

# 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 &amp; 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*

# FINsights

Technology Insights for the Financial Services Industry



## Demystifying financial compliance through an integrated IT framework

Over the years there have been a number of frameworks and standards to address compliance issues in IT. This article examines these frameworks and defines an integrated framework that when implemented in the IT products and services arena, will help organizations achieve regulatory compliance, superior quality standards and business competitiveness.

Ravishankar N.  
*Principal Consultant*  
*Infosys Technologies Limited*

Ramachandran Sundaresan  
*Senior Consultant*  
*Infosys Technologies Limited*

## Current Challenge

Models, frameworks and standards such as COBIT®, CMMI®, ITIL® and Six Sigma have provided organizations with tangible benefits. These models, by and large, focus on a single main theme as follows

- COBIT® on IT Controls
- CMMI® on Software Process Improvement
- ITIL® on Service Delivery and
- Six Sigma on continuous improvement in customer satisfaction

Thus, when the implementation of these models and frameworks is done in isolation, an IT organization would only achieve limited success in specific areas and may tend to lose out on seeing the benefits of the synergies.

On the other hand, implementing all of these would lead to process proliferation, resulting in some level of confusion. This could also result in competing or conflicting goals and a blurred organizational focus across multiple diverse objectives. Without stringent gating and benefits tracking some of these improvement initiatives would have to be shelved or abandoned altogether.

of Governance, Risk and Compliance, Application Development and Maintenance (ADM) process improvement, better support, service delivery and customer satisfaction.

To adopt an integrated approach to quality improvement, governance and compliance it is important to identify the synergies of the models described above and explore avenues for leveraging the synergies. A first step towards this is to look at how these models compare with each other and then utilize the best of each model placing them in the perspective of GRC and competitiveness in an IT environment specifically for Banking and Financial Services domain.

As shown in Fig 2, although each of these models serves specific overall objectives, they have commonalities that could be leveraged for competitive advantage. For example, the tools and techniques of continuous improvement methodology such as Six Sigma could be applied across any functional layer in an IT organization along with the specific components of the other models and frameworks such as COBIT®, CMMI® and ITIL®.

COBIT® can be considered as the umbrella framework that encompasses best practices in all phases of the IT lifecycle at a high level – from business case to

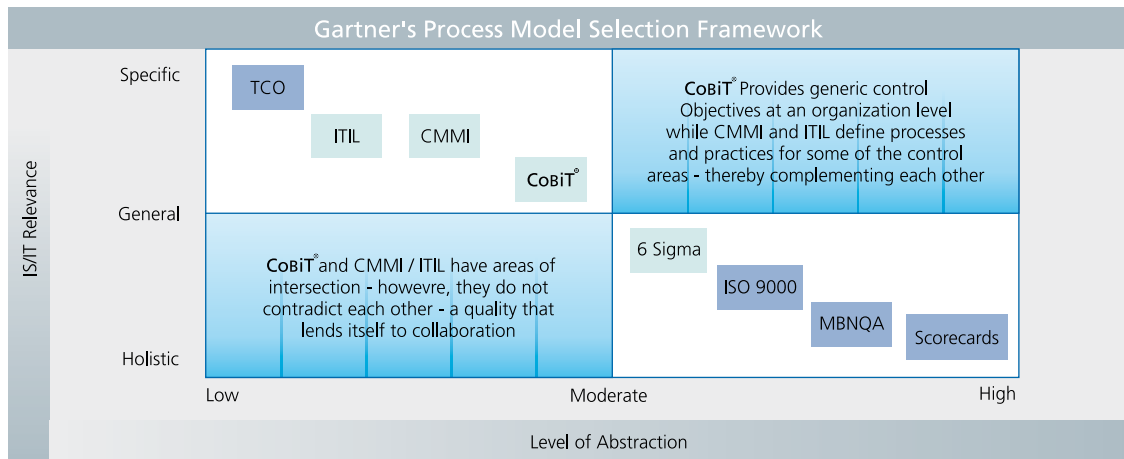


Fig 1: Gartner's Process Model Selection Framework

Although Fig 1 depicting the Gartner Process Model Selection Framework is useful in visualizing where each of the models being discussed would fit in the overall scheme of things, it still does not address the problem effectively as many of the frameworks have overlapping commonalities.

## Proposed Integrated Framework

The current business imperative therefore is to have an integrated framework that reaps the benefits of these and takes advantages of the synergies in the areas

decommissioning of an IT asset. COBIT® serves as the preferred framework amongst banking and financial services companies to support the key objectives of IT Governance and Control.

CMMI® defines 5 Maturity Levels - each level describing specific process areas with specific practices across the Application Development and Maintenance (ADM) lifecycle. CMMI® has been the differentiator of competitiveness on the basis of quality in the ADM area of Banking and Financial Services companies.

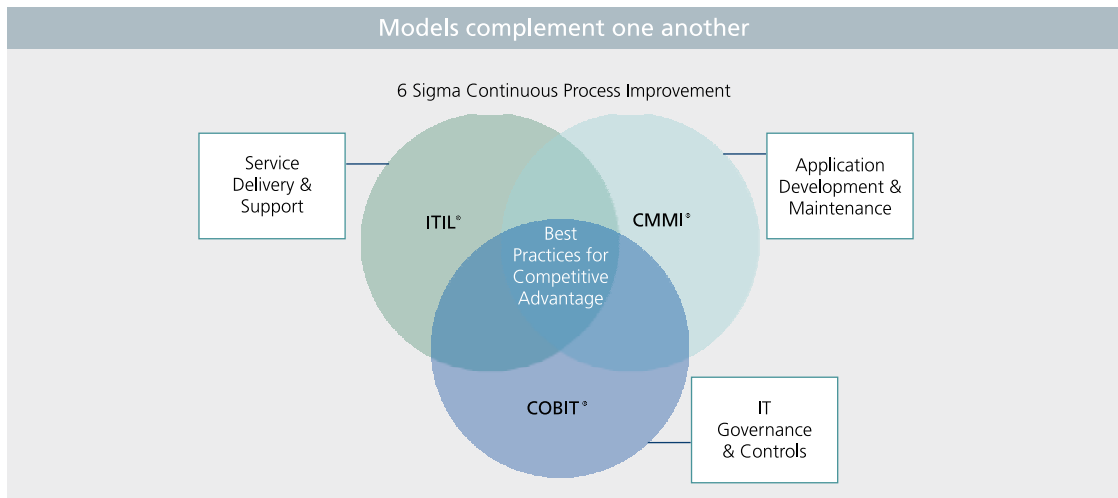


Fig 2: Models complement one another

ITIL® addresses the Production Support and Service Delivery space and comprises 5 core volumes: Service Strategy, Service Design, Service Transition, Service Operation and Continual Service Improvement. It focuses on the management of life cycle of the IT Services and the importance of creating business value.

benefit from the synergies in terms of optimal utilization of resources avoiding effort duplication and cost over runs.

The above integrated framework provides a structure and a discipline for IT processes using the industry best practices and the synergies of models. It also provides the necessary flexibility to include new practices and tailor

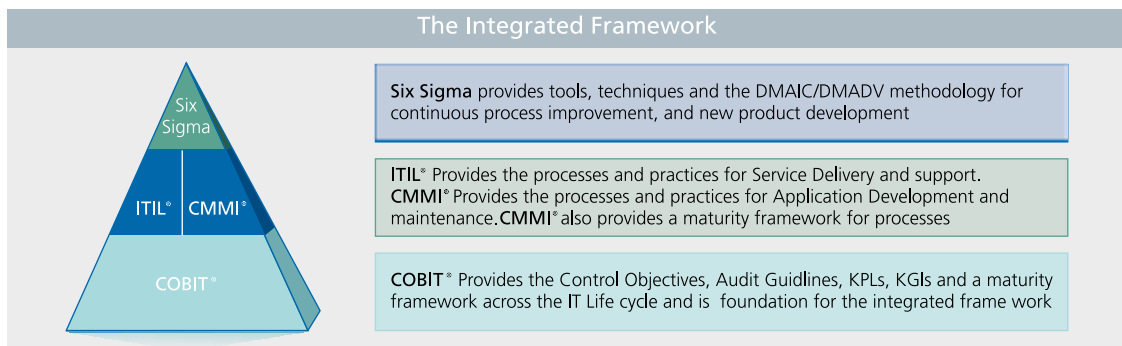


Fig 3: The Integrated Framework

Six Sigma has two key methodologies DMAIC (Define, Measure, Analyze, Improve and Control) used to improve existing processes and DMADV (Define, Measure, Analyse, Design and Verify) used to create new product or designs for predictable and defect free performance. Six Sigma provides a number of tools and techniques aimed at a statistical approach to continuous process improvement with customer satisfaction as the key goal.

The mapping between the various models previously discussed leads to the following integrated framework shown in Fig 3, where the IT organization of a Banking and Finance organization could tap into the best practices offered by each of the models / standards and

the existing processes and procedures to cater to the updates in compliance regulations from time to time.

### Application of the Integrated Framework

The following scenarios highlight as to how Banks and Financial Institutions can leverage the synergies of the integrated framework to address specific compliance requirements while maintaining competitiveness and achieving reduction in cost of compliance and quality. The scenarios show which components of the Integrated Framework could be applied to the specific requirements of regulations such as SOX, Gramm-Leach-Bliley Act and Basel II.

### Scenario-1 : SOX Controls and Integrated Framework

#	Compliance Specifications	Guidelines to apply Integrated Framework Components
1	Evaluating IT General Controls (Management Assessment of Internal Controls Sec 404)  Specific Requirement: There should be an access control policy that provides users privileges to view / add / change / delete interest rates on deposits on a need to have basis in a Banking organization	<ul style="list-style-type: none"> <li>ITIL® Incident Management process area: Incidents and transaction logs will help detect and respond to unauthorised access</li> <li>COBIT® Control Objective AI 6: Manage Changes ensures that changes performed are authorized and conform to appropriate change standards and procedures</li> </ul>
2	Evaluating IT Application Controls (Management Assessment of Internal Controls Sec 404)  Specific Requirement: System controls should be in place to segregate posting and approval functions	<ul style="list-style-type: none"> <li>COBIT® Control Objective: AI 2: Acquire and Maintain Application Software – AI 2.3 Application Control and Auditability ensures business controls, where appropriate, are implemented into automated application controls such that processing is accurate, complete, timely, authorized and auditable</li> </ul>
3	Evaluating Controls at vendor organization – Specific Requirement: PCAOB Auditing Standard 5 (SAS 70 and SAS 70 Examination Reports)	<ul style="list-style-type: none"> <li>CMMI® Supplier Agreement Management process area - SP 1.3: This specific practice provides the processes and best practices to establish Supplier Agreements where the required internal control processes expected at the vendor organization can be mandated. SP 2.2 and 2.3 provide the processes to monitor and evaluate the processes at the vendor organization.</li> </ul>

### Scenario-2 : Gramm-Leach-Bliley Act and Integrated Framework

#	Compliance Specifications	Guidelines to apply Integrated Framework Components
1	Privacy Controls (Privacy Rule of GLBA – 16 CFR Part 313)  Specific Requirement: Banks have data classification rules and access is provided to third parties in accordance with the rules. Customers are provided with Opt Out clauses.	<ul style="list-style-type: none"> <li>COBIT® Controls to maintain Confidentiality, Integrity and Availability of Data (Information criteria)</li> <li>COBIT® Control Objectives Data Classification Scheme PO 2.3 and DS 11 Manage Data ensure that an Application has in built business rules to classify data</li> <li>ITIL®IT Security Policies and Procedures help maintain confidentiality of customer data</li> </ul>
2	Safeguards Customer Non Public Personal Information (Safeguards Rule of GLBA – 16 CFR Part 314)  Specific Requirement: Develop, implement and maintain a comprehensive written information security program	<ul style="list-style-type: none"> <li>COBIT® DS 5 Ensure Systems Security and in particular DS 5.11 Exchange of Sensitive Data</li> <li>ITIL® Security and Incident Management Process Areas</li> </ul>

### Scenario-3 : Basel II and Integrated Framework

#	Compliance Specifications	Guidelines to apply Integrated Framework Components
1	Basel II First Pillar – Minimum Capital Requirements: Manage Risk.  Specific Requirement: Risk of Unauthorized Change: The bank or financial institution has appropriate IT Controls to detect / prevent an unauthorized change	<ul style="list-style-type: none"> <li>COBIT® AI 6 Manage Change / AI 6.2 Impact Assessment, Prioritization and Authorization of Changes: Defines the control objectives / practices and audit guidelines to manage change</li> </ul>

#	Compliance Specifications	Guidelines to apply Integrated Framework Components
2	Basel II First Pillar – Minimum Capital Requirements: Operational Risk Management Specific Requirement: The bank or financial institution recovers quickly from any disruption or disaster	<ul style="list-style-type: none"> <li>• COBIT® Business Continuity controls are defined and in place (COBIT).</li> <li>• The application has been designed to avoid single points of failure (DFSS, FMEA of Six Sigma)</li> <li>• ITIL® The application provides for redundancy (IT Service Continuity and Availability processes from ITIL)</li> </ul>
3	Basel II Second Pillar – Supervisory Review: Sound Capital Assessment Specific Requirement: The bank has policies and procedures to ensure that it identifies, measures and reports all material risks affecting capital	<ul style="list-style-type: none"> <li>• COBIT® Risk Management is one of the key IT Governance focus areas of the COBIT Framework and is embedded in a significant number of control objectives</li> <li>• ITIL® Service Delivery and Service Level Management process area address IT Operations Risk</li> </ul>

Six Sigma, being a data driven approach, instinctively appeals to banking and financial services companies; It provides the tools and techniques required to continuously improve COBIT® controls, CMMI® /ITIL® processes and practices. Six Sigma can be implemented on top of COBIT®, CMMI® and ITIL® as a focused methodology that ensures products and services with zero defects for critical compliance requirements while achieving customer satisfaction and reducing Cost of Quality as resultant benefits.

## Benefits of the Integrated Framework

The benefits of the proposed integrated framework have been indicated in the above sections. To summarize:

- The framework gives a structure and a path in the pursuit of competitiveness while fulfilling GRC obligations
- Instead of the ‘one size fits all’ paradigm, components of each of these models are utilized based on organization’s specific objectives

- Increased alignment of business, IT and quality goals – constant focus on re-alignment of business, IT and quality goals
- No over-dependence on one model – a holistic approach that leverages the best of what each model has to offer
- Control alone is not the focus – while GRC is key to an organization’s survival, customer satisfaction and continuous process improvement help achieve and retain the competitive edge

## Conclusion

Increasingly, organizations in the Banking and Financial Services industry are subject to stringent regulations to prevent irregularities. In pursuing GRC, there is a danger of organizations losing the competitive edge. Models implemented in isolation could result in confusion, duplication of efforts and cost overruns. An integrated framework marrying organization’s issues and needs with the best practices from the various models is imperative.



**Ravishankar N**  
Principal Consultant  
Infosys Technologies Limited

Ravishankar is a Principal Consultant in the Infosys’ Quality Consulting Practice. He has over 15 years of experience in the software industry and works with customers in the US, UK and APAC to improve their software quality processes. His area of expertise is in software process and quality engineering.



**Ramachandran Sundