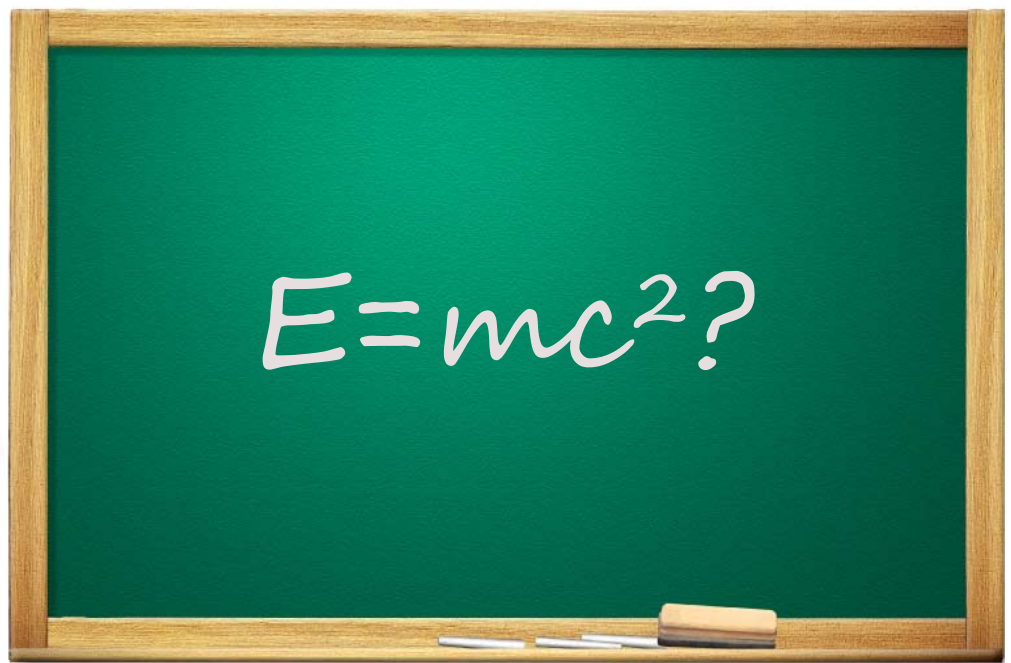


Integrated Compliance and Risk Management: Rethinking the approach



Shaping the New Financial Services Marketplace

A new financial services marketplace that's very different from the old is emerging from the credit crisis. The new market will be more transparent, simplified, standardized, and regulated with fewer intermediaries.

In this series, entitled *Shaping the New Financial Services Marketplace*, the Deloitte Center for Banking Solutions will examine the rules, regulations, and operating models that evolve as the industry sails uncharted waters. Specifically, these articles will focus on strategies for success in the new marketplace, different types of global regulatory systems, the gap between financial innovation and risk management, the burden on compliance as change occurs, and steps for integrating compliance and risk management.

In this paper, we examine the extent to which financial services firms can increase the effectiveness and reduce the costs of compliance management. Most firms can achieve both simultaneously by streamlining their compliance management while taking a risk-based, enterprise-wide approach to compliance.

Foreword



Last year, we presented the results of our survey on compliance management at major financial institutions. The study explored some of the challenges facing banks as they attempt to navigate what we called “the compliance labyrinth.” Since that time, the challenges of risk and compliance management have grown with the crisis in the financial markets and the increasing role of government and regulatory agencies. This current report reflects these changes, as well as more recent insights from the field.

What has emerged from our work is a new, more integrated approach to compliance and risk management. Such an approach encourages a complete view of risk, including the need to implement and apply compliance management across the enterprise to ensure it is truly effective and efficient. Anything less only adds to the risks the enterprise faces and the costs of operating in a more transparent and, in all likelihood, more regulated market.

We trust that the information and insights presented in this report will further discussion of compliance and risk management in your organization, and with your industry peers. The need for effective, efficient methods of compliance has never been greater and we expect that need only to intensify in the future.

Sincerely,

A handwritten signature in black ink, appearing to read 'Don Ogilvie'.

Don Ogilvie
Independent Chairman
Deloitte Center for Banking Solutions

February 2009



Executive summary

The current crisis is likely to place compliance and risk management in the forefront of the market's priorities. New regulatory requirements will compel financial institutions to rethink existing compliance programs, many of which have failed to keep pace with evolving levels of risk. Given the increased demand on compliance resources, this paper addresses the need for a fresh approach to the compliance challenge.

New regulatory initiatives are already pending. For example, the Basel Committee on Banking Supervision has proposed new measures for stronger risk protocols and improved procedures for valuing and disclosing assets, including the capital treatment of complex structured products.¹ The Senior Supervisors Group has issued a report² with observations on successful risk management practices based on a sample of leading banks and securities firms. The Institute of International Finance (IIF) has published recommendations for improvements in risk management,³ while the U.S. Treasury has recommended an overhaul of the U.S. regulatory structure.⁴ As new regulations and requirements are added, the cost of compliance continues to grow, while increased risks mean that the cost of non-compliance may be growing even more.

Today, many financial services firms conduct compliance management in silos. The likely results are redundancy, overlap and an increased burden on the business, in addition to potential non-compliance with critical regulatory requirements. Large organizations typically respond at a line of business level to jurisdictional regulatory mandates rather than globally coordinating efforts. Additionally, compliance management is often handled outside the traditional risk management process in most financial institutions. This leads to a fragmented approach that separates the management of compliance risk from management of other risks.

New regulatory requirements will compel financial institutions to rethink existing compliance programs, many of which have failed to keep pace with evolving levels of risk.

Adding further stress to an already inefficient process, the cost of compliance for many financial institutions has increased substantially. Research conducted by the Deloitte Center for Banking Solutions⁵ shows that compliance management spending for some larger U.S. financial services firms increased on average by 159% from 2002 to 2006. For these same firms, compliance management costs can be anywhere between \$200 million and \$400 million a year, representing a conservative estimate which could be understated by up to 30%. Given the magnitude of investment, even a 10% savings becomes significant. This also does not take into account indirect costs associated with line management becoming increasingly involved in compliance management.

In this paper, we examine the extent to which financial services firms can increase the effectiveness and reduce the costs of compliance. Most firms can achieve both simultaneously by streamlining their compliance and risk management while taking a risk-based, enterprise-wide approach to compliance. Based on our research and client experiences, we also provide a roadmap for financial services firms seeking to achieve a more effective outcome from their compliance management at a more appropriate cost. This approach to compliance risk management is part of Deloitte's risk intelligence philosophy.⁶

¹ Bank for International Settlements Web site, www.bis.org/press/p080416.htm April 16, 2008.

² Observations on Risk Management Practices during the Recent Market Turbulence, March 6, 2008, The Senior Supervisors Group.

³ Final Report on the IIF Committee on Market Best Practices, July 17, 2008, IIF.

⁴ Blueprint for a Modernized Financial Regulatory Structure, March 31, 2008. US Treasury Web site, www.treas.gov/offices/domestic-finance/regulatory-blueprint/.

⁵ Navigating the Compliance Labyrinth – The Challenge for Banks, Deloitte Center for Banking Solutions.

⁶ Visit www.deloitte.com/RiskIntelligence for additional information on Risk Intelligence.

Current state of compliance and risk management in financial services

Clearly a new approach is called for that brings compliance and all other risks into a framework that enables management to measure, prioritize and manage them efficiently and effectively.

The integration of compliance and risk management

In financial services, innovation in products and services has often outpaced the development of compliance and risk management capabilities. As a result, compliance and risk management remains in constant flux and risk managers must understand current risks as well as evolving ones. Defining the full extent of the risks the organization faces and how they should be managed is one of the key challenges of a senior risk executive.

Clearly a new approach is called for that brings compliance and all other risks into a framework that enables management to measure, prioritize and manage them efficiently and effectively. Such an approach must consider the full spectrum of risks across the enterprise. Defining compliance and risk management is preferably done through an enterprise-wide approach. Yet enterprise risk management in many firms remains a work in progress. A study by Deloitte⁷ of major financial firms globally revealed that only 35% of executives reported their financial institution had implemented an enterprise risk management program. Many still had significant work to do in reaching Basel II standards and only a quarter considered their operational risk management systems to be very capable in terms of reporting and data gathering.

An enterprise-wide approach does pay off. The Senior Supervisors Group report⁸ observed that during periods of market turmoil firms that had made the most progress towards implementing such an approach outperformed those that had not. Given the events of 2008, financial institutions face increasing pressure to improve compliance and risk management capabilities.

Compliance defined

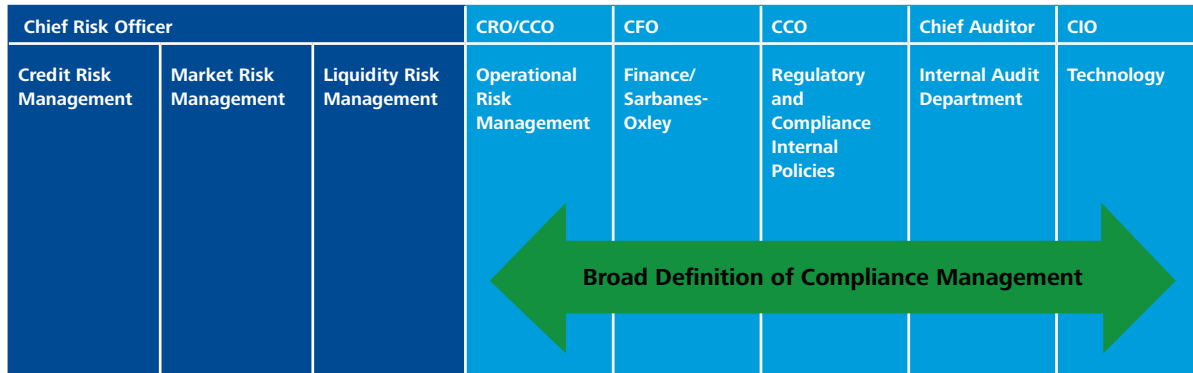
Compliance itself can be defined narrowly or broadly. For example, a narrow definition of compliance management might be compliance with all banking “laws, rules and standards” such as the USA PATRIOT Act, Basel II or the Bank Secrecy Act (BSA). A broader definition, by comparison, might include compliance with all external and internal regulations and requirements such as Sarbanes-Oxley. It might also include the separation of roles and responsibilities for accessing bank systems and encompass compliance responsibilities from operations to technology.

Exhibit 1 is an illustration of a typical financial institution’s structure. In this example, traditional financial risk management is managed by a single manager, the Chief Risk Officer (CRO), while the departments across which compliance responsibilities extend each have a manager. Compliance in the broader sense includes all activities in the light blue box. This traditional approach often results in a siloed and fragmented process that can lead to significant gaps in the compliance and risk management functions.

⁷ Deloitte Global Risk Management Survey: Fifth Edition, 2006.

⁸ Observations on Risk Management Practices during the Recent Market Turbulence The Senior Supervisors Group, March 6, 2008

Exhibit 1: An evolving definition of risk management (Illustrative)



CIO - Chief Information Officer CFO - Chief Financial Officer CCO - Chief Compliance Officer

Source: Deloitte Center for Banking Solutions

Risk management is growing in importance

The risk management landscape has undergone a seismic shift in recent years, driven by five primary factors:

- Dramatic growth in the number and complexity of risks
- Continuing consolidation and diversification of banking organizations
- Continuing globalization of the industry
- Greater scrutiny by government regulators
- Increasing business volatility with systemic implications

These factors make risk more difficult to identify and measure while magnifying the exposure and effects of unforeseen developments.

There has been serious financial market instability over the last 25 years in equities (1987, 2001 and 2007/8), currencies (Mexico in 1994 and Asia in 1997), government debt (Russia in 1998) and the failure or difficulties of various financial institutions and markets (Continental Illinois National Bank in 1984, S&L failures in 1987-89 and the junk bond crisis, Long Term Capital Management in 1998, and Northern Rock in 2007 and IndyMac in 2008). Many of these crises have been followed by a regulatory response designed to ensure that similar crises will not reoccur.

The cost of compliance

In our previously noted survey, *Navigating the Compliance Labyrinth*, we asked leading financial firms to assess their cost of compliance, how it had changed over recent years (2002-06), what their current approach to compliance management had been and how they have invested in their compliance management activities.

In summary, the results were:

- There was a 159% increase in compliance costs between 2002 and 2006
- Ninety percent of respondents said their compliance information was not timely enough and 85% said it was not always comprehensive enough
- Seventy percent of respondents agreed that there had been a greater demand for public transparency around compliance activities and they expected that trend to continue over the next three to five years. Eighty-five percent of respondents expected penalties to continue to rise
- Most of the increase in compliance costs has come through compensation costs implying that most institutions have responded to increased compliance responsibilities by adding more people to rather, than through process improvement and technology. This is also reflected in a substantial growth in administrative and management costs (See Exhibit 2.)

Penalties

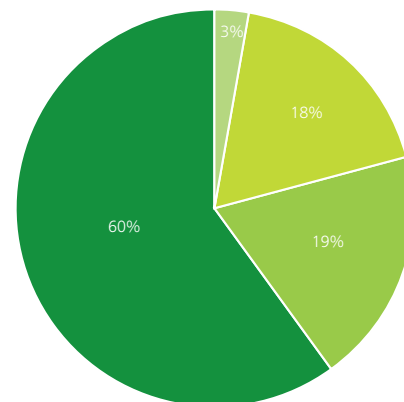
To provide further “incentives,” regulators have turned to warnings, censure, dismissal from the industry and even penalties to force financial institutions to implement stronger risk management and compliance systems. In such circumstances, fines imposed at a federal level can be dramatically increased by the impact of state and other government agencies.

Between 2000 and 2007, the Federal Reserve Board and the Office of the Comptroller of the Currency (OCC) imposed civil penalties on over 350 banks for more than \$450 million. While many of these penalties represent failures concerning of money

laundering activities more than issues concerning market dislocation, they nevertheless represent compliance issues. Fourteen of these cases could be defined as high profile, with fines varying between \$5 million and \$100 million.⁹ More than 3,500 actions have been taken by the OCC alone during this period. Since 1998, the Department of Housing and Urban Development (HUD), at first an unlikely bank regulator, has imposed fines of at least \$57 million in more than 290 actions against mortgage lenders focusing on fraudulent lending activities.¹⁰ The role of HUD emphasizes the risk of the regulatory “perfect storm,” where multiple regulators come together to impact an individual institution.

Exhibit 2: Compliance spending by category

Compliance Spend by Category



Source: Deloitte Center for Banking Solutions

⁹ Federal Reserve Civil Penalties, Federal Reserve Web site, www.federalreserve.gov, and OCC Enforcement Actions, OCC Web site, (www.occ.treas.gov).

¹⁰ HUD Web site, www.hud.gov.

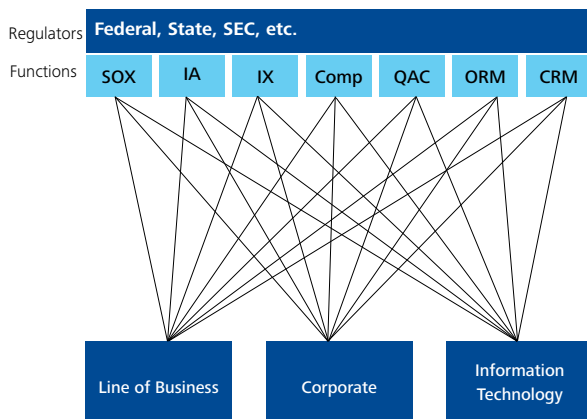
The dangers of a traditional approach

How do these additional compliance costs arise and how does the traditional approach to compliance management fail to manage them well? One reason is the siloed nature of financial services firms and their failure to fully explore the common elements of regulations and internal processes. Often, when regulations are strengthened or added, the firm adds levels of oversight, testing and interfaces, which result in redundant, overlapping functions, processes and controls. The businesses then need to comply through multiple compliance groups, testing the same processes at different times and frequencies,

often to different standards and with different outcomes. Exhibit 3 contrasts two approaches to compliance management. Exhibit 3A illustrates the traditional compliance-related approach employed by many financial services firms. The lack of alignment and coordination creates multiple layers of compliance activity. The result is additional direct and indirect costs, as well as an inability to produce complete and timely information. Exhibit 3B represents a more integrated structure where duplicative activities are eliminated and the compliance effort is more clearly focused on individual lines of business and the overall enterprise.

Exhibit 3: From a traditional to an integrated approach to compliance management

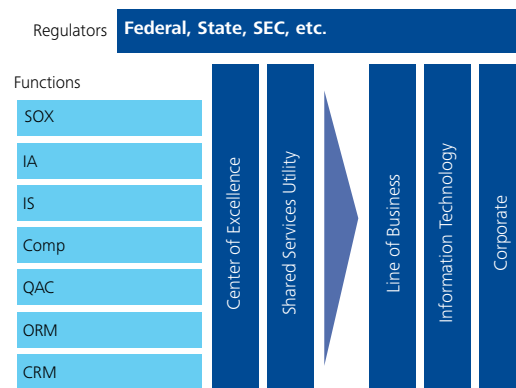
3A. Existing Process



Observations

- Underestimated cost of compliance-related activities
- Overlap, redundancy, inefficient, inconsistency, non-compliance
- Legacy systems and poor coordination with technology
- Lack of standardized risk-related definitions
- Design and framework of day-to-day activities inconsistent with leading practices

3B. Organized Process



Results

- Improved effectiveness at lower cost
- Improved operational efficiency
- Clear accountability and defined reactions
- Standardized risk assessment
- Consolidated reporting
- Streamlined governance and coordination

SOX-Sarbanes-Oxley
IA-Internal Audit
IS-Information Security
Comp-Compliance
QAC-Quality Assurance & Control
ORM-Operational Risk Management
CRM-Credit Risk Management

In many financial services firms, risk and compliance management remain not only separate, but also fragmented.

In many financial services firms, risk and compliance management remain not only separate, but also fragmented. As a result, activities are dispersed across functions and managed by various entities. This is particularly true where functional areas and lines of business coincide. Many firms will appoint specialists to address compliance and risk issues both on behalf of the function and the line of business. These separate resources unknowingly often perform similar activities, but use different approaches for collecting, gathering, and presenting information.

During our work with clients, one organization had more than 25 such areas with limited or no integration. Generally, there may be overlap between 10%-30% of testing and assessment activities and 40%-50% of operational risk and SOX controls, both operational risk and SOX are considered compliance-related functions. This often leads to a fragmented technology infrastructure. Improvements in the relationship between compliance management processes and technology not only increase effectiveness, but may reduce costs by up to 15%.¹¹

Additionally, some financial services institutions may fail to fully leverage the similar elements in regulations such as BSA, SOX, and Basel II. This creates costs without a corresponding increase and perhaps even a decrease in efficiency and effectiveness. For example, each of these regulations has common requirements regarding the design and implementation of fraud programs, the testing of internal controls, and the process for transaction disclosures. Creating separate processes for each adds costs without increasing effectiveness.

In attempting to control costs and integrate compliance and risk management, many firms face challenges in the following areas:

- 1. Evolving material risks.** Deloitte recognizes the existence of “rewarded” and “unrewarded” risks. Unrewarded risks are the minimum obligations expected of financial institutions fulfilling their responsibilities. There may be limited value creation in meeting these expectations, but consequences if the expectations are not met. The primary incentive is thus value protection, not value creation. Conversely, rewarded risks represent the strategic choices that institutions make to develop their businesses. These strategic decisions are often associated with new products, markets and services with value creation.
- 2. Inconsistent definition of risk.** In a Risk Intelligent Enterprise™, a common definition of risk, which addresses both value preservation and value creation, is used consistently throughout the organization. When risks are defined at a line of business or a product level, there is no common standard for compliance and risk management across the enterprise. This makes it difficult to measure and prioritize risks. The resulting lack of oversight and governance makes it easier for local managers to favor short-term business considerations over risk considerations. Leading practices in managing compliance and risk across the business become harder to identify and transplant. Also, what might be considered a serious risk in one part of the business might be treated as minor in another although it might be essentially the same risk. Lack of consistency in defining risks makes it difficult to leverage common processes and makes technology integration particularly difficult.
- 3. Inefficient technology.** When processes are redundant or ineffective, technology is as well. The current state of many compliance infrastructures reflects an “accidental architecture” of technologies. This generates manual information gathering and reporting tasks, which often add costs, delays and errors. In many organizations disparate systems make it hard to generate timely reports and analyze information. For example, one organization we worked with had a 50% overlap in its processes for managing Section 404 and IT risk responsibilities. Another institution had more than 250 separate applications for addressing similar risk and compliance responsibilities. Many of those applications needed to be integrated or eliminated. The various

¹¹ Individual results will vary by institution.

applications were developed and implemented over the last 30 years and cost the organization about \$240 million annually to maintain. Technology “work-arounds” typically comprise a significant portion of the total cost within the compliance functions.

4. **Redundant functional activities.** In a traditional compliance structure, there are many common activities across different areas. In our experience, 10%-30% of testing and assessment activities overlap as a result. Many regulations contain similar elements (e.g., SOX, BSA, Gramm-Leach-Bliley) that allow similar information to be provided only once. Eliminating redundancy can significantly reduce the cost of compliance monitoring. It can also help produce more timely and wide-ranging compliance information.
5. **Manual Work-Arounds.** Many compliance activities lend themselves to automation, particularly through integrated databases and dashboards that provide a single view of the risks, responsibilities and adequacy of controls across the enterprise. Testing procedures and results can be recorded and areas of deficiency highlighted for attention. Integrating databases will foster common information standards and reduce duplicative and inconsistent reporting.
6. **Cost.** Our research has attempted to pinpoint the cost of compliance, but our discussions with clients suggest that even these numbers may be significantly underestimated, often by as much as 30% or more.¹² Typically there are a number of “shadow” employees involved in the process, numerous databases and testing processes kept on individuals’ computers, manual processes, duplicative functions, roles and technologies all pointing to a significant effort to quantify the compliance cost baseline. An effective compliance management process should achieve efficiency and cost-effectiveness, and accommodate future obligations. Indeed, with the need to address increasing regulation and the rising level of unanticipated risk, efficiency is critical for any compliance program.

These challenges are certainly numerous and difficult, particularly given other strategic and operational priorities. Yet the return on solutions to these challenges—costs reduced, risks averted and goals achieved—is not only significant, but realizable.

Case study: taking an integrated approach

A series of new and stronger regulatory controls and supervisory guidance had caused a bank to review its compliance structure across finance, SOX, and the compliance and internal audit departments. Having gone through a diagnostic process, they found that their response to new regulations had been to increase the number of inefficient, redundant and overlapping processes and controls. Lacking enterprise-wide oversight, the compliance functions placed an increasing burden on individual lines of business.

Three main recommendations came out of the diagnostic analysis:

- **Implement a standard view of risk to gain consistency across the organization.** Multiple risk assessments throughout the organization focused on similar or identical attributes, yet resulted in different risk ratings. It was difficult to understand whether risk assessment had any impact on control-related activities.
- **Develop a shared services approach.** Duplicative compliance-related activities occurred throughout the organization. The core processes needed redesigning prior to wholesale elimination and the enabling technologies adjusted to support a shared services design.
- **Continue building utilities.** This would help to increase efficiencies, improve process governance, allow for consistent measurement metrics, enhance service delivery and reduce costs. Such considerations should be based on strategic value, and the ability to standardize, achieve scale and address internal customer needs.

The bank realized the following benefits.

- **A much clearer view of the existing compliance structure.** A greater understanding emerged of what compliance activities were conducted, where and why the activities were conducted and the risks embedded in the current processes.
- **A better understanding of compliance costs and a plan for significant cost savings.** The legacy compliance architecture revealed numerous quick fixes and manual processing, representing a 10%-15% cost saving opportunity.
- **A future-state compliance management function.** A monitoring approach across the enterprise was combined with new processes to help keep the organization’s compliance and risk management functions on track.

With its new compliance management function in place, the bank saw a significant increase in compliance effectiveness at a significantly reduced cost. This confirmed that compliance resources were in place where they could be most effective. An opportunity for cost savings of 15% was identified, which were later raised to 30%.

¹² Actual savings may vary from institution to institution.

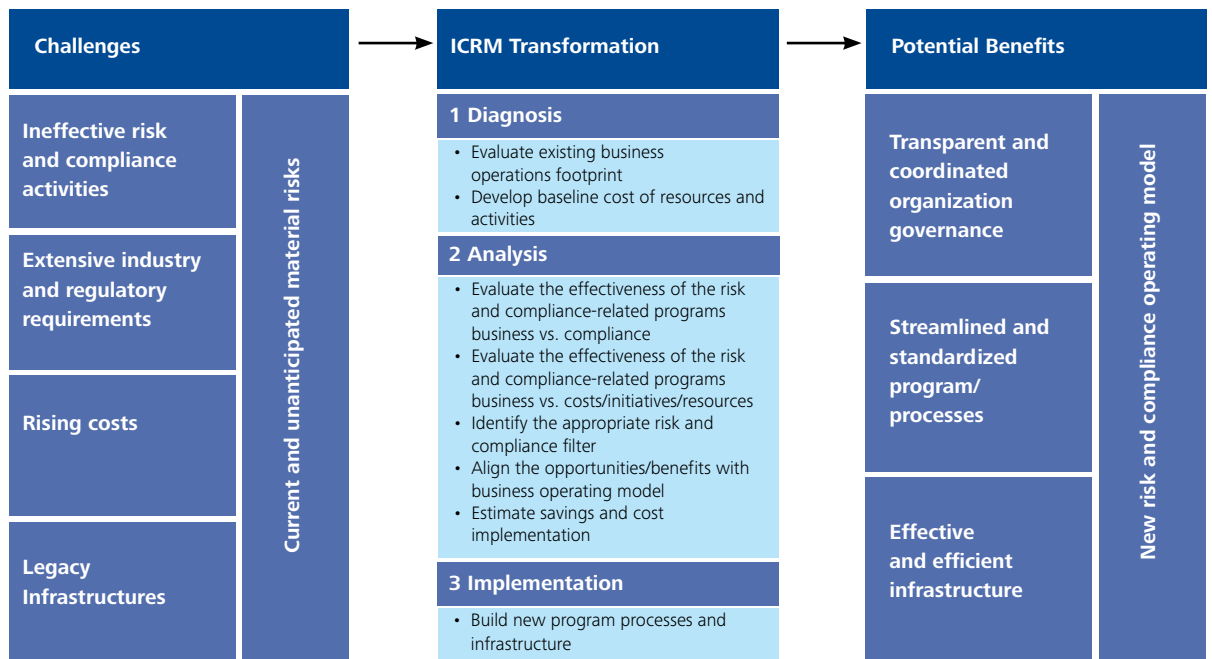
Transforming compliance and risk management – an integrated approach

Creating a compliance and risk management process

A more efficient compliance management approach employs a streamlined framework that integrates compliance activities across lines of business and shared service functions, and eliminates redundancies and overlap. Such an approach starts with a clear understanding of existing compliance activities and their environment and a solid business case for change. It then works to align and streamline compliance activities by addressing the functions, programs, processes and infrastructure.

This Integrated Compliance and Risk Management (ICRM) approach is the basis for our solution for improving compliance effectiveness and efficiency across the enterprise, and is outlined in Exhibit 4. ICRM is one of the tools designed as part of Deloitte’s risk intelligent framework.

Exhibit 4: Integrated compliance and risk management process



Source: Deloitte Center for Banking Solutions

The first column in Exhibit 4 depicts the major challenges that ICRM addresses, while the third column highlights the typical benefits it may deliver. The second column defines the three stages of the ICRM transformation process.

Three key steps in an ICRM transformation

- 1. Diagnosis.** The transformation begins with an evaluation of current business operations and the compliance implications. This step identifies compliance resources, technologies and activities and develops an initial baseline cost of compliance. The existing risks, regulatory requirements and controls are divided into work streams and catalogued. This step defines the baseline business operating model and establishes a starting point for the development of a new model.
- 2. Analysis.** This step analyzes the effectiveness of the existing compliance programs against the existing risks. This analysis identifies a compliance gap (programs not addressing identified risks) and the potential need for additional controls. By analyzing the current work streams in place and the new ones to be developed, potential synergies can be identified and leveraged. Duplicative activities can be eliminated. This rationalization of work streams and the processes within them makes it possible to rationalize the infrastructure that supports them and to quantify the impact to the bottom line through improvements in effectiveness and efficiency. Our experience indicates that cost savings of this process can be up to 10%-15%, over a 6-12 month period, although this will vary based on the individual circumstances of each client. This step finalizes with prioritization of the risks to the business implied by the compliance gap. Additional cost savings and implementation costs may be identified and resources allocated by risk and compliance priorities.¹³
- 3. Implementation.** Once the new compliance operating model (business operating model) has been developed, it can be implemented with a governance structure to facilitate alignment with the firm's strategy. To ensure performance standards are met, metrics should be established with periodic benchmarking against a defined "leading class" peer group.

These three steps should generate greater compliance effectiveness at a lower cost. The model can be modified to suit the changing needs of the enterprise through periodic reviews. With performance metrics in place, investments can be made with a clearer understanding of the outcome and enable monitoring so anticipated cost reductions are achieved. In this way, compliance expenditures can be justified based on potential returns; an issue with which many banks have struggled with.

The benefits of a structured approach are illustrated in our two case studies, "Taking an Integrated Approach" and "Rationalizing Compliance at a Major Finance Firm." In each of the case studies, an institution completely redesigned its approach to compliance and risk management, simultaneously improving effectiveness and reducing costs.



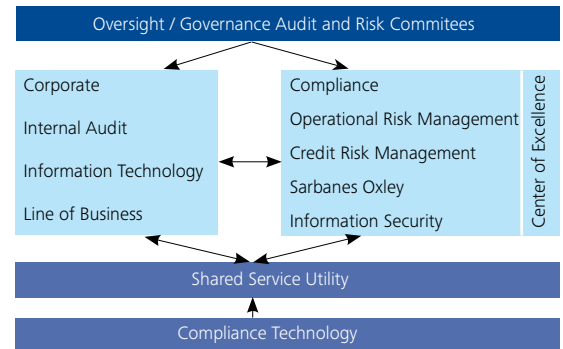
¹³Individual results will vary by institution.

Exhibit 5: Original and new risk intelligent operating models

Existing Operating Structure

Risk Management Committee	Audit Committee
Compliance	Information Technology
Operational Risk Management Credit Risk Management	Training
Sarbanes Oxley	Legal
Information Security	Line of Business
Internal Audit	
Compliance Technology Infrastructure	

New Risk Intelligent Operating Model



Source: Deloitte Center for Banking Solutions.

Developing a new risk intelligent operating model

What might a new risk intelligent operating model look like? How might it differ from current compliance activities? To answer these questions, in Exhibit 5 we contrast an example of a baseline business operating model with a desired end-state design. Certain elements clearly distinguish the new operating model from the traditional one.

- Integrated compliance functions.** In the traditional model, specialist compliance functions are separately organized and managed much as they might be in the framework outlined in Exhibit 1. In the new Risk Intelligent operating model, they are integrated under a single manager. This facilitates a more consistent approach to compliance management across the enterprise ensuring that standards are consistently being met.
- Compliance and risk center of excellence.** We have developed a center of excellence in which specialists provide compliance support to lines of business. A center of excellence promotes a common approach to testing and reporting by providing a consistent set of key performance indicators. Compliance management

controls can be assessed against a common enterprise-wide standard that replaces individual standards set at a line of business level.

- Shared services utility.** Common elements of compliance management are concentrated within a shared services utility, which manages the interface with the lines of business. Duplication and unnecessary activities are reduced, if not eliminated and therefore, costs are reduced. Activities such as testing of internal controls can be performed to a common standard across compliance functions and lines of business.
- Integrated compliance technology.** With process rationalization and clearer priorities, the technology infrastructure can be more closely aligned with compliance needs. The institution can automate manual activities and eliminate duplicative applications, potentially further driving down its cost structure. In our experience, financial institutions often delay sun-setting of applications and systems. This is more likely to occur at the more decentralized the institution. Traditional compliance management systems may feature multiple databases or standards of information, which can be eliminated in an integrated system.

- **Transparent enterprise-wide structure.** Integration of reporting relationships across risk and compliance management functions improves communication about risk and compliance issues. These issues are no longer buried within individual lines of business or obscured from management attention. A more integrated and transparent structure creates a more informed dialogue and increases awareness of risk and compliance issues, which fosters a stronger risk and compliance management culture. This transparency also improves an organization's ability to quantify costs when making compliance business decisions.

From here, management can build additional value-added activities based on priorities. The needs of individual businesses can be compared through a common framework. This more streamlined approach is designed to limit the burden on the lines of business, provides management with more timely and accurate information and offers an enterprise-wide view of compliance risk. Compliance effectiveness is dramatically increased and costs may be significantly reduced. An example of how this might work in practice is provided by our case study "Rationalizing Compliance at a Major Finance Firm."

Case study: rationalizing compliance at a major finance firm

The institution faced increasing compliance requirements over several years, reflecting multiple lines of business and diversified consumer and commercial customers in various geographic locations. New regulations had resulted in a fragmented program with overlapping compliance groups and processes generating growing compliance burdens and costs. Management had recognized the problem, but previous efforts had resulted in little savings. It was time for a more holistic, sustainable approach.

The institution started by tailoring an ICRM program to identify what, where, and why testing activities were being performed, the overlaps and redundancies, and the desired end state. The goals were to simplify compliance-related activities, ease the burden on the lines of business, and close effectiveness gaps.

- **Implement a new business operating model.** The diagnostic and assessment process within ICRM provided the design and development of a new business function model. The ICRM analysis found that as much as half of compliance processes were overlapping across internal groups.
- **Develop an overarching governance structure.** This was required to determine the areas of focus for compliance resources to decide optimal allocation.
- **Develop common terminology.** Different compliance groups used different compliance languages, methodologies, and policies, obscuring an enterprise-wide view of compliance risks and their status. To coordinate reporting, the institution created common compliance terminology.
- **Employ risk-based testing.** Many employees were performing duplicative tasks. Implementing such testing led the firm to eliminate 80% of its FTEs in certain areas and to define risk tolerances more consistently.
- **Streamline reporting.** The lack of a defined view of risk had resulted in 20% of the compliance group's time spent generating more than 200 summary management reports annually. The institution is now designing dashboards for different levels of management to reduce the number of reports they receive and to focus attention on high-priority issues.

Results

Within the next year, these and other enhancements are expected to generate annual savings of approximately 20%. As compliance becomes more efficient, management is gaining a clearer picture of risks and a greater ability to assign more resources to higher priority areas and fewer to lower risk priorities. This has allowed the firm to improve its compliance effectiveness largely on a self-funded basis.

Reaping the benefits

An enterprise-wide approach facilitates a constant dialogue among risk management areas regarding improvements, enables the development of a true cost of compliance and fosters a compliance culture at all levels of the firm.

Employing an integrated, risk-based approach to compliance may boost effectiveness, target resources to high-priority areas and give executives visibility into the state of enterprise-wide compliance. An effective compliance risk management process frees up financial resources and senior management time for revenue generation, customer service enhancements, and other business opportunities.

This framework may generate significant benefits over the short term (0-180 days) and medium term (181 to 360 days), which may yield a 10% to 20% reduction in compliance cost. In these time frames, savings result from risk-based testing, eliminating overlapping activities, and streamlined reporting. Longer term, firms can reduce compliance expenditures by up to 20% to 30% through consistent risk assessment and improved supporting technology.¹⁴ These efforts can include standardizing processes and controls and automating workflows. The cost savings and efficiency gains will depend on decisions made to reallocate resources and invest in infrastructure and technology changes.

Beyond this, there are additional benefits. A holistic approach to compliance and risk management better positions financial institutions to address future risks and anticipate the impact of changing conditions. An

enterprise-wide approach facilitates a constant dialogue among risk management areas regarding improvements, enables the development of a true cost of compliance and fosters a compliance culture at all levels of the firm.

Understand your costs. Again, many financial firms underestimate compliance costs—by up to 30%. Determining the current costs of compliance can be challenging, but it's critical to making the business case for ICRM.

Be realistic about what can be accomplished. While a comprehensive, enterprise-wide program will likely deliver the best results, this may be more change than the institution can manage at one time. A phased approach or one of limited scope is not only acceptable, but at times preferable.

Focus on what matters. We often see too many resources focused on low risk areas and not enough on higher risk areas. Assess risks carefully and set priorities accordingly.

Win C-suite buy-in. A C-suite executive must understand the ICRM effort, ensure sufficient resources, communicate with other senior-level stakeholders, and help manage or resolve any conflicts.

Integrated compliance and risk management may increase effectiveness, efficiency and reduce costs. At the same time, compliance becomes more effective as firms view requirements across the enterprise and assess risks more accurately. The cost savings and improved risk management may provide a competitive advantage. As markets become more risky, it may provide the most important basis for competitive success.

¹⁴ Individual results will vary by institution.

A roadmap for compliance proficiency

Financial services firms often have difficulty assessing their baseline compliance proficiency without a guide. Such a guide is outlined in the ICRM Maturity Matrix (see Exhibit 6). By assessing their current and desired levels of compliance effectiveness, firms can assess the degree of change and the major steps required to achieve their desired level.

Exhibit 6: ICRM maturity matrix ¹⁵

	Unaware	Fragmented	Top-Down	Systematic	Risk Intelligent
Awareness	Firm has limited awareness of its compliance responsibilities and activities.	Firm is aware of compliance responsibilities and activities but has limited prioritization.	Firm has prioritized compliance activities consistent with its business footprint.	Firm is consistently testing the extent and adequacy of its compliance activities.	Firm regularly reviews and redefines its definition of risk and compliance activities. Full self-governing model.
Accountability/ Organization	Role and responsibilities not clearly defined. Accountability confused. Limited structural oversight. Narrow definition of compliance.	Oversight structure exists but duplicative with LOB. Duplication of roles and responsibilities. Narrow definition of compliance.	Clear oversight structure. Clear roles and responsibilities. Transparent accountability. Broader definition of compliance.	Independent oversight perspective. Compensation structure in place to incent behavior.	Deeply ingrained compliance ethics culture across the enterprise sponsored by C-suite.
Process and Controls	Limited process and controls in place. Significant manual activity.	Processes and controls in place but highly duplicative and fragmented.	Shared services structure in place with prioritized resource allocation based on degree of risk.	Firm constantly audits its business function model and stress tests it against its updated compliance risk footprint.	Processes and controls are constantly revisited through RCSA or similar process.
Measurement	Metrics in place to measure compliance management effectiveness are limited or nonexistent.	Metrics established by some or all lines of business but are inconsistent across the enterprise.	Metrics in place are consistent across the enterprise and subject to regular management review.	Metrics are in place and benchmarking takes place to compare firms against best-in-practice institutions within the industry.	Metrics and benchmarking are in place and constantly reviewed for effectiveness. Benchmarking is with best-in-class independent of industry.
Technology	Limited resource allocation to compliance. Fragmented and siloed IT approach. Heavy dependence on manual activities.	IT has compliance systems in place but they are largely LOB specific. Limited integration between process improvement and IT development.	Integrated approach between process improvement and IT development across the enterprise. Common systems for compliance independent of LOB.	Alignment and leverage of compliance platform to achieve continually enhanced business benefits of improved efficiency and technology utilization.	Have language and set of metrics to continually improve the compliance infrastructure year on year. Compliance activities are embedded in all enterprise systems across the firm.
Culture	No clearly defined ethics culture within the firm.	Some degree of awareness around the importance of adhering to external regulations, subject to overriding business priorities.	Strong culture of ethics compliance with consequences for serious breaches.	Aggressive ethics culture for compliance seeking out new areas of exposure as part of the management DNA of the enterprise.	Strong ethics leadership throughout the industry. Strong commitment by the C-suite to ethics as part of the external brand identity of the firm.

We have added culture to the familiar elements in the chart, such as awareness, oversight, processes, measurements, technology, and accountability. That is because behavior, which is determined by culture, is essential to the success of any compliance program. The leadership creates the culture and sets the tone. For instance, some firms have established a strong ethics culture to reinforce their brand identity, seeing an opportunity to build customer relationships, strengthen counterparty engagement and instill confidence among regulators. This is easier to do with clearly defined roles, responsibilities, accountability and performance metrics.

¹⁵ Based on the OCEG Corporate Compliance Maturity Model.

Deloitte risk intelligence framework

The Risk Intelligent Enterprise™

Financial institutions are in the business of taking risks, but can falter when those risks are not managed effectively. One way of addressing this is to have a framework in place for risk management. The Deloitte risk intelligence framework suggests such an approach. The risk intelligence framework envisages three lines of defense: risk ownership, infrastructure and oversight, and finally governance to ensure the effectiveness and efficiency of the whole process.

Risk infrastructure and oversight

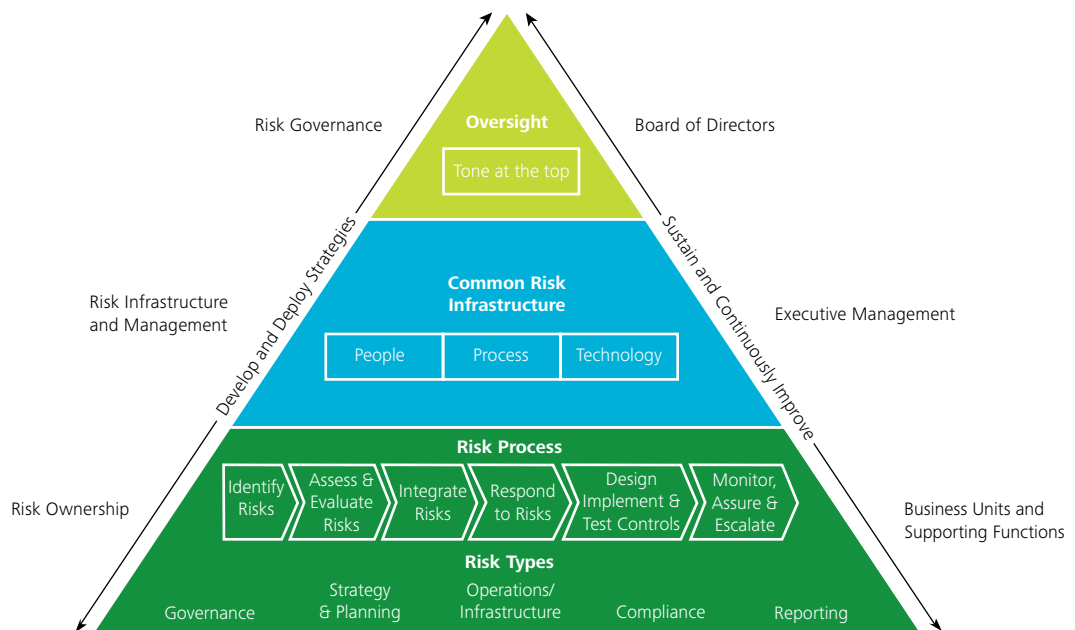
- Design, implement and maintain a common risk and compliance infrastructure
- Establish an enterprise-wide approach

Risk ownership

- Identify and manage risks at a business line and enterprise level
- Integrate risk and compliance management activities

Board-level risk governance

- Improve Board effectiveness
- Assess ethics, risk and compliance programs
- Set the right tone for effective risk and compliance management



Source: Risk Intelligence Enterprise™.

Visit www.deloitte.com/RiskIntelligence for additional information on Risk Intelligence.

Authors

A. Scott Baret

Partner
Regulatory & Capital Markets Consulting
Deloitte & Touche LLP
sbaret@deloitte.com
+1 212 436 5456

Julia Kirby

Director
Regulatory & Capital Markets Consulting
Deloitte & Touche LLP
jukirby@deloitte.com
+1 202 879 5685

David Cox

Director of Research
Deloitte Center for Banking Solutions
dcox@deloitte.com
+1 212 436 5805

Contributors

James H. Caldwell

Partner
Regulatory & Capital Markets Consulting
Deloitte & Touche LLP
jacaldwell@deloitte.com
+1 704 227 1444

Paul Legere

Principal
Financial Services
Deloitte Consulting LLP
plegere@deloitte.com
+1 312 486 2289

Vincent Tarantino

Manager
Regulatory & Capital Markets Consulting
Deloitte & Touche LLP
vtarantino@deloitte.com
+1 212 436 2462

Industry Leadership

Jim Reichbach

Vice Chairman
U.S. Financial Services
Deloitte LLP
jreichbach@deloitte.com
+1 212 436 5730

Deloitte Center for Banking Solutions

Don Ogilvie

Independent Chairman
Deloitte Center for Banking Solutions
dogilvie@deloitte.com

Laura Breslaw

Executive Director
Deloitte Center for Banking Solutions
Two World Financial Center
New York, NY 10281
lbreslaw@deloitte.com
+1 212 436 5024

About the Center

The Deloitte Center for Banking Solutions provides insight and strategies to solve complex issues that affect the competitiveness of banks operating in the United States. These issues are often not resolved in day-to-day commercial transactions. They require multi-dimensional solutions from a combination of business disciplines to provide actionable strategies that will dramatically alter business performance. The Center focuses on three core themes: public policy, operational excellence, and growth.

To learn more about the Deloitte Center for Banking Solutions, its projects and events, please visit www.deloitte.com/us/bankingsolutions. To receive publications produced by the Center, click on "Complimentary Subscriptions."

Disclaimer

These materials and the information contained herein are provided by Deloitte and are intended to provide general information on a particular subject or subjects and are not an exhaustive treatment of such subject(s).

Accordingly, the information in these materials is not intended to constitute accounting, tax, legal, investment, consulting, or other professional advice or services. The information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

These materials and the information contained therein are provided as is, and Deloitte makes no express or implied representations or warranties regarding these materials or the information contained therein. Without limiting the foregoing, Deloitte does not warrant that the materials or information contained therein will be error-free or will meet any particular criteria of performance or quality. Deloitte expressly disclaims all implied warranties, including, without limitation, warranties of merchantability, title, fitness for a particular purpose, noninfringement, compatibility, security, and accuracy.

Your use of these materials and information contained therein is at your own risk, and you assume full responsibility and risk of loss resulting from the use thereof. Deloitte will not be liable for any special, indirect, incidental, consequential, or punitive damages or any other damages whatsoever, whether in an action of contract, statute, tort (including, without limitation, negligence), or otherwise, relating to the use of these materials or the information contained therein.

If any of the foregoing is not fully enforceable for any reason, the remainder shall nonetheless continue to apply.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

Copyright © 2009 Deloitte Development LLC. All rights reserved.

**Member of
Deloitte Touche Tohmatsu**