



Cutting through the complexity of compliance

A clean-sheet approach allows the compliance function to improve decision making and manage risk.

By Jason Heinrich, Sean O'Neill and Neal Goldman

Jason Heinrich is a partner with Bain & Company's Financial Services and Performance Improvement practices. Sean O'Neill is a partner with the Financial Services practice. Both are based in Chicago. Neal Goldman is a legal management adviser to Bain. The authors thank Andrea Eschmeyer, a Bain principal, for her contributions to this publication.

When a US-based transaction processing company decided to upgrade its know-your-customer (KYC) process for a rollout in 50 countries, it devised a system and risk-based sequence that would appease regulators in each country, rein in costs, and yet also deliver a convenient, easy experience for customers.

A major Canadian bank aspired to design a best-in-class anti-fraud experience for customers while also improving employee engagement and the economics of its antifraud system. To do this, it assembled a cross-functional team that could design the experience, improve the bank's capabilities and accelerate initial tests before rolling out the new experience across the bank network.

The common thread for these initiatives? Risk and Compliance partnered with the lines of business not only to ensure that the firm fulfilled legal requirements but also to enhance the customer experience.

Organizational complexity, more than a few rogue employees, lies at the heart of recent compliance and risk management breakdowns.

Financial services companies face unprecedented complexity in their regulatory and risk environments. Moreover, the businesses themselves have become harder to manage as technology and competitors move ever faster. With the proliferation of digital channels and greater customer involvement in core activities such as remote deposit capture, compliance processes designed for physical locations have had to be reworked to handle “invisible” customers operating remotely. Many third parties also get involved in this omnichannel ecosystem, and problems can occur at any node on the network.

Organizational complexity, more than a few rogue employees, lies at the heart of recent compliance and risk

management breakdowns. Failures at large, multifaceted organizations such as Lehman Brothers, the Irish banks and AIG resulted from some combination of inadequate coordination, process breakdowns, outdated policies and systems, and unclear decision processes. The rise of Big Data is adding to the challenge: Putting more data into bad processes and poor decision architectures clogs the system until it breaks down.

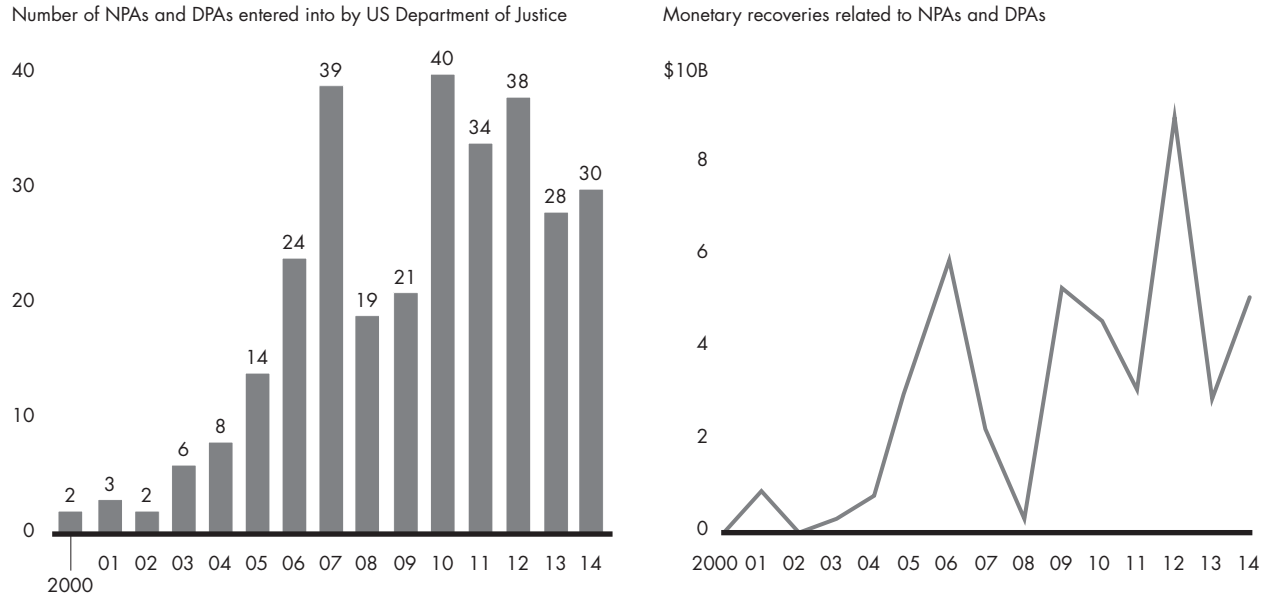
System failures have led to major financial penalties for companies and their executives (*see Figure 1*). Since 2009, more than 190 companies have entered into agreements with the US Department of Justice, paying \$30 billion in fines. Late in 2014, the US Financial Crimes Enforcement Network filed charges seeking a \$1 million penalty against the former chief compliance officer (CCO) of MoneyGram International for failure to stop money laundering activities. Similar regulatory trends are occurring around the world, particularly in Europe and increasingly in Asia. The damage in reputation, lost customers and loss of shareholder value can be even more severe.

