

FINsights

Technology Insights for the Financial Services Industry

Governance, Risk and Compliance »



Infosys®

POWERED BY INTELLECT
DRIVEN BY VALUES.

Contents

From the Editors Desk

Strategic themes in Risk and Compliance	02
<i>Ashok Vemuri</i>	
Red light, green light – playing the risk game	06
<i>Adam D. Honore</i>	
Sub-prime crisis and credit risk measurement: lessons learnt.....	11
<i>Thadi Murali, Srividhya Muralikrishnan and Balaji Yellavalli</i>	
Credit risk management: back to basics	17
<i>Godwin George, Arup Sinha and Thadi Murali</i>	
Risk Measurement: It’s all about data, data and master data.....	24
<i>Anita Stephen, Sabitha Vuppula and Abhijit Ghosh</i>	
Raising the bar: Executive risk reporting using fractal maps.....	29
<i>Raghu Anantharam and Shriram Subramanian</i>	
Navigating through the compliance maze in a post-merger world.....	33
<i>Debashis Pradhan and Naveen Balawat</i>	
Managing the problem within - Employee Surveillance.....	39
<i>Anand Bhushan, Debodeb Datta and Rajesh Menon</i>	
Addressing the partial compliance trap in the wealth management industry.....	45
<i>Bob Skea and Vikesh Gupta</i>	
Demystifying financial compliance through an integrated IT framework	50
<i>Ravishankar N and Ramachandran Sundaresan</i>	
Integrated Controls Management– a cost effective approach to implementing GRC..	55
<i>Uttam Purushottam, Satnam Gill and Ashwin Roongta</i>	
Conversations with Tim Leech – Perspectives from an industry expert.....	61
<i>Q & A session conducted by Satnam Gill</i>	
Leveraging SaaS to manage GRC.....	66
<i>Ravi U. and Vishakha C.</i>	
Case study – Information Risk Management: A mandatory need	71
<i>Amar Bawagi and Viswananath Shenoy</i>	

From the Editors Desk

We are delighted to present the second issue of the Infosys Banking and Capital Markets journal FINsights. The spotlight in this issue is on Governance, Risk and Compliance and the compilation of articles reflect perspectives on risk and its measurement, governance, the compliance conundrum and our take on the priorities in risk and compliance and their technology implications in the coming years.

The increased incidence of failures in the financial services marketplace over the past decade has given visibility to the science (and art) of understanding and measuring risk in running a business, making strategic and tactical decisions and participating in markets and economies that are increasingly linked in a flattening world. A recent such event, covered in one of the articles, has been the sub-prime crisis and the unforeseen ripple effects in markets in distant parts of the world.

As always we have tried to reflect in these articles the unique value that Infosys brings to its clients through a combination of deep domain understanding, technology best practices and global sourcing expertise. The article on sub-prime crisis reflects the current challenges in credit risk measurement and brings a perspective that combines credit risk measurement approaches with a global knowledge process outsourcing (KPO) option.

Risk and compliance is a multi faceted animal and the focus in the past few years has been on giving it a holistic view through a unified Governance, Risk and Compliance (GRC) program. The articles featured on GRC explore integrated controls to implement GRC, use of SaaS in GRC and industry perspectives on GRC and the road ahead. In the area of compliance, the articles look at addressing compliance challenges, an aspect of internal compliance namely employee surveillance and the partial compliance challenge in the wealth management industry. Our articles on risk address credit risk management, the role of master data in risk measurement and risk reporting. Included in this issue is also a case study highlighting the importance of Information Risk Management (IRM).

We would like to thank all the authors from Infosys as well as external contributors - Adam D. Honoré from Aite Group, Tim Leech from Navigant Consulting and Bob Skea of Northstar Systems. As always, we look forward to your queries or comments on Governance, Risk and Compliance or any feedback and suggestions in making FINsights a more relevant and topical journal.

Happy reading and all the best for the new year 2008!

