. Regulators have suggested that employees' performance reviews include a line for effective compliance. Regulators have stated that compensation and bonuses should be tied to the ability of employees to follow company compliance policies and procedures.[79] This creates accountability throughout the organization in relation to compliance.

Although corporate compliance oversees the program, business units ultimately own compliance and are responsible for its effectiveness. Compliance partners with business to help achieve the goal of earning revenue for the organization.[80] This means that compliance has a role in working with business units in product development and new business opportunities before they become a potential compliance risk.

[77] Mary Ann Gadziala, SEC Associate Director, Remarks before the 5th Annual Regulatory Compliance Conference for Financial Institutions: Strengthening Investors Confidence Through Sound Compliance and Risk Controls, 5th Annual Regulatory Compliance Conference for Financial Institutions, Toronto, Canada ,(September 24, 2003), available at http://www.sec.gov/news/speech/spch092403mag.htm.

[78] See McNulty Memorandum, supra note 45 at p. 14.

[79] Federal Reserve Governor Mark W. Olson speech to The Financial Services Roundtable and the Morin Center for Banking and Financial Services Compliance Conference, Washington, D.C., supra note 25.

[80] See Deloitte White Paper, Global Financial Services Industry Outlook, Shaping Your Strategy in a Changing World (April 21, 2006) at p. 10.

Adequate Resources and the Use of Technology

Management is tasked with determining what resources are necessary to minimize regulatory and compliance risks. This includes personnel and systems. Management must be committed to allocating significant resources to the effort. As previously noted, these expenses are often a large percentage of a company's revenue. Management must find people with the proper level of expertise in each business and geographic location in which the company operates. Compliance executives must ensure that these resources are distributed efficiently and that roles and responsibilities are defined and understood.

It is often difficult to find the right balance of manual versus technological solutions for meeting compliance objectives. Because of the risks, complexity and globalization of organizations, technology has become a useful tool for compliance. Technology can be used to create databases, monitor transactions, review trends, and issue information reports to management. Technology may also be used to reach areas not previously accessible to compliance and track trends in the compliance function. One compliance executive interviewed for this study outlined how technology has bolstered his company's compliance program. This broker-dealer recently purchased a program that could monitor transactions to determine if the purchase of a security deviated from the customer's stated investment objectives and therefore created a potential violation of broker-dealer suitability rules. If a deviation is found, the transaction is flagged and a report is generated for compliance to review. Compliance executives also reported many similar effective software programs used to monitor customers and transactions for anti-money laundering purposes and to evaluate internal controls as required under the Sarbanes-Oxley Act.

There are issues, however, associated with technology. In light of significant merger and acquisition activity, in some cases multiple systems are being used which creates overlap and inefficiency. In addition, there are challenges in updating legacy systems to meet new and updated regulatory requirements. Systems are inefficient if not used correctly and if staff is not trained on proper implementation. Systems can create gaps in compliance programs if not properly managed. Often, systems are not able to interpret data as well as individuals. In addition, systems are costly and are prone to technical errors that can create additional risks. Business continuity planning and redundancies are critical when dealing with technology that is associated with compliance.

Rules-based regulation promotes a "check the box" mentality toward compliance. This frame of mind glorifies technical compliance over substantive compliance.

Staff Expertise

Acquiring the intellectual capital required to implement compliance programs is essential. According to the Basel Committee, compliance function staff should have the necessary qualifications, experience, and professional and personal qualities to enable them to carry out their specific duties.[81] These duties include an understanding of compliance laws, rules, and standards that impact a financial institution. Most regulators not only review a compliance

[81] Basel Committee on Banking Supervision, Compliance and the Compliance Function in Banks, supra note 50 at p. 13.

program, but the individuals implementing the policies and procedures. Therefore, companies should exercise extreme due diligence in the hiring process. This includes formal background checks and other procedures to ensure the integrity of potential candidates.

Hiring the right people is difficult in the current environment because of the competitiveness of these positions and the lack of qualified individuals available. As former Federal Reserve Governor Mark Olson stated, there is a "war on talent" when it comes to compliance professionals.[82] Financial institutions have hired former regulators and individuals with other specific talents to fill the void; however, since this area is developing so quickly, the number of truly qualified individuals is small. Financial institutions should attempt to attract talented persons who not only understand rules and regulations, but have a firm grasp of the business lines they are monitoring.

It is also helpful to attract resources with knowledge of technology. Compliance staff must possess the requisite training needed to perform the job. Financial institutions have developed programs to ensure gaps in knowledge are addressed by continuing education and training of compliance staff.

Finally, regulators review financial institutions to ensure they have adequate resources to carry out their mission. The number of personnel varies depending on the size and complexity of the firm. Companies perform ongoing risk assessments to ensure that they have the proper number of staff with adequate expertise to execute the compliance plan. Staffing presents challenges at all levels. Larger, complex firms require more staff with a higher degree of regulatory knowledge. Smaller institutions, subject to many of the same regulations, have a significant compliance burden due to the lack of in-house resources. Many times compliance officials in smaller organizations also have other responsibilities. In an effort to meet these challenges, both small and large firms outsource some of the key functions. Regulators have stated that certain functions may be outsourced; however, the compliance officer, senior management, and the board of directors remain responsible for compliance with applicable laws and standards and should maintain supervision and oversight of the outsourced functions.[83]

[82] Federal Reserve Governor Mark W. Olson speech to The Financial Services Roundtable and the Morin Center for Banking and Financial Services Compliance Conference, Washington, D.C., supra note 25.

[83] Basel Committee on Banking Supervision, Compliance and the Compliance Function in Banks, supra note 50 at p. 15.

VII. Recommendations

Inconsistent regulations and uncoordinated supervisory practices across borders and sectors diminish regulatory efficiency and create unnecessary burdens for both regulators and firms.[84]

There are several areas of concern in the current regulatory environment, most notably the impact of regulations and enforcement on the competitiveness of U.S. financial institutions in international markets. Strong regulation and enforcement is important for consumer protection and to ensure the integrity of U.S. financial markets. Based on the recent corporate scandals, there is clearly a need to maintain diligence in these areas. However, excessive and duplicative regulation and enforcement can stifle competitiveness.

Recent studies have highlighted several areas of concern in the current regulatory environment, most notably the impact of regulations and enforcement on the competitiveness issue. All agree that strong regulation and enforcement is important for consumer protection and to ensure the integrity of U.S. financial markets. Corporate scandals have demonstrated the need to maintain diligence in these areas. However, excessive and duplicative regulation stifles competition and impedes the very objectives that regulation seeks to achieve. The authors of this paper endorse many of the recommendations of recent studies including those in the report published by the Commission on the Regulation of U.S. Capital Markets in the 21st Century, the *Interim Report of the Committee on Capital Markets Regulation,* the Bloomberg-Schumer report on *Sustaining New York's and the U.S.'s Global Financial Services Leadership,* and the GAO report, *Financial Market Regulation, Agencies Engaged in Consolidated Supervision Can Strengthen Performance, Measurement, and Collaboration.*

Regulatory overlap and inconsistent approaches to regulation have placed a burden on the financial services industry in general and the compliance function in particular. These burdens are compounded by the conflicting missions of regulatory bodies and the differing attitudes that regulators display both inter-agency and intra-agency. The result of this conflict is high compliance costs and significant risks associated with noncompliance.

The goal of the recommendations below is to demonstrate how the compliance function could benefit from changes in regulatory and enforcement practices as well as to set forth proactive measures that can be taken to achieve efficiencies and, more importantly, regulatory harmony. It is recommended that:

1. There be an overall harmonization of similar regulatory missions
2. Current enforcement practices of federal and state authorities be revamped
3. An attempt be made to bridge the gap under the current regulatory structure in order to harmonize the regulator and industry approaches toward compliance
4. Institutions should create a culture of compliance that extends beyond the current rules and regulations and encompass industry "best practices" and "business rules."

A. Harmonize the Missions of All Financial Services Regulators

Regulation of financial services institutions is complex and multi-layered. Despite the passage of GLBA and the genesis of diversified financial institutions and functional regulation, financial institutions are still subject to supervisory review by multiple federal regulators and state agencies, including four banking regulators, the SEC, self-regulatory organizations, state banking, securities, insurance departments, and state attorneys general, among others. Each agency has its own mission and culture. These differing missions and cultures were tolerable during an era when the industry was Balkanized. The differences are counterproductive and anti-competitive, however,

[84] Institute of International Finance, Inc., Proposal for a Strategic Dialogue on Effective Regulation, (December 2006) at p. 6.

now that previously separate businesses have converged under one corporate roof.

Among the federal bank regulators, the FDIC is concerned with protecting the insurance fund supporting deposits of institutions while the Federal Reserve, for which bank regulation is a secondary responsibility, analyzes the safety and soundness of institutions and the banking system in general. The SEC's goal, in contrast, is to protect investors and promote capital market efficiency. These contrasting regulatory missions produce staffs and internal cultures that reflect their missions. The Federal Reserve, for example, employs more economists in its role as central banker while the SEC employs more attorneys in its effort to enforce securities laws. Despite these differences, there is common ground in principles that can apply to all regulators.

Establish High Level Principles

As the Bloomberg-Schumer Report suggests, there should be a shared vision for financial services and a set of supporting regulatory principles similar to the approach taken by the Financial Services Authority (FSA) in the United Kingdom.[85] U.S. regulators should consider moving toward principles-based regulations similar to the approach taken by the FSA. The FSA's website states the following: "The FSA's intention behind a move towards a more principles-based approach is to achieve better treatment of customers through firms' own initiatives and actions. As a regulated firm you will be given greater flexibility to decide how to meet your regulatory responsibilities. This means you will have more discretion in how you do your business."[86]

Rules-based regulation promotes a "check the box" mentality toward compliance. This frame of mind glorifies technical compliance over substantive compliance. It has been said, for example, that it is this lack of attention to substantive issues that allowed market timing and late trading practices to take hold in the mutual fund industry. Compliance departments should proactively manage and assess risks across the organization, rather than reviewing for potential individual violations of the law. Although it is important to understand the regulations and the laws that impact business, there should be a level of flexibility that enables institutions to innovate and evolve. Principles-based regulations allow institutions to accomplish this objective.

On April 17, 2007, the U.S. Supreme Court ruled in Watters v. Wachovia Bank, N.A., upholding federal preemption of state laws with respect to operating subsidiaries of national banks.

Reconstitute and Empower the Federal Financial Institutions Examination Council and President's Working Group on Financial Markets

The Federal Financial Institutions Examination Council (FFIEC) is a formal interagency body, established in 1979 to prescribe uniform principles, standards, and report forms for the examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS), and to make recommendations to promote uniformity in the supervision of financial institutions. Its powers are severely limited and its membership is restricted to bank and credit union regulators only. In 2006, the State Liaison Committee was added to the FFIEC as a voting member.

To date, the FFIEC has largely served as a forum for voluntary collaboration among bank regulators. There are some recent examples that have proven how coordination among regulators within the FFIEC and beyond has benefited the industry and the compliance function. In June 2005, the FFIEC released the Bank Secrecy Act/Anti-Money Laundering Examination Manual.[87] The goal of the manual was to ensure the consistent application of the BSA to all banking organizations, including commercial banks, savings associations, and credit unions. Empirical evidence, such as reduced SAR filings and enforcement actions against financial firms for AML violations, demonstrate the effectiveness of the FFIEC model. In another example of inter-agency collaboration, the federal banking regulators and the SEC, at the specific direction of Congress, combined efforts to propose a rule that details which securities activities can be conducted directly by a bank and which activities must be "pushed out" to a broker-dealer affiliate.[88] Prior to coordination of efforts among the SEC and banking regulators, this rule had been in limbo for over six years since the passage of the GLBA.

We believe that if properly reconstituted and empowered by Congress, the FFIEC could serve as the essential vehicle for the harmonization of the U.S. financial services regulatory system. For it to succeed in this new and expanded mission:

1. The FFIEC's membership would be expanded to include the SEC, major SROs, and the National Association of Insurance Commissioners
2. It would be charged legislatively with reconciling conflicting regulatory actions.