Moreover, disparate systems, often the result of incomplete integration after mergers and acquisitions, make compliance and risk management more difficult. As new regulatory efforts, such as the Office of the Comptroller of the Currency's Standard on Heightened Expectations, require these processes to function well, quickly reconciling the gaps has become a more urgent challenge.

In our experience working with financial services companies around the world, and validated by various surveys, compliance has become a top priority for management and boards. Compliance department budgets generally are growing faster than other functions. JPMorgan Chase, for instance, spent about \$2 billion on compliance in 2014, roughly double the amount from the previous year. Yet in some cases, the higher spending focuses on short-term fixes that may introduce further complexity.

How can the chief compliance officer (CCO), chief risk officer (CRO) and team satisfy the demands of more

Figure 1: Financial services fines generally have been rising



Source: Gibson Dunn, 2014 Year-End Update on Corporate Non-Prosecution Agreements (NPAs) and Deferred Prosecution Agreements (DPAs), January 6, 2015.

complex regulations while also helping their companies grow their top and bottom lines? Unless financial services companies chart a clear compliance strategy and investment roadmap that’s tightly linked to business objectives, compliance work remains tactical and reactive, and may itself increase organizational complexity, paradoxically increasing risk. (See the sidebar on page 3, “10 signs that you should consider a clean-sheet assessment of the compliance program.”)

A clean-sheet approach to business activities

The best-performing companies are fully reexamining *which* compliance and risk management activities they perform and *how* they are performed—not just within the Risk and Compliance departments but across the seams of the organization. This clean-sheet approach, also called zero-basing, looks to identify the activities that truly need to occur, who should do them, how they should be executed to enhance decision making,

and then pinpoints those tasks that could be eliminated altogether to reduce complexity and lower the risk of system failure. The greater a company’s aspirations, the deeper the structural changes required.

For instance, many banks’ manual controls have to be tested multiple times to comply with multiple regulatory frameworks, such as Basel, Sarbanes-Oxley, Comprehensive Capital Analysis and Review. In addition, operational risk assessments, compliance risk assessments, internal testing and internal audits all review the same controls repeatedly. Multiple reviews that never become fully integrated invite the spread of inconsistent conclusions and plans. A clean-sheet approach can build the right solution the first time, eliminating redundancy and cost and lowering risk.

The transaction-processing company mentioned earlier, for example, used this approach to reduce its total compliance-related budget by over 20%, while

10 signs that you should consider a clean-sheet assessment of the compliance program

1. Frequent compliance breaches and failed audits, exams, government inquiries, litigation
2. Weak culture of compliance and excessive risk taking
3. Unclear roles and responsibilities
4. CCO without a consistent seat at the strategy table
5. Failure to make compliance part of the performance management system
6. Under-budgeting of compliance-related spending, as compliance costs and issues both increase
7. Cumbersome policies, procedures and processes in lieu of clear principles
8. Poor experience for customers who hit compliance queues
9. Limited automation, outsourcing or low-cost locations
10. Inconsistent assessment of risk in strategic transactions and significant business deals

greatly improving effectiveness and reducing risk. The savings and risk mitigation came from eliminating or reducing non-critical work, aligning controls with risks and improved planning and execution. The gains in effectiveness came from working closely with the business units to improve compliance while enhancing the customer experience. For instance, the company tested the new KYC process with customers, listened to the feedback, and made adjustments to features—such as text messaging at the point of sale—until customers perceived the process as easy and convenient. That helped to earn customers' trust and loyalty.

Leading financial services firms have embraced the clean-sheet mentality and redesigned four critical elements of compliance: its roles, policies and priorities, oper-

ating model and key capabilities essential to making the system work (see *Figure 2*).

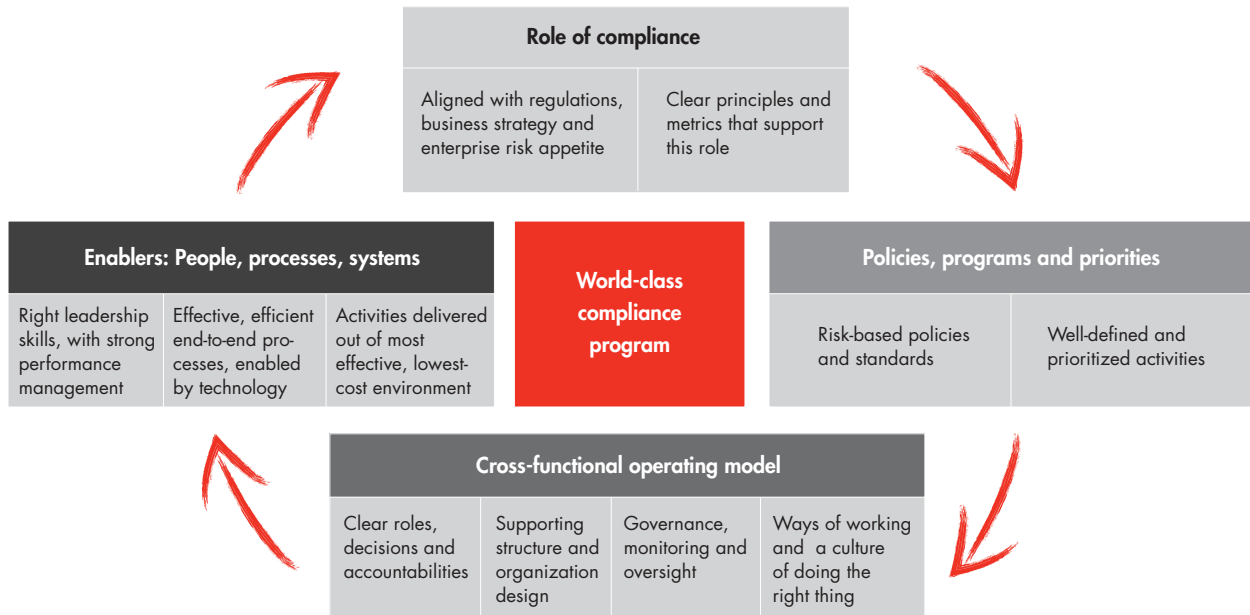
New roles in an ensemble cast

CCOs generally play three roles: *adviser* to the business, *reviewer* of key policies and processes performed by others to ensure efficacy, and *operator* of critical compliance activities. In most financial regulatory regimes, the business unit is the first line of defense and Compliance the second line.

But because Compliance touches so many parts of the organization, from customer-facing front lines to back-end IT, CCOs have a big opportunity to strengthen their partnership with the business. One CCO, for instance,

Cutting through the complexity of compliance

Figure 2: High-performing compliance organizations focus on four key elements



Source: Bain & Company

runs a substantial fraud call center, which requires strong general management skills beyond his legal and regulatory expertise. And anti-money-laundering (AML) processes often give CCOs immediate access to troves of customer information that can potentially influence how a financial institution makes new growth investments.

At many leading companies, CCOs have taken a more active role in supporting growth and managing risks. They spend more time with business leaders, to build trust and devise solutions. That partnership allows the Compliance function to do its job in a way that does not break the business but rather, when done right, provides information that’s extremely useful in advancing the business.

Data management is one area that offers an opportunity for greater collaboration between Compliance and other parts of the business. Many banks have not fully integrated their KYC or AML processes into a broader set

of customer data collection processes or into a comprehensive customer data infrastructure that can support Compliance, Marketing, Risk, and the lines of business. In most cases, KYC and AML are handled in a completely different fashion than customer relationship management databases, marketing data warehouses and other processes.

Instead of operating discrete processes that only capture one component of the bigger picture, banks can design efficient processes to enhance customer data up front to meet all these needs. And Compliance has an integral role in doing so.

With policies and programs, less can do more

Although laws require financial firms to have effective compliance programs, the activities that define a firm’s program should be customized based on its unique situation, including the underlying risks, organization,

products and customers. Compliance departments can collect the universe of regulatory requirements and use a risk assessment to define the policies and activities that work best for each part of the organization. Embedding compliance reviews at the right decision points and in the right departments can reduce costs and streamline decision making, adding value beyond risk avoidance.

Taking a clean-sheet perspective, Compliance can establish a set of principles and a baseline of clear minimum standards that give the organization flexibility to create bespoke policies commensurate with the risks involved. For instance, money services businesses may have high AML risk and low politically exposed person (PEP) risk, given the nature of their customer base. A private wealth firm may have a high risk for PEPs and lower AML risk. The specific risk profile guides the organization in determining where to invest its resources and how to size compliance activities appropriately.

Fewer policies with strong statements of principle and a culture of doing the right thing may well trump tomes of policies and procedures.

At one US financial services firm, hundreds of new, often redundant, business rules were stacked on top of each other over the years. The web of unclear rules led to a rise in the number of blocked or held transactions, which in turn prompted more manual reviews and diminished the customer experience. By zero-basing these rules, the firm was able to untangle the mess and deliver a more efficient and customer-friendly outcome.

The most aggressive or stringent policies won't be suitable for every checkpoint. A stance of "more policies equal more risk mitigation" creates a zero-tolerance

mentality and a proliferation of sub-optimal decisions. While this conservative approach might boost compliance with regulations, it can strangle the business and discourage employees. It's easy to add rules, but harder to remove them. Leading companies increasingly understand that "less can be more"; fewer policies with strong statements of principle and a culture of doing the right thing may well trump tomes of policies and procedures. This is where the CCO can manage compliance in a way that streamlines business processes.

Consider how a Canadian pension fund governs the information flow between its trading floor and private investing groups. To ensure that investment professionals don't share proprietary information with traders, the pension fund relies on its strong code of conduct and culture of doing the right thing. That's allowed the fund to maintain a strong compliance track record with minimal governance complexity.

Redesigning the operating model

An operating model serves as a blueprint for the way resources are organized and operated. Effective models encompass several elements:

- Strong governance
- Decisions around the shape and size of the compliance function
- Where to draw the boundaries between the compliance function and the lines of business
- How people work together within and across these boundaries
- How the compliance function will add value to the business units
- How to integrate compliance into the business
- What norms and behaviors should be encouraged
- How conflict will be resolved

Cutting through the complexity of compliance

This blueprint of enhanced decision making, with the right level of compliance embedded in the system, serves as the core of an effective cross-functional compliance program.