Balaji Yellavalli and Sudhir Singh
Editors

FINsights Editorial Board

Balaji Yellavalli

*Associate Vice President
Banking & Capital Markets Group*

Edward L Smith

*Associate Vice President
Banking & Capital Markets Group*

Jonathan Stauber

*Vice President
Banking & Capital Markets Group*

Lars Skari

*Practice Leader
Infosys Consulting*

Thadi Murali

*Senior Principal
Banking & Capital Markets Group*

Mohit Joshi

*Global Head of Sales
Banking & Capital Markets Group*

Pankaj Kulkarni

*Senior Engagement Manager
Banking & Capital Markets Group*

Roopa Bhandarkar

*Senior Engagement Manager
Banking & Capital Markets Group*

Sudhir Singh

*Associate Vice President
Banking & Capital Markets Group*



Navigating through the compliance maze in a post-merger world

More mergers fail due to poor execution than due to a lack of strategic fit. This lack of rigor is often more pronounced in back office functions like compliance with its relatively lower potential to create business disruptions or direct losses. Our experience shows that companies that take a phased approach to integrating compliance IT systems and back it up with detailed analysis and planning will be able to achieve more from the integration. A phased approach can help firms shift focus from simply complying to effectively optimizing their compliance IT.

Debashis Pradhan
Principal
Infosys Technologies Limited

Naveen Balawat
Senior Associate
Infosys Technologies Limited

Financial services firms continue to be on a buying spree. While headwinds from the credit crunch have certainly hit investment firms hard, it seems 2008 would still turn out to be a banner year for mergers and acquisitions (M&As). But this seemingly unending zest to merge belies the fact that more than half of all mergers fail. Even those that succeed go through uncertainties and disruptions. Each acquisition or merger brings in its challenges making it difficult for firms to realize the projected economies of scale and synergies. There is a growing body of evidence that suggests that more mergers fail due to poor execution than due to a lack of strategic fit. And often this lack of rigor is more pronounced in back office functions like compliance than in revenue generating ones that are more visible.

A phased approach to integration

The extent of integration that a firm wants to achieve will be driven by the merger objectives, extent of overlap between the two companies' systems and processes, time available and cost. Since most companies take a program level approach to IT integration, the level of detail required to achieve desired synergies in Compliance IT is either missing or given a short shrift. Compliance silos, redundant applications and multiple data sources continue to exist. There is also an inherent lack of incentive to squeeze out more from compliance systems due to its relatively lower potential to create business disruptions or direct losses. Our experience shows that companies that take a phased approach to integrating compliance IT systems and back it up with detailed analysis and planning will be able to achieve more from the integration.

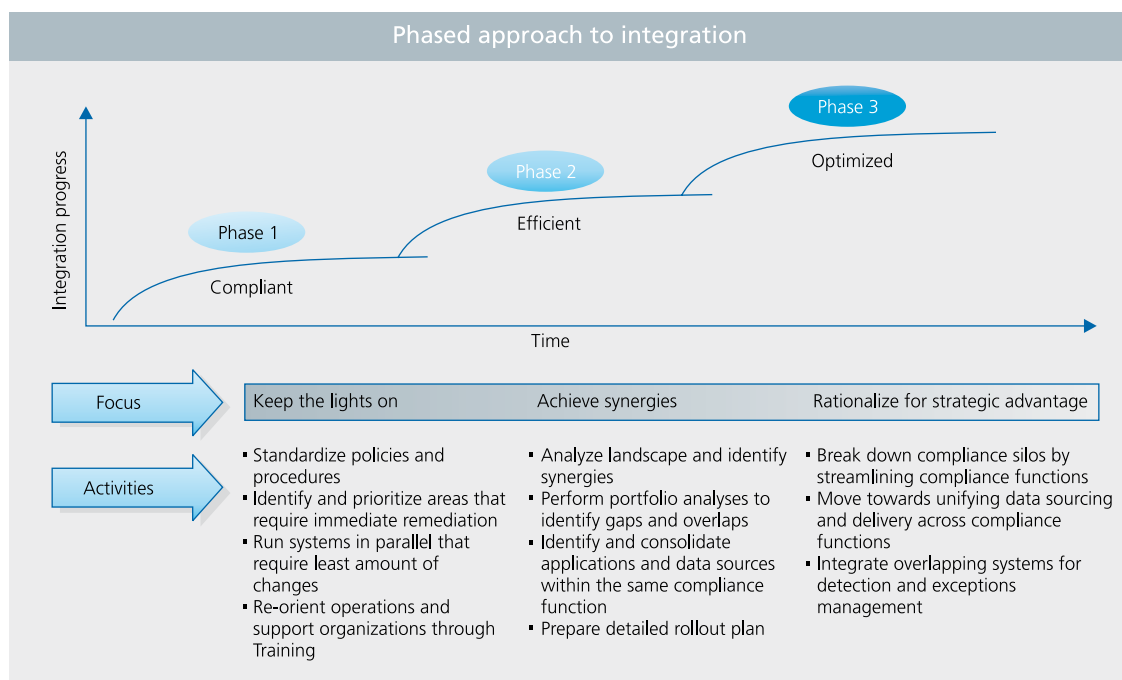
The speed and extent of integration during these phases will vary based on several factors:

Nature of the merger: Mergers could take various shapes based on the objectives and rationale. A complete takeover to gain access to specific capabilities in the same business would eventually lead to fully integrated processes and systems in compliance. If the target is small and operates in a different line of business, systems and processes may coexist for a longer time. A merger of equals would generally entail consolidation of systems to achieve economies of scale.

Functional overlap: When both the companies operate in the same businesses, there will be overlaps in compliance processes and systems. For example, they could be monitoring transactions for similar behaviors or reporting the same information to external regulators. Greater the similarity, faster will be the need to consolidate.

Proximity to regulators and customers: Compliance functions that are closer to regulators or end customers will need to come together faster. The need to provide a seamless interface to both customer groups or respond consistently to regulators will hasten the integration process in such functions. However, this will play out differently for different merger scenarios. When entities are in the same areas, initial measures will focus on bridging the key differences. This will be followed by a more detailed portfolio rationalization exercise. On the other hand, when the two companies are in different areas, the scope to merge the systems may be limited. As such, the systems may continue to exist independently.

Fig 1: Phased approach to integration



Cost to integrate: The cost to rejig systems has a big impact on the integration roadmap. When the functional differences are manageable and support costs are not prohibitive, it may be cost-effective to maintain systems in parallel. For example, it may be cheaper to retain the surveillance platforms of both the firms when there are significant infrastructure and data differences. The cost of building costly interfaces and migrating data and the opportunity cost of lost time may well outweigh the benefits of a full integration (Fig 1).

Compliant: Keeping the lights on

The focus during the initial phase of the integration is to keep everything running as smoothly as possible while attending to obvious differences that need immediate attention.

When the merging entities are in the same business, opening moves will be around standardizing policies, procedures and compliance operations after taking minor differences and practices into consideration. For example, the KYC process in case of retail banks or best execution policy in case of trading firms will need early consolidation for a seamless customer experience. Reporting function will need to be merged to provide a consistent view of holdings or transactions to regulators.

For all of this to happen there needs to be a consolidated view of data. Migration routines can be created to move data – transactional and referential, to the merged entity. While physical storage may continue to remain separate during the initial phase, logical models will have to be aligned through data mapping and translation.

Applications that have a lot in common but are relatively farther away from customers or regulators will be easier to run in parallel. Minor modifications can be made to ‘bridge’ the differences as a tactical measure. Typically, surveillance and detection platforms will fall into this category. While they may differ in their implementation and coverage, packaged detection platforms usually focus on regulations that affect the wider industry and cover vanilla products like stocks and bonds. It is not uncommon to find similar detection models when the two merging entities are in the same business. In such a scenario, the first phase of the integration can focus on harmonizing the detection models, thresholds and parameters. This will ensure consistency in monitoring of clients, employees, or transactions across the two entities. However, this harmonization may not be easy in the case of legacy surveillances that monitor more complex products and derivatives where there could be big differences in approach. Early identification of such areas will help build a migration plan that will be feasible and acceptable to the business.