The FFIEC, as reconstituted, should be the driving force behind effective changes in financial services regulation as outlined above. The FFIEC could establish the aforementioned core principles for the financial services industry and create a singular purpose for financial services regulators. To ensure it is fulfilling this purpose, the FFIEC should be subject to Congressional oversight or report directly to the President's Working Group on Financial Markets (PWG).

Bank examiners have complete and total access to the books and records of the bank being examined, while SEC examiners' access is considerably more limited.

President's Working Group on Financial Markets

The PWG could be a useful forum to review the coordination efforts between financial regulators and settle differences that exist among these agencies. The PWG should oversee and work with groups such as the FFIEC in an effort to establish core principles for the financial services industry and create a singular purpose for financial services regulators.

[85] Michael R. Bloomberg, and Charles E. Schumer, Sustaining New York's and the US' Global Financial Services Leadership, supra note 12 at p. 82.
[86] See generally, www.fsa.gov.uk

[87] See FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual InfoBase, www.ffiec.gov/bsa_aml_
[88] Proposed Regulation R, 12 CFR Part 218; 17 CFR Parts 240 and 247; Securities and Exchange Act of 1934— Broker Exemption for Banks; Proposed Rules and Notice (12/26/06).

The Commission on the Regulation of U.S. Capital Markets in the 21st Century recommended that the PWG take the following actions:

- Develop a unified, coherent vision for the financial sector and a more efficient unified regulatory structure
- Develop a comprehensive, forward-looking strategy for the sector and its regulation
- Develop a set of shared values to support the vision and drive the strategy
- Develop mechanisms and policies regarding the U.S. interaction with foreign markets and regulators
- Define the relationship between federal and state jurisdiction in different aspects of the U.S. capital markets
- Develop a blueprint for a modern U.S. financial services regulatory regime that will ensure our markets remain competitive and globally attractive. [89]

In its oversight role, the PWG should review how regulation and enforcement practices affect financial institutions' business planning and competitiveness in world markets as well as the potential impact on consumers, business conduct, and the compliance function within financial firms.

Review and Update Prescriptive Rules

In some instances, there is clearly a need for prescriptive rules. In other instances, regulations are outdated due to the complexity of firms, the role of technology, or other factors. Examples of overly prescriptive areas of regulation include exemptions from the Investment Company Act of 1940, allowance for loan and lease loss calculations for banks, Basel II capital rules, and the Community Reinvestment Act.

It is recommended that regulators perform a more effective cost-benefit analysis on all current and proposed rules to reassess the original purpose of the rules and determine the rules' impact on institutions, consumers, and the market. In addition, rules should be reviewed periodically to assess the level of burden they place on covered firms. Some rules, especially those with the most direct impact (i.e., Sarbanes-Oxley Act and the Bank Secrecy Act) should be reviewed more often and include input from the industry. Finally, regulators should consider reducing the volume of regulations or at least controlling the pace of new regulations to ensure current regulations have been sufficiently implemented prior to releasing additional regulations.

Prudential regulation would require the SEC to examine its culture and personnel.

Create Uniform National Standards Where Appropriate and Move Toward a More Productive Form of Federalism

The marketplace for most financial services products, even at the retail level, is national and in many instances global. Yet the impact of inappropriate or illegal activity is felt most intensely at the local level (witness the fall-out from recent subprime mortgage lending activities). Local enforcement officials are generally more sensitive to corporate wrongdoing and its consequences. However, local officials, when prompted to action, tend to be less cognizant of the systemic consequences of their enforcement actions than are their federal counterparts. Moreover, financial firms themselves, mindful of reputational issues, are wary of challenging local actions. The result is often a toxic brew of misguided settlements, regulatory one-upsmanship, and an obfuscation of the original goals of regulation. The OCC's unilateral action in asserting its plenary authority over national banks has tended to aggravate this situation. On April 17, 2007, the U.S. Supreme Court ruled in *Watters v. Wachovia Bank, N.A.*, upholding federal preemption of state laws with respect to operating subsidiaries of national banks. While clarifying the legal position of one segment of the financial services industry, the ruling does not further the goal of industry-wide harmonization.

[89] Commission on the Regulation of U.S. Capital Markets in the 21st Century, Report and Recommendations, supra note 12 at p. 118-119.

It is in the long term interest of the U.S. that Congress develops a systemic solution to this problem. The elements of any such solution should:

- Take advantage of the resources, sensitivities, and intelligence that local authorities offer
- Recognize the national scope of the marketplace for most financial services products. There are some areas where complying with laws in multiple jurisdictions creates challenges for financial institutions. Congress should consider creating uniform national standards where necessary to eliminate the inefficiency of complying with multiple and often vastly different standards. For example, pre-empting state privacy laws would provide firms one uniform set of privacy laws versus the numerous state laws that institutions must comply with at this time. National standards should be at a level that provides adequate protection to the consumer.
- Provide for an optional federal insurance charter to further modernize this segment of the financial services industry. Changes in the size and complexity of insurance firms, along with the removal of various barriers post-GLBA, have made this legislation necessary. The compliance function within insurance companies faces cost burdens and operational challenges under the current regulatory regime. There is also a regulatory disparity between banks conducting insurance activities which are not subject to similar requirements and restrictions as insurance companies. An optional federal insurance charter would provide insurance companies with the ability to conduct business more efficiently across all fifty states.

B. Review Enforcement Practices of State and Federal Authorities

Current enforcement practices and attitudes are negatively impacting financial institutions and need to be analyzed. As the Bloomberg-Schumer Report suggests, the SEC should "conduct an assessment of the enforcement mechanisms used by federal and state regulators today, along with state and federal judiciary agencies, to improve the consistency and predictability of enforcement efforts.[90]

SEC and SRO Examination and Enforcement Practices Should be More "Prudential"

The contrast in missions and cultures among the regulatory agencies is not only reflected in the composition of the agencies' staffs, it is also reflected in the way that the regulated firms interact with the agencies that regulate them. In the banking environment, bank personnel for the most part have an open and collaborative relationship with examiners. In the securities and broker/dealer environment, however, the relationship with examiners is more strained. Investment firms have been largely critical of the SEC's and SRO's approach to regulation in that these agencies tend to react to reporting of issues by beginning enforcement actions and investigations.

The causes for this difference in attitudes are at least two-fold. First, bank examiners have complete and total access to the books and records of the bank being examined, while SEC examiners' access is considerably more limited. Second, large banks are examined at least annually and some are examined perennially while securities examinations tend to be more episodic. The upshot of these contrasting environments is that in the banking culture there is a clear understanding that problems will eventually come to examiners' attention and it is far better to reveal problems than to have them discovered by examiners. The securities and broker/dealer environment, in contrast, is less conducive to the early sharing of problems with examiners.

Recent reports have recommended that the SEC move toward a more "prudential" and bank-like method of regulation. We concur in these recommendations; however, to achieve the full effect of this change we recommend:

[90] Report on Sustaining New York's and the US' Global Financial Services Leadership issued by Mayor Michael Bloomberg and Rep. Charles Schumer, supra note 12 at p. 115.

- SEC and SRO examiners should have the same access to the books and records of the firms they regulate as do bank examiners
- Where appropriate in light of the activities of the firms they regulate, the SEC and the SROs should explicitly adopt "safety and soundness" as one of their core regulatory missions
- An examination privilege similar to that contained in the Regulatory Relief Act of 2006 should be extended to SEC and SRO examinations.

Prudential regulation would require the SEC to examine its culture and personnel. This would include hiring more economists to properly review cost, benefits, and risks associated with relevant regulations. The SEC would have to restructure its examination divisions, which would include the possibility of utilizing resident examiners. As a prudential regulator, the SEC should also seek to coordinate and communicate with the industry prior to enacting rules. The SEC and other State and Federal authorities should not operate under a "rulemaking by enforcement" mentality. As is the case with banking regulators, the rulemaking process should be a thoroughly researched, transparent, and interactive process.

Protect the Attorney-Client Privilege

As part of the review of enforcement practices, authorities must ensure that the viability of the attorney-client privilege is protected. Financial institutions should not be required to waive privilege in the course of investigations. This practice places stress on the legal and compliance departments and has a chilling effect on internal communications within a corporation. It also acts as a disincentive for companies to conduct internal investigations on compliance-related matters.

The DOJ's McNulty Memorandum is a positive step in that it requires federal prosecutors to get approval from the Attorney General's Office prior to requesting companies to disclose privileged information; however, more needs to be done. It is recommended that the SEC and other agencies draft similar guidance and controls on when and how waiver of privilege is requested. Government officials should consider safe harbors and other measures to protect internal communications and allow companies to conduct these internal investigations which may produce beneficial information.

It is also recommended that Congress act to protect SEC-regulated firms in a similar fashion as firms regulated by banking supervisors which have an examination privilege. Under the examination privilege, information shared by institutions with federal banking regulators is protected from third parties.[91] Because of this privilege, those dealing with bank regulators are confident that information provided to these supervisory authorities will be protected. This fosters better relations and communication between the industry and regulatory officials.

Coordination of State and Federal Regulators

The friction between state and federal prosecutors has been evident over the past few years. One prime example is the numerous actions brought by the New York Attorney General against securities firms. These actions were beneficial in that they brought to light and then arrested practices in the securities, investment management, and insurance industries that deserved attention. In many instances, however, the actions were taken without consultation or coordination with the primary state or federal regulators. As the Committee on Capital Markets Regulation (Committee) recently suggested, Congress should take steps to improve enforcement coordination between the federal government and the states.[92] This Committee has recommended that states act when the SEC does not, that states notify the SEC of all their enforcement actions, and that the states permit the SEC to take the lead in matters of national importance.

[91] Financial Services Regulatory Relief Act of 2006, (Pub. L. No 109-351), Section 607.
[92] Interim Report of the Committee on Capital Markets supra note 12 at p. 68.

C. Bridge the Gaps between Regulator and Industry Approach Toward Regulation and Compliance

It is recommended that compliance departments review all business practices and look beyond the law to ask not simply whether practices are legal, but whether they are in accordance with the firms' ethical culture.

Greater Coordination among U.S. Financial Services Regulators

Compliance executives interviewed for this study unanimously agreed that one of the biggest areas of concern is the redundancies associated with examination and supervision. These redundancies apply to institutions of all sizes, but especially larger, more diverse firms. As diversified financial institutions become more complex, they become subject to multiple regulatory authorities. Under GLBA, the concept of functional regulation was aimed at reducing overlap by having regulators examine specific subsidiaries based on their activities. However, there still is a need to examine institutions at the holding company level which gives multiple regulators jurisdiction over each subsidiary. In addition, certain state authorities have jurisdiction over subsidiaries in relation to business practices. This creates a climate where institutions are reviewed and investigated by multiple authorities. Unfortunately, these examinations are not coordinated and are often duplicative in nature.

In order to reduce redundancies, the Government Accountability Office (GAO) has suggested that Congress consider alternative regulatory structures, including consolidating some or all of the current regulatory agencies or having a single regulator to oversee complex, internationally active firms.[93] Even without Congressional action, there are some alternative solutions for coordination that could be considered. Since modern financial services firms use holding company structures to manage risks, it is recommended that there be additional regulatory coordination with respect to large, complex firms managing risks on a consolidated basis. On the federal level, the Federal Reserve, OTS, and the SEC currently oversee firms on a consolidated basis. The SEC has only recently begun overseeing large, complex investment firms that elected to become consolidated supervised entities under its alternative net capital rules. The SEC oversees five such entities while the Federal Reserve and the OTS oversee more than 5,600 entities on a consolidated basis.[94] The FDIC Chairman has recently called for similar supervisory authority for parent companies of Industrial Loan Companies (ILCs) which may add to the overlapping oversight.[95]

In March 2007, the GAO issued a report concerning the consolidated regulatory supervision of financial services firms' (FSFs) programs. In "Financial Market Regulation: Agencies Engaged in Consolidated Supervision Can Strengthen Performance Measurement and Collaboration" (GAO Report), the GAO reviewed the supervision programs of the Federal Reserve, OTS, and SEC (collectively, the Agencies). The GAO Report states that consolidated supervision of FSFs have become more important because firms have grown dramatically and become more complex in terms of the products and services they offer; firms increasingly operate on a global basis; and firms manage risk on an enterprise-wide basis. The policies of the three agencies that oversee firms on a consolidated basis vary because of the differences in the activities of the FSFs they oversee. For example, the Federal Reserve and the OTS focus on protecting depositors, while the SEC is focused on investor protection.

The GAO Report suggests that the Agencies improve their collaboration and exchange information concerning FSFs. The GAO states that the Agencies

[93] GAO Report, supra note 17 at p. 3.
[94] Id. at p. 12.
[95] Joe Adler, FDIC Asking for Fed-like ILC Authority, American Banker (March 23, 2007).

have made progress by coordinating examination approaches and by holding joint supervisory meetings, but this collaboration needs to be expanded. The GAO Report urges the Agencies to "take a more systematic approach to agreeing on roles and responsibilities and establishing compatible goals, policies, and procedures on how to use available measures as efficiently as possible". Furthermore, according to the report, the "U.S. regulatory system could benefit from more systematic collaboration, both between consolidated and primary bank and functional supervisors in the oversight of the largest, most complex firms and among consolidated supervisors themselves". It is evident that this type of coordination would provide benefits to the industry and is needed under the current environment. For example, the SEC does not have the experience or the staff needed to review firms on a consolidated basis. The SEC could benefit greatly from coordinating with the Federal Reserve and OTS who have the experience and understanding of the risks associated with these entities.

Attempts have been made to eliminate overlapping supervisory authority in other areas. The financial services industry has largely applauded the decision of the NASD and NYSE to combine supervision of their regulated entities. The NASD regulates more than 5,100 securities firms in the U.S. Almost 200 firms, including many of the industry's largest, are also members of NYSE and regulated by both organizations.[96] In November 2006, the two firms signed a letter of intent to combine entities. In January 2007, members of NASD approved bylaw changes needed to combine regulatory functions and form one organization to oversee U.S. securities brokers and dealers. There will be significant benefits in merging the activities of the two entities, including eliminating duplicative examinations and inconsistent rules, reducing costs associated with unnecessary overlap, and providing one clear voice for the SROs regulated firms. Among the supporters of this action was SEC Chairman Christopher Cox who said, "Eliminating overlapping regulation, establishing a uniform set of rules, and placing oversight responsibility in a single organization will therefore enhance investor protection while increasing competitiveness in our markets."

Other areas of coordination need to occur, including more communication between state and federal regulatory authorities in the course of examinations, investigations, and enforcement actions. As the Federal Reserve Consumer Compliance Handbook states, coordination with other supervisory disciplines and other regulators is sometimes warranted to ensure a full understanding of an organization's risk profile. Federal and state regulators should routinely enter into information sharing agreements and memorandums of understanding in order to effectively supervise institutions without duplication. The FFIEC could play a crucial role in facilitating cooperation among all federal and state regulatory agencies. In addition other joint forums, such as the Financial and Banking Information and Infrastructure Committee, could act as a venue for enhanced communication and coordination.

Adopt Additional Regulatory Guidance on Compliance to Provide Clarity

It is recommended that regulators continue to provide clear guidance on their expectations in relation to compliance. Transparency in relation to regulatory and supervisory expectations is crucial. As a senior regulatory official recently stated, "How can compliance professionals in the industry be proactive in identifying compliance risk issues, in implementing policies and procedures, in training employees and in giving guidance, if they have inadequate understanding of what the regulatory requirements are?"[97] More guidance on the framework for corporate governance and the compliance function would allow the industry to continue to develop programs and apply resources needed to achieve high ethical standards. Conversely, a lack of guidance will make companies more risk averse and constrain the growth of the capital markets.

[96] See NASD press release, NASD and NYSE Group Announce Plan to Consolidate Regulation of Securities Firms (November 28, 2006), available at http://www.nasd.com/PressRoom/NewsReleases/2006NewsReleases/NASDW_017973.

[97] Lori Richards, SEC Director, OCIE, remarks before the NYSE Regulation Second Annual Securities Conference, New York, NY: Transparency in Regulatory Examinations (June 20, 2006) available at http://www.sec.gov/news/speech/2006/spch062006lar.htm.

Regulators could provide more specific guidance in the following areas:

1. The role of boards of directors in approving compliance policies and procedures (in particular when policy approval is required)
2. The structure of the compliance function
3. The level and type of testing required and the appropriate division of testing responsibilities between audit and compliance
4. The proper methods to assess the compliance function.

If there are areas where regulators believe companies can be allowed discretion, that should be formally communicated. It is recommended that regulators provide additional clarity to the industry about their risk-based supervisory process and outline what elements of a compliance program are required and what elements are subject to review based on individual circumstances and potential risks. The regulators' risk-focused approach reduces burden on institutions and accounts for those areas where firms have sufficient risk controls in place. Under a risk-based supervisory program, the frequency and depth of reviews are commensurate with a financial institution's risk profile.[98]

Finally, regulators and industry compliance executives agree that the compliance function should understand and be sensitive to the business operating environment. One way to achieve this sensitivity is to redefine the role of compliance to include not just legal and regulatory compliance but compliance with the policies and procedures that drive the business, the so-called "business rules". This broadened scope of compliance would serve to improve corporate governance, make the compliance function itself more cost effective, and enhance the overall effectiveness of the compliance function. Two of the regulators we spoke with indicated that their agencies were agnostic regarding broadening the mandate of compliance in this fashion. It is recommended that the regulators send an affirmative signal that this is an acceptable practice.

The implementation of an effective compliance program should benefit a company's regulatory capital and earnings and enhance its prospects.

D. Institutions Should Promote Ethics and Integrity Beyond the Law

It is recommended that compliance departments review all business practices and look beyond the law to ask not simply whether practices are legal, but whether they are in accordance with the firms' ethical culture. Institutions should never allow practices to continue simply because it is common in the industry and someone else is doing the same thing. Good corporate governance and business ethics are necessary to ensure that financial services institutions avoid situations such as market timing. If this type of questionable activity is discovered by compliance departments, it must be dealt with promptly and reported to regulators. Compliance departments should conduct full investigations and management should hold employees responsible for their actions. In the end, if the organization has a strong compliance culture in place, these instances will be the rare exception rather than the rule.

[98] E.g., Board of Governors of the Federal Reserve System's Consumer Compliance Handbook Overview (January 2006).

VIII. Conclusion: Future of Compliance and Challenges for Financial Services Institutions

Compliance has become a risk management function which involves an assessment of legal, regulatory, reputational, and operational risks on an enterprise-wide basis.

Compliance is a vital function for all corporations. Compliance has become a risk management function which involves an assessment of legal, regulatory, reputational, and operational risks on an enterprise-wide basis. The implementation of an effective compliance program should benefit a company's regulatory capital and earnings and enhance its prospects. Conversely, the absence of an effective compliance program can lead to significant cost and reputational damage.

It is difficult to anticipate what the compliance function in diversified financial services institutions will look like in the next 10 years and beyond. The modern compliance function, which measures risks on an enterprise-wide basis, is still somewhat in its infancy. New regulations and guidance impacting compliance are continually being enacted due to external factors, including:

- Natural disasters
- War
- Acts of terrorism
- The state of the economy and the financial markets
- Technological developments
- Improper business conduct
- New or altered legal mandates

The key challenges for diversified financial institutions in the near future can be met by:

- Nurturing an ethical culture and avoiding compliance risk through a comprehensive and effective compliance program
- Diligently managing risks on an enterprise-wide basis
- Maintaining adequate staff and resources
- Being proactive and adapting to regulatory changes
- Continuously updating the compliance program and incorporating lessons learned

The financial services industry and its regulators have made significant strides in a relatively short period of time in adapting to a new compliance atmosphere. We hope that this study and its recommendations serve to draw attention to steps that will continue this trend of continuous improvement.

The Anthony T. Cluff Research Fund designs, approves, and funds research on issues affecting the financial services industry and related public policy. The results of these studies advance the policies of the Roundtable, and inform and educate opinion leaders and policymakers.

The Anthony T. Cluff Research Fund of The Financial Services Roundtable
1001 Pennsylvania Ave., NW, Suite 500 South
Telephone: 202.289.4322 | Fax: 202.628.2507
Website: www.fsround.org

THE FINANCIAL SERVICES ROUNDTABLE