

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*



Conversations with Tim Leech – Perspectives from an industry expert

The objective behind the Governance, Risk and Compliance program or simply GRC as it is called, is to have governance processes and systems through which Board and Management can work together to reduce overall business risk, ensure better compliance and thereby, create competitive advantage for the firm.

In this article, Satnam Gill interviews Tim Leech, an industry expert to get a better perspective on GRC.

Satnam Pal Singh Gill
Principal
Infosys Technologies Limited

Tim Leech
Director
Navigant Consulting

Satnam Gill (SG): *We are observing a movement away from Enterprise Risk Management (ERM) towards Governance, Risk and Compliance (GRC). What is really behind this movement?*

Tim Leech (TL): The IT vendor community plays an important role in dreaming and envisioning solutions that have the ability to reduce one or more customer pain points. GRC is one of those examples where the IT vendors are seeing clients suffer compliance overload. Sarbanes Oxley, AML, Basel II, Gramm-Leach-Bliley (GLB) the list goes on and on. This is accentuated by resurgence in enforcement of Foreign Corrupt Practices Act (FCPA) in USA and MiFID in Europe. Vendors watch, see, hear and read about these customer pain points and think about ways to offer solutions to treat this “regulatory compliance overload” pain point. What we have seen is that many companies aren’t willing to buy risk management systems for the pure beauty and comfort of risk management - a growing number will buy it to relieve pain points, things like large compliance cost increases, embarrassing press coverage, large punitive law suites, huge settlements that impact shareholder return, credit agency negative grades etc

SG: *How does banking industry compare with other industries in terms of evolution from ERM to Integrated GRC?*

TL: Right now the demand for integrated GRC is most prominent in the banking and the insurance sectors, in that order. Sarbanes-Oxley in my opinion has significantly set back the ERM movement because the SEC/PCAOB rules have focused on documenting and testing controls with limited focus on true risk assessment. The good news is that Basel II really elevated the idea, at least in the banking sector, that an effective enterprise-wide risk approach should have direct correlation with reserve capital. If banks prove good risk management systems, they can have less reserve risk capital, which all other things equal, is a competitive advantage.

Large strides are being made by banking industry to put in place high quality risk management systems due to incentive provided by Basel II. It is also because a “perfect storm” of regulatory regimes is causing banks to comply with Basel II reforms at the same time that they are being forced to implement AML, SOX, MiFID in Europe and other regulatory reforms.

SG: *Why is there such a strong need for a new approach of looking at risk and compliance when the industry is already using other approaches?*

TL: I think we need to step back and look at the fundamental issue of whether compliance has been

approached using a fact-based approach and whether it has applied the learning of the Quality movement. In my work with the Institute of Management Accountants (IMA) we are studying the frequency of restatements of financial statements issued by large accelerated filers in the US that have now gone through at least three full rounds of Sarbanes-Oxley section 404 assessment and testing. In companies that we are analyzing, both management and the company’s auditors, after doing an extensive amount of work formed an opinion that accounting controls were “effective”. In spite of that, we are seeing a rate of material errors in those large accelerated filers of more than one in ten. Given the amount of money being spent on compliance, why the world hasn’t focused much energy or serious attention rigorously researching why governance and particularly risk and control governance, systems fail is a question that needs to be asked.

SG: *GRC is made up of three complex disciplines of governance, risk and compliance and some organizations have different “silo” based manifestations in the form of IT GRC, Finance GRC and so on. Where should an organization begin?*

TL: To move away from silo based approach of current GRC, a decision at the top to create a single consolidated report on the significant residual risks facing the organization is required. Charging an individual with producing that consolidated report is one of the biggest steps a company can take to start the process of assurance system integration. In most companies today, the head of internal audit comes to the audit committee and talks about certain risk areas, the external auditors come and talk about financial statements and financial statement controls, the law department comes and talks about legal issues, the safety and environment, Anti-Money Laundering (AML) and Foreign Corrupt Practices Act (FCPA) etc. However in many organizations nobody comes to the board and talks about customer service, product quality issues and a host of other issues important to the long term success of an organization or what issues are falling through the specialty silo cracks. Risks related to sub-prime mortgages is classic example. The approach I recommend focuses on establishing an environment where business units take primary responsibility for reporting on significant risks they face in the operations and the specialist groups play more of a role reporting on how well the business units are disclosing where the significant risks are.

SG: *Within the approach recommended by you, what role will this specialist risk and assurance group play?*

TL: A risk and assurance group quite simply has to act as the catalyst to ensure that the necessary motivation,

tools, training and reporting processes are developed, implemented and sustained to produce reliable consolidated reports on residual risk status for the senior executive of a company and their board.

SG: *As CFO, CIO, CTO, CISO, CCO and CRO are all key stakeholders in GRC, where does one begin in terms of stakeholders?*

TL: The journey begins with decisions at very senior levels on the target destination. As a general statement, most audit committees tended to focus heavily on financial reporting risk which is only one dimension of the total array of risks a company faces. When we do training at the board level, one of the things we suggest to the board is to consider asking for a consolidated current report on the significant residual risks in the company of all types that could materially and negatively impact the company. When board asks for a report like this it immediately creates a chain reaction that works its way down and across the organization. If the report didn't mention an area in risk assessment and that area subsequently comes along and causes a major embarrassment and the company's shares to drop by 10%, the company should rethink how information is gathered to prepare the residual risk report. Boards should want a report that doesn't have perfect predictive accuracy, but does have reasonable predictive accuracy.

For example, we are talking about an approach where boards of directors of all of the major banks that had this sub-prime exposure should have been told there was at least some chance that these investments could implode with negative loss risk scenarios running into billions of dollars. If board of directors and senior management were given reliable information on retained risk and said "OK, we are on board with this," fair enough; that is what business is about, calculated and conscious risk taking. That's the end game we are looking for – conscious, consensus agreement on tolerable residual risk.

SG: *How does an organization go about developing a business case for Integrated GRC?*

TL: The business case analysis should start with an inventory of what I call the current cost of formal assurance. Very few companies have even an approximate idea of how much money they spend on formalized assurance. When inventorying the current cost of assurance, my experience with companies is that they are often shocked at how much money is being spent. When you add up the work of the internal auditors, the external auditors, the lawyers working on compliance, the compliance department, the SOX work, AML work etc together with the time compliance related issues

take away from management and business unit staff etc. it can be staggering. If a company is spending a lot on compliance and still having a lot of very bad outcomes, it should certainly be cause for a re-evaluation. I am very confident that an integrated GRC system, properly developed and implemented, can cut total enterprise risk and assurance costs by 20-30% and produce better consolidated reports on retained risk than the current silo-based assurance approaches

SG: *What should be the objective of an integrated GRC platform?*

TL: Simply put, I think an integrated GRC system is one capable of producing reliable consolidated reports on the most significant residual risks related to all areas of an organization's operations.

SG: *What is the notion of GRC-IT maturity model and how could future GRC technology evolve?*

TL: OCEG, (Open Compliance & Ethics Group) classifies maturity of GRC IT capability in organizations into five stages – Unaware, Fragmented, Integrated, Aligned and Optimized. 'Unaware' is first stage where firms have adhoc approach to technology. In 'Fragmented' stage, firms have tactical and "siloed" approach to technology with no information exchange between silos. In 'Integrated' stage, silos are broken down and unified approach created for GRC. In 'Aligned' stage, firms have strategic approach to aligning GRC with business and GRC technology consolidated across the firm. In 'Optimized' stage, firms optimize GRC platform making no distinction between GRC and non-GRC technology.

We need to merge the power of IT with a continuous improvement framework to reduce error frequency and, in the case of risk management, reduce the frequency of big risks materializing that we hadn't thought about or severely under-estimated. OCEG is doing a lot of excellent work to raise the profile and business case for GRC.

SG: *It looks like the banking industry is well ahead from a GRC-IT maturity model stand point. So, do you think banks will be in a better place from Integrated GRC perspective?*

TL: Yes and No. I am concerned that the bank regulators are going to make the same fundamental errors that the SEC and the PCAOB have made. In the case of Sarbanes-Oxley section 404 reforms, the result was supposed to be fewer incidences of materially wrong financial statements. In the case of the bank regulators, I am not sure that they have fully articulated exactly what the end results should be. I guess from my work it would be fewer instances where people that provide banks

with funds lose their money and/or regulators have to bail out the banking sector because of big mistakes. My point here is that regulators need to carefully research whether all regulatory interventions, especially the costly ones, are in fact achieving the intended results, assuming the intended results have been clearly articulated in the first place.. The question needs to be asked loudly and often - have the regulatory steps prescribed actually started to cure the perceived problem? In the case of SOX, our research suggests billions have been spent and there is at least some evidence in the form of accounting restatement statistics and that suggests U.S. listed financial statements, at least based on restatement statistics from companies like Audit Analytics, are less reliable. Regulators should, by law, have to regularly and publicly report if laws and regulations they enact are accomplishing the intended outcomes.

SG: *Based on your experience, what are the key data requirements for an integrated GRC initiative?*

TL: The integrated GRC data element overview I have developed to help clients see the “big picture” starts with an identified universe of “assurance contexts”. These are objectives, business areas and end results for which the organization believes some form of formal assurance is required. For state of the art risk and control assessments, data that documents risks, controls, residual risk data, loss events, action plans, key risk indicators, escalator triggers, warning indicators, correlated factors, relevant policy and other elements are required. Then we add relevant external data that helps an organization better evaluate and understand risk likelihood and consequences. All too often people form subjective and seriously wrong views on risk likelihood and consequence. Wrong decisions in this area can literally kill you. Other relevant external data is information that helps you understand where your organization is relevant to others in your industry as well as globally. All this data helps an organization form more reliable views on the severity and acceptability of their current residual risk status. We recommend that senior executives get one simple report that shows all the residual risks that have a “Residual Risk Index (“RRI”)” of 4 or higher. This helps reduce a complicated world to a manageable number of issues. An RRI of 7 for example is called terminal and refers to situations where the retained risk is capable of leading to the demise of the entire organization.

SG: *Is an off-the-shelf integrated GRC solution possible? If not, how far are we from a true integrated GRC solution?*

TL: No. There has been a major void in the way assurance profession, external and internal audit approached the task of coming up with methods that actually work

with high reliability. Part of the problem is the current highly litigious environment in the U.S. It discourages collection and analysis of the root causes of material control breakdowns because of fears that it will be used against the company, the board and management.

However, not doing cause of failure analysis in a rigorous and systematic way also increases the risk of a continuation of major failures in the future – a tough dilemma. The challenge is, can we develop a system that encourages conscious disclosure and assessment of risks or are we doomed to a situation, especially in the U.S., where companies and people are encouraged by the litigation environment to hide information about risks and continue to suffer ill effects that come from inadequate analysis of systemic risk trends? I am increasingly concerned that U.S. companies are “rationally precluded” from doing a better job to manage risks of all types because of the very valid and real fear of having the retained risk data used against them when 20/20 hindsight proves one of their risk acceptance decisions was wrong.

The main challenges to integrated GRC are structural barriers and constraints due to silos, absence of a senior executive appointed to produce consolidated residual risk reports and lack of awareness in higher echelons on finding a better and cheaper way to approach assurance. I could argue that change and better solutions would emerge faster if the Chief Risk Officer is called Chief Risk and Assurance officer and charged with producing integrated enterprise reports on residual risk.



Tim Leech

*Director
Navigant Consulting*

Tim is a Director in the Toronto office of Navigant Consulting, a major independent consulting firm headquartered in Chicago, Illinois. Tim leads Navigant's Risk and Control Governance practice (RCG). RCG service offerings include risk and control governance consulting, integrated Governance, Risk and Compliance (GRC) implementation assistance, entity-level assurance optimization reviews, Sarbanes-Oxley 404/NI 52-109 efficiency/effectiveness reviews, Anti-Money Laundering (AML) compliance reviews, enterprise-wide anti-fraud assessments, ERM training and consulting, internal audit advisory services, Basel II operational risk reviews and implementation support and expert witness services related to actual and/or suspected risk and control governance break-downs.




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).

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>