When the merging entities operate in different areas, focus of the initial phase should be on systems that require little integration with core business processes.

Take the case of an asset manager merging with a securities broker-dealer. Both businesses require monitoring for insider trading or money laundering behavior. Such behavior can be identified by monitoring employee trades or money movements – activities that are not tightly coupled to the underlying business. Another such area is customer data integration. This is crucial to presenting a seamless view to both customers and regulators and bringing in consistency of coverage.

On the other hand, business-specific surveillance systems may have to run separately. The asset manager’s primary focus is on monitoring registered rep/investment advisor activity, customer suitability and mutual fund breakpoints. The broker-dealer is more interested in scenarios that involve market manipulation, best execution or fair dealing with clients. These areas vary not only in what they monitor but also in their approach to identifying suspect behavior. Given these differences, there may not be a need to consolidate these systems during early days of the merger.

Efficient: Achieving Synergies

Once the early projects are done with, firms need to shift gears to identify and converge on systems or processes best aligned with the desired future state. The limited integration achieved in the first phase will almost always fall short of achieving synergies identified during due diligence. Firms will need to assess their systems, functionality, current and future plans for a more rigorous consolidation exercise.

This assessment will need to focus on several things including compliance coverage, functional fit, alignment with integration end-state and data integration requirements. Multiple compliance functions like AML/KYC, Surveillance, Regulatory Reporting and Employee Compliance will be analyzed for both acquirer and target. Analysis during initial due diligence will be fed into this detailed assessment. Current and future plans will also be reviewed to gauge the extent of overlap and see how close each other’s plans are to the integration end state. Chances are there will similar projects that could be rationalized to achieve the twin objectives of lowering costs and reaching the future state.

Factors	Questions to consider
Compliance Coverage	<ul style="list-style-type: none"> • What regulations do the two entities need to comply with? • How different or similar are these in their requirements?
Functional Fit	<ul style="list-style-type: none"> • How different are the compliance processes at the two entities? • What is the extent of overlap across systems supporting compliance? • Are there similarities in surveillance, exception management and reporting? • What additional requirements need to be fulfilled through the merger?
Technical Fit	<ul style="list-style-type: none"> • How much do the systems and platforms employed at the two firms overlap with each other? • What are their architectural and infrastructural biases?
Alignment with Planned Integration End State	<ul style="list-style-type: none"> • What are the current and future plans and how do they dovetail into the planned integration end state? • Are there opportunities for consolidating planned projects?
Data Integration	<ul style="list-style-type: none"> • What are the differences in the data models for transactional, referential and market data? • Is data sourcing and delivery centralized or do the various units in compliance pursue this effort independently? • How will the source systems evolve during and after the merger?

Fig 2: Synergy Identification – Questions to Consider

When the target is in the same business, most if not all systems from the acquiring company will be retained. Phase two of the integration will center on moving data and functionality from the target company to the acquiring one. This migration will be bulkier when applications were tactically bridged in the initial phase. Both logical and physical data models will need to be merged to ensure a single source for compliance data. While the first phase focused primarily on melding the data models, this phase will also look at consolidating data repositories and rationalizing the primary data sources. Data required for compliance like orders, executions, positions and client data will need to reside centrally to eliminate redundancy in data support services. This migration, however, is tied to the plans in the areas supplying the data - trade processing systems in case of securities firms, core banking system in case of retail banks etc. Strong integration planning and communication across the IT organization will be required to meet the schedule deadline.

Analysis will be required to identify functionality from the target's systems that need to be made available on the acquirer's systems. These features may represent slight differences in the compliance procedures of the two companies or may reflect best practices that the acquirer wants to retain. For example, name matching for AML surveillance may be more sophisticated at the target firm than the acquirer. This may prompt the acquirer to create a project to integrate this functionality into its AML surveillance platform. A target firm with better

exception and case management features can be another example. Instead of building from scratch, the acquirer may decide to port this functionality during post-merger integration. Proper prioritization of these enhancements taking into consideration regulatory risks, impact on core compliance processes and time to market, will be crucial to meeting deadlines.

