

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*



Integrated Controls Management– a cost effective approach to implementing GRC

There is consensus that the current risk and compliance environment in most firms is siloed and that an integrated environment of Governance, Risk and Compliance (GRC) is the way forward. However, the common perception is GRC is expensive and will require a major IT realignment or large data base integration effort. This article tries to address that problem taking a top down approach known as Integrated Control Management approach – that will leverage existing infrastructure/controls and accrue minimal costs. The article illustrates the steps required by taking an example of a company which already has AML and SOX controls and wants to implement a GRC approach.

Uttam Purushottam
Associate
Infosys Technologies Limited

Satnam Pal Singh Gill
Principal
Infosys Technologies Limited

Ashwin Roongta
Senior Principal
Infosys Technologies Limited

Overview of trends in addressing risk and compliance

The history of financial services industry is littered with scandals or financial losses followed by reactionary compliance changes. Be it a rogue trader at Barings Bank, or a liquidity crisis at LTCM or the Enron failure, or the most recent sub-prime mortgage crisis, the past decade has seen a slew of such financial debacles. Regulatory regimes have reacted by proposing more regulations. Even though financial services firms have been complying with these regulations, there has been no respite from operational process failures or scandals that prove costly not only for the firm but the entire industry. The recent sub-prime mortgage crisis has wiped out several lending firms and has caused a severe liquidity crunch, which has brought into question the credibility of rating industries, who, in turn, are seeking to make amends by tightening the rating process through several measures. The chief among them is the decision of Standard and Poor's to rate the enterprise risk management (ERM) systems at organizations.

Analyzing past failures, it is also clear that Managements and Boards (representing shareholders) in most Cases are unaware of risk inherent in the firm's business model and processes. In some cases, like Enron, the Board had no visibility to the Management's risky initiatives, resulting in its inability to intervene and prevent huge loss to shareholders. So, it becomes imperative for not only the Management but also the Board to have a good information system that helps them stay current on all aspects related to the organization's risk and compliance. For this system to be effective, it needs to be enterprise wide with ability to extract relevant risk and compliance information from silos into a centralized system that could be used in mitigating risk and enhancing compliance.

Governance, Risk and Compliance (GRC) and why it is gaining popularity

The objective behind the Governance, Risk and Compliance (GRC) program is to have governance Processes and systems through which the board and the management can work together to reduce overall business risk, ensure better compliance and create competitive advantage for the firm. There are several external and internal drivers influencing the move towards GRC:

- Increase in scale of operation, mergers and acquisitions – Organizations need a way to manage the complexity and scale of risk and compliance of operating in multiple regional markets and across multiple lines of business.

- Change in approach to regulation – Compliance overload is forcing firms to shift away from a statute based reactive approach and adopt a more proactive approach to compliance.
- Globalization – The blurring of organizational boundaries due to international operations and outsourcing arrangements is making traditional risk management systems obsolete, forcing the need for a new and effective approach.
- Fragmentation of risk and compliance efforts – Lack of central visibility or oversight and the increased spread of siloed islands of information all over the enterprise has increased the need for a centralized system to manage risk and compliance.

Basic Components of GRC Program and challenges of implementation

Fig 1 shows the key building blocks of a GRC program. As shown, the end goal of the GRC program is to have an integrated view of all controls and risks so as to enable easy identification of areas in the business that do not have sufficient controls and yet have significant potential for financial losses. Only when the Board knows what significant material residual risks firms face, can it then force Management to act on those risks to rectify the situation. This kind of governance system can protect shareholder value, reduce business risk and create a competitive advantage for firms.

However, there are several challenges in implementing such a system.

- Perception issue – The biggest challenge is a perception that GRC is costly and needs a major IT realignment or significant data integration effort.
- Direction challenge – Although firms realize that the current approach to Governance, Risk and Compliance needs change, they do not know how to go about the same due to lack of awareness of an effective end-state.
- Senior management buy in – as many organizations do not know the real cost of current system of governance, risk and compliance, businesses cases do not really get comparable scenarios to justify the costs incurred on GRC program.
- Extreme fragmentation – Silos or fragmentation of risk and compliance activities is a serious problem – 65% of respondents who participated in an OCEG survey have been adversely impacted by redundant and inconsistent processes. They suffer from cost and pain of having to reconcile disparate data to meet GRC needs and struggle to establish a single version of the truth.

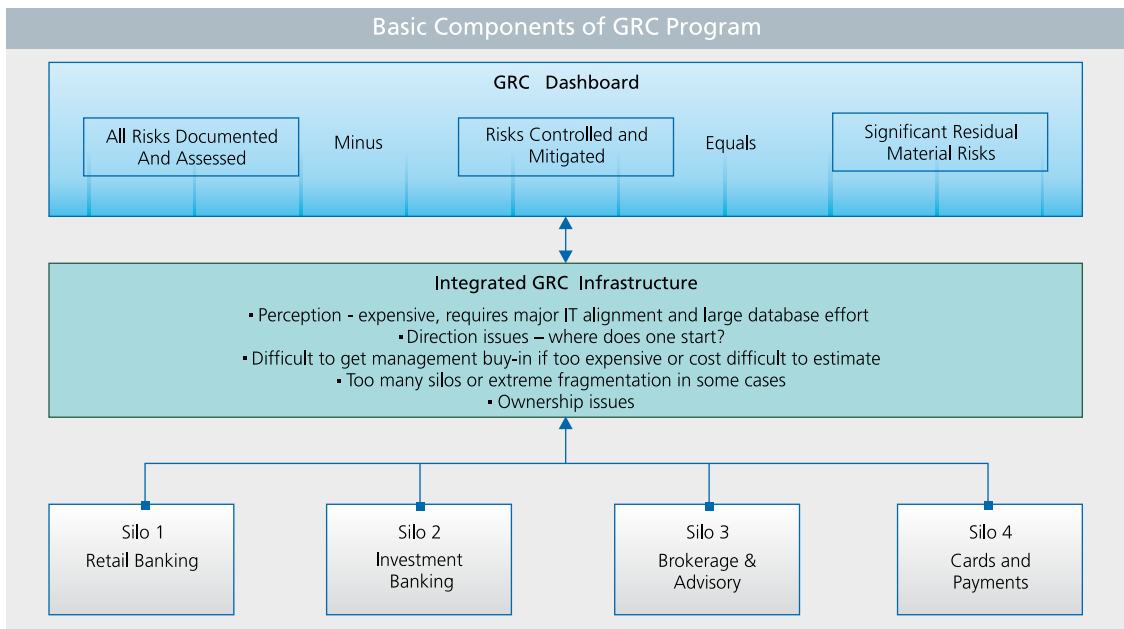


Fig 1: Basic Components of GRC Program

- Collaboration and ownership – Specialist groups such as Audit, Safety, Risk and Compliance are primarily responsible for governance, risk and compliance activities. Each of these groups has its own niche area. Getting all these groups to collaborate can be a tall order. Without the push from senior management, an effective collaboration across the organization to achieve this objective may not work.

Integrated Controls Management Approach and how it helps reduce costs

It is quite clear that there are several hurdles to implementing a GRC program. Fig 2 illustrates the Integrated Controls Management Approach which takes an evolutionary approach to address these challenges.

The implementation of the approach requires the steps described in the shaded box in Fig 2 namely:

- Create an inventory of all activities, associated risks and controls

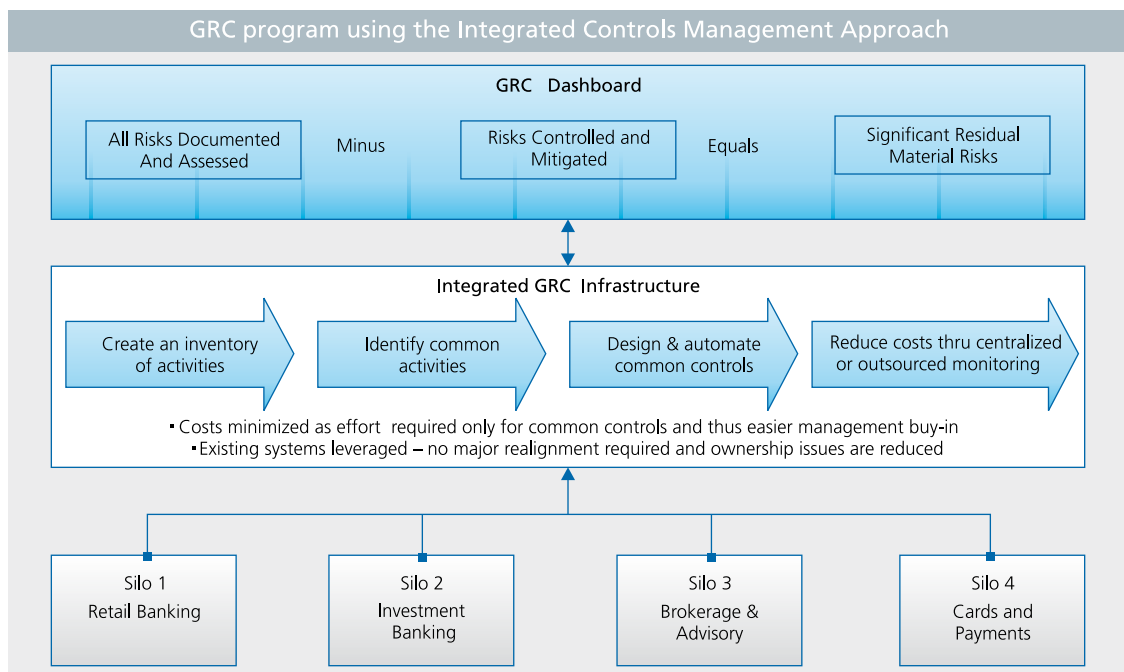


Fig 2: GRC program using the Integrated Controls Management Approach

- Assess risks and ways to mitigate
- Standardize, rationalize and automate the controls; consolidate common controls
- Reduce costs further by centralizing or outsourcing monitoring

approach. Consolidation of SOX and AML controls in Integrated Control Management approach is divided into three areas – activities specific to SOX, activities specific to AML and common activities. Integrated controls management program tries to increase the

Controls Management Processes	SOX Controls Management Activities	AML Controls Management Activities
Identify Processes	Revenue Management Processes	Funds Transfer Service
Document Processes	Define sub-processes - pricing, collection etc	Define sub-processes - KYC, relationship accounting
Identify Risks	Internal Fraud, Manipulated Revenue records	Internal Fraud, Flow of laundered money
Identify associated Controls	Revenue Recognition Controls	KYC Controls
Map controls against objectives	Compliance with COSO/COBIT	Compliance with USA PATRIOT / FAC
Design Controls	Design controls for Internal fraud, revenue manipulation	Design Controls for Internal Fraud, transactions surveillance
Deploy Controls	Deploy controls on ERM - PeopleSoft, SAP	Deploy Controls on systems - PeopleSoft, Banking software
Test Controls	Execute fraud & revenue management control tests	Execute fraud and surveillance control tests
Document Results	Store results of tests and history	Store results of tests and history
Assess Controls	Assess if fraud and revenue controls are effective	Assess if fraud and surveillance controls effective
Audit Controls	Audit of fraud and revenue controls	Audit of fraud and surveillance controls
Monitor Controls	Periodic monitoring of fraud & revenue management controls	Periodic monitoring of fraud and surveillance controls
Compliance Report	Extraction of inputs for compliance reporting	Extraction of inputs for compliance reporting

Fig 3: Illustration of sample activities for implementation of SOX & AML controls (not exhaustive)

In order to better understand let us take an example of a company which currently has separate controls in SOX and AML and wants to implement a integrated GRC program. Let us look at how each of the above steps will be implemented for this company

Create an inventory of all activities: If this was done for the above company, the activity list would look similar to Fig 3, which is an illustration of the inventory activities if SOX and AML controls were managed separately. Documenting activities can be done by the organization by leveraging existing assets e.g. organization can leverage the system that the organization might already be using for SOX or Basel II Operational Risk Management implementation.

Identify common activities and controls: Fig 4 illustrates how SOX and AML controls for this company could be consolidated using Integrated Controls Management

common activities to enhance economies of scale and scope. The same approach could be used to consolidate other compliance controls across the enterprise.

Design, rationalize and automate controls: In this step, controls across the enterprise are checked for duplication to reduce redundancy. In the case of the company above with SOX and AML, it is likely that an overlap exists in areas like internal fraud controls. This gives one the opportunity to consolidate similar controls resulting in fewer controls and reduction in costs of controls management.

Reduce further costs through centralizing or outsourcing monitoring: Controls are typically monitored in silos by specialist groups in the organization. The GRC program will need to be monitored by a centralized unit. Conflict of interests can be avoided by entrusting this activity to an external specialist organization that directly reports to the Board and Management. Monitoring activity and maintenance could thus be outsourced allowing the organizations to derive further cost benefits.

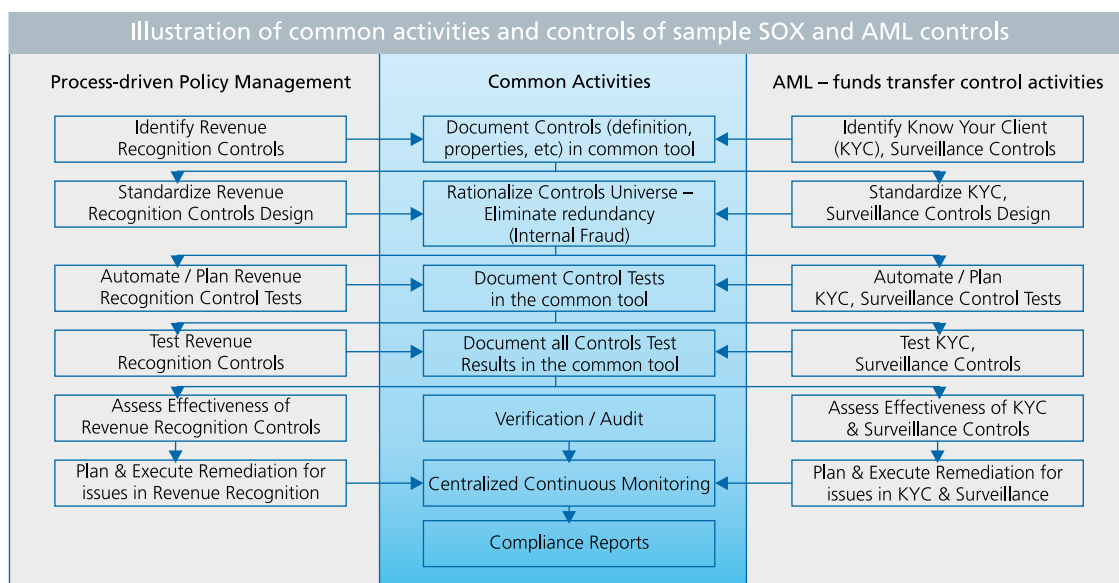


Fig 4: Illustration of common activities and controls of sample SOX and AML controls

However, implementing this approach is not devoid of challenges. Consolidation of all controls at once is a challenge and its implementation will take time. This program derives better value if done in a phased manner taking a couple of regulations (e.g. SOX and AML) at a time. Another challenge is that the bridges built to connect various silos will become redundant once IT assets are consolidated as well. However the advantage is that one does not wait for integration of IT assets to start the GRC program. The third challenge is in the management of a central controls cell, where different skills from existing ones will be required. This is where outsourcing or centralizing this function under a dedicated unit reporting to Management and Board could make sense.

The key advantage of this approach is that the organization need not wait for elimination of silos or costly realignment of IT assets. It can be achieved with existing IT assets by bridging information silos and focusing on controls that could be consolidated.

Conclusion

The Integrated Controls Management approach can help organizations move towards an integrated GRC program quickly in a cost effective manner without a large IT realignment or a major buy-in from the top management. Implementation of this approach will require organizations to consolidate controls across the organization and reduce redundancy by focusing on common control automation. Although there are some challenges in the implementation of the Integrated Controls Management approach, there are several ways to address these challenges making this a practical approach to implementing GRC.



Uttam Purushottam

Associate

Infosys Technologies Limited

Uttam is an Associate in the Banking & Capital Markets practice of Infosys Consulting. He has over 6 years of experience providing customized solutions and improving business processes of clients in financial services industry. His areas of focus are Market Regulation and Operational Risk Management.



Satnam Pal Singh Gill

Principal

Infosys Technologies Limited

Satnam is a Principal in the Infosys Banking and Capital Market Practice. He has over 20 years of experience in global banking and consulting. His area of expertise is in Governance, Risk and Compliance and his consulting work has included impact studies, business process re-engineering, business-IT alignment and offshore program management. He is a Certified Anti-Money Laundering Specialist (CAMS).




Ashwin Roongta

Senior Principal

Infosys Technologies Limited

Ashwin is a Senior Principal responsible for managing client relationships at Infosys' Banking & Capital Markets Practice. He has over 11 years of consulting experience. His primary areas of expertise include the wealth management space and treasury and risk management. Ashwin holds a Financial Risk Manager certification from GARP and has completed his CFA Level III exams.

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>