Several factors have heightened the need for operating models to evolve. The pursuit of growth has led to organizational complexity as financial services companies extend to new customer segments, products and geographies. Financial institutions have also added staff and made large technology investments to address gaps exposed by the financial crisis, actions that potentially add complexity.

In addition, digital technology has changed every aspect of business operations, including how and where companies interact with customers. Although Big Data analysis can provide valuable new insights, the growing volume of data can drown an unprepared enterprise. IT systems must ensure that relevant, actionable data gets to the right Compliance and business managers.

For a more integrated approach to compliance, firms need to complement traditional subject matter expertise in areas such as consumer protection, trading rules and corruption with strong communication and general business skills to get things done across the organization.

Breakdowns in compliance typically result from process deficiencies where well-meaning managers make bad decisions or fail to recognize or escalate high-risk issues. The right processes with clear accountabilities, decision making, and reporting can greatly help. At the Canadian pension fund mentioned previously, clarifying and documenting the compliance accountabilities that spanned

the central group and functional areas reduced the risk of items falling through the cracks.

Designing a compliance-focused operating model starts by fully describing the compliance strategy requirements to the senior executive team. Then that team must agree on a compliance strategy. That allows the CCO's team, together with the business leaders, to create a detailed plan that articulates the activities and priorities required to execute that strategy. It may take some debate among the senior team to agree on the priorities, but that discussion is essential, otherwise the execution will fail. This effort sets the framework for employees to have a clear sense of their compliance-related accountabilities as well as an understanding of expected behaviors and ways of working.

The right people with the right tools

All of the elements discussed so far—roles, policies, the operating model—hinge on having employees with the right skills, training, incentives and tools to implement them. For a more integrated approach to compliance, firms need to complement traditional subject matter expertise in areas such as consumer protection, trading rules and corruption with strong communication and general business skills to get things done across the organization.

The CCO is on point to recruit other talented business people who can improve operational performance, build trust and enhance collaboration with the business, and also reduce some of the administrative burden on the CCO. The CCO also has to champion the Compliance function and gain the stature of a trusted senior adviser to the CEO and board, demonstrating business acumen beyond compliance. To that end, CCOs, particularly in larger organizations, should aim to create or amplify a few key capabilities to complement the regulatory subject matter experts:

- An *operations officer* who can play a meaningful role in sponsoring significant change, like zero-based budgeting, and make it stick. Good candidates

Cutting through the complexity of compliance

- could come from within Compliance or outside; the main criteria are an understanding of compliance perspectives and strong operational and general management skills, including familiarity with lean techniques.
- A dedicated *IT liaison* familiar with compliance issues and processes. He or she can help the IT staff keep up with trends in areas like consumer protection and ensure that the right information is collected accurately and cost-effectively. A liaison can also help Compliance identify opportunities to better use technology, sequence IT requests, and evaluate specific solutions for purchase.
- Embedded finance* or other analytical personnel can help illuminate spending patterns, workforce modeling and scorecard and metrics management—all of which should come with clear returns. This role should also help to ensure that business cases and new opportunities fully reflect compliance costs.
- Data analytics* personnel, particularly in transaction-heavy businesses, serve to identify and substantiate the risk-based approach.
- HR and talent development personnel* can help hire and develop middle managers who have excellent coaching and general management skills required to make the desired changes happen.

Besides the right mix of talent, companies' performance metrics and incentives should encourage people to do the right things (see Figure 3). Reward systems must establish firmly that not every deal or sale is a good one. For example, in countries where bribery or corruption are pervasive, companies must confirm that they have the appropriate safeguards to operate in such high-risk environments, even if it means walking away from a short-term revenue opportunity.

Compared with simply adding headcount, a smarter deployment of technology and lean method will help raise the effectiveness of the Compliance function at a

Figure 3: Strong performance management helps to promote accountability

Area	Metrics	Target
Customers	Customer loyalty scores	>X%
	"Know your customer" completion rates	>X%
	Reduction in fraud incidents and corresponding complaints	X
Effectiveness	Number of regulatory violations and material exam findings	X
	Look-back and remediation project costs and associated penalties	\$X
	Adherence to policies and procedures	X
	Reduction in reimbursements for fraud incidents	\$X
Efficiency	Cost per transaction for compliance	\$X
	Average time between opening and closing an investigation case	X minutes
	Number of transactions requiring manual review	X
	Cost per "know your customer" diligence	\$X
Partnership	Employee training feedback	X
	Feedback from business and operational leaders	X

Source: Bain & Company

Cutting through the complexity of compliance

Figure 4: Technology will dramatically change how compliance is delivered

	Current state		Future state
Customer identity management	Transaction-based customers	▶	Single customer record
Customer data management	Data collection	▶	Data collection, validation and verification
Customer interactions	Multichannel	▶	Omnichannel
Customer and transaction monitoring	Rigid, binary rules	▶	Sophisticated risk modeling and assessment
Transaction intervention	Manual, lengthy intervention process	▶	Automated, efficient intervention process
Customer communication	Reactive communication	▶	Proactive communication
Front- and back-end processes	Paper-based processes	▶	Digital processes
Investigation effectiveness	Fragmented case intelligence	▶	Unified case intelligence
Disposition efficiencies	Limited decision automation	▶	Sophisticated decision automation

Source: Bain & Company

lower cost (see *Figure 4*). Technology can identify high-risk patterns of behavior that currently require manual intervention. That will greatly reduce human error and free up more time for Compliance officers to focus on other high-value activities. Regulatory changes heighten the need to accelerate initiatives that digitize more information and processes. Banks that can provide real-time access to data, for instance, will become more transparent to regulators.

Organizing for success

Adopting an end-to-end compliance program that's embedded at just the right process points and adds the least possible friction to the system entails a lot of change across the whole enterprise. It typically benefits from a cross-functional transformation office composed of

top talent, not average project managers, from across the businesses who have the diplomatic skills to guide the effort. When properly staffed, the transformation office can serve as a catalyst to facilitate internal discussions about sensitive issues such as revenue at risk.

Done right, integrating Compliance as a close but independent partner with other functions and the business units will reduce complexity, improve decision making, build trust with customers and business partners and foster a culture of integrity where top talent wants to work. 

Shared Ambition, True Results

Bain & Company is the management consulting firm that the world's business leaders come to when they want results.

Bain advises clients on strategy, operations, technology, organization, private equity and mergers and acquisitions. We develop practical, customized insights that clients act on and transfer skills that make change stick. Founded in 1973, Bain has 51 offices in 33 countries, and our deep expertise and client roster cross every industry and economic sector. Our clients have outperformed the stock market 4 to 1.

What sets us apart

We believe a consulting firm should be more than an adviser. So we put ourselves in our clients' shoes, selling outcomes, not projects. We align our incentives with our clients' by linking our fees to their results and collaborate to unlock the full potential of their business. Our Results Delivery® process builds our clients' capabilities, and our True North values mean we do the right thing for our clients, people and communities—always.



Key contacts at Bain & Company

Americas:

Mike Baxter in New York (*mike.baxter@bain.com*)

Jason Heinrich in Chicago (*jason.heinrich@bain.com*)

Sean O’Neill in Chicago (*sean.o’neill@bain.com*)

Jean-Claude Ramirez in São Paulo (*jean-claude.ramirez@bain.com*)

Asia-Pacific:

Gary Turner in Sydney (*gary.turner@bain.com*)

Europe, Middle East and Africa:

Henrik Naujoks in Düsseldorf (*henrik.naujoks@bain.com*)

For more information, visit www.bain.com