The integration effort in a merger of equals is usually the longest and most complex. With the two firms operating in similar business lines with comparable compliance processes, systems and size, there is a need to find the "best of both worlds". But often, integration teams founder as they get bogged down in lengthy comparisons and building costly interfaces to connect the preferred systems. We believe a "portfolio approach" to selecting the systems that takes into account both functional and technical fit and the integration effort is a better option. To succeed, firms must draw up a guiding strategy for the compliance IT organization based on the M&A objectives and the desired future state that will help take these portfolio decisions.

Firms can approach this using the following four steps. First, they need to identify a set of compliance considerations by function which will help choose the applications that best fit the bill. Application functionalities can then be compared based on these key considerations. Second, a set of portfolios with a mix of applications from both sides can be constructed with varying degrees of functional and technical fit, alignment with M&A objectives and desired future state. Third, the

effort to integrate applications in a portfolio including the effort to connect with systems in other divisions and transform data as required, will need to be estimated. Finally, a business case that takes into account fitment, cost and time to integrate can be put together to choose the most optimal portfolio.

Compliance Function	Considerations
Anti-Money Laundering (AML) Surveillance	Scenario coverage Sophistication of name matching Scalability Exception and case management Product roadmap
Trade Surveillance	Scenario coverage Instrument coverage Scalability Flexibility to add custom scenarios Exception management Product roadmap
Know Your Customer (KYC)	Level of integration with account opening procedures Comprehensiveness of customer information Ability to handle multiple entity types Sophistication of risk-scoring
Regulatory Reporting	Regulatory coverage (SEC, Fed etc) Instrument coverage Business line coverage Scalability Data controls and validation Linking & reconciliation
Employee Compliance	Efficacy of pre-clearance process Holdings disclosure Registration and certifications Gifts and contributions Outside business activities

Fig 3: Key Considerations in Selecting a Compliance Application Portfolio

Optimized: Rationalizing for strategic advantage

Most integration efforts focus on identifying synergies within similar compliance functions but firms generally fail to notice synergies across functions. For example, while there may be a project to integrate data sources within AML divisions, opportunities to rationalize

data sources across the entire compliance division are overlooked. Compliance is in a rare position where it has visibility over almost the entire firm's processes and systems. We think compliance IT organizations may be able to leverage this to their advantage by considering projects that take a backseat during the integration. Interestingly, many of the initiatives needed to make compliance IT lean and efficient are also relevant in a post-merger scenario. Some of such initiatives that we had proposed in an earlier article on compliance are:

- Breaking down compliance silos
- Unifying data
- Integrating detection and exceptions management

Breaking down compliance silos: The opportunity to break down compliance silos will depend partly on the post-merger legal entity structures. When the two companies are in the same business, business functions are usually streamlined and legal entities consolidated. This can offer opportunities to consolidate compliance functions with strong overlaps either in their technology requirements or in their need for product- or business-specific awareness. For example, it may be possible to combine surveillance functions monitoring equities and fixed income products. Though these products have different characteristics and demand different, there are commonalities in data capture, transaction monitoring, process automation and workflow.

The opportunities to break down these silos are fewer when the two merging entities are in different business lines.

Unifying data: It is easier to rationalize data sources within the same compliance function than doing so at the compliance organization level. Diverse data requirements and conflicting priorities make it difficult to pull off such projects. But a merger scenario offers one of the best opportunities to act on data disparities and move towards a truly consolidated data source. A centralized compliance data warehouse that takes into account all transactional data—orders, executions, positions, journals etc.—can allow the merging entities to monitor complex scenarios, provide consistency in reporting and reduce data support costs.

The biggest benefits of such an exercise will accrue when the two companies operate in similar areas. There is greater scope for a unified data model when the business processes, clients and transactions are similar in nature. There is also greater potential to cut out redundancies. However, this may be an overly complex and costly effort when two equals merge. In such cases, differences in data

across the two compliance organizations can be bridged through 'data abstraction layers' that provide uniformity in definition.

When the two companies supplement each other, the scope of such an effort is usually limited to referential data – products, clients and accounts. Differences in the nature of the businesses may not justify extensive changes to the way data is sourced and delivered.

Integrating detection and exceptions management: It is not uncommon to find compliance organizations with multiple surveillance systems. This problem is even more pronounced when both firms are in similar businesses. A careful analysis of AML, Equities and Fixed Income surveillance can reveal that though there are differences in data requirements and implementation, they exhibit common patterns in detection. These common detection patterns (for e.g. logic for aggregation, sequencing, scoring decision trees etc) can be identified and implemented in a more flexible way. This will allow firms to introduce scenarios faster and without the need for costly interface work or product enhancements. Another easier way would be to redo legacy surveillances on the detection platform retained after the merger. But this will depend on the flexibility of the product platform and the cost of customizing it.

Even when the merging entities supplement each other, there are common areas that can be streamlined as part of the merger integration effort. Processes like managing

exceptions are fairly commonplace. By developing a framework to support integrated management of exceptions, companies can reduce investigation time and gain critical insights through trend analysis. Another related area is workflow. We have often found that companies have many different workflow systems – both packaged and custom built – to cater to different process-oriented requirements. There could be workflow systems supporting exceptions routing, account opening, registrations, or employee pre-clearance. Companies need to find process overlaps and identify opportunities to bring together these disparate systems to reduce costs. Some of this effort should be made a part of the post merger integration phase in so far as it doesn't impact overall timelines.

Summary

Despite the impact of the sub-prime crisis on the financial markets, 2007 turned out to a record year for deal making activity. But the continuing credit turmoil is sure to force companies to exercise greater discipline and focus on capturing value. A phased approach to integrating the compliance IT organizations of the two merging entities can help companies to capture greater synergies. Such an approach allows for more rigorous integration planning and prioritization while taking key factors like nature of the merger, degree of functional overlap, regulatory focus and cost into consideration.



Debashis Pradhan

*Principal
Infosys Technologies Limited*

Debashis is a Principal in the Banking & Capital Markets practice of Infosys Consulting. He has about 7 years of professional experience collaborating with clients to develop and implement complex business transformational programs. His areas of focus include Regulatory Compliance, Operational Effectiveness, Data Strategy and IT-enabled Business Solutions.




Naveen Balawat

*Senior Associate
Infosys Technologies Limited*

Naveen is a Senior Associate with the Banking and Capital Markets practice of Infosys Consulting. He has more than 7 years of consulting experience in the financial services industry. His areas of focus are Private Wealth Management, Middle Office and Compliance.

For information on obtaining additional copies, reprinting or translating articles, and all other correspondence, please e-mail: bcm@infosys.com.

Global Presence	About Infosys
<p>North America Atlanta, Bellevue, Bridgewater, Charlotte, Detroit, Fremont, Houston, Lake Forest, Lisle, Mexico, New York, Phoenix, Plano, Quincy, Reston, Toronto</p> <p>Europe Brussels, Copenhagen, Frankfurt, Geneva, Helsinki, London, Milano, Oslo, Paris, Stockholm, Stuttgart, Utrecht, Zurich</p> <p>For more information, contact bcm@infosys.com</p>	<p>Infosys Technologies Ltd. (NASDAQ: INFY) defines, designs and delivers IT-enabled business solutions that help Global 2000 companies win in a flat world. These solutions focus on providing strategic differentiation and operational superiority to clients. Infosys creates these solutions for its clients by leveraging its domain and business expertise along with a complete range of services. With Infosys, clients are assured of a transparent business partner, world-class processes, speed of execution and the power to stretch their IT budget by leveraging the Global Delivery Model that Infosys pioneered.</p> <p> POWERED BY INTELLECT DRIVEN BY VALUES</p> <p>www.infosys.com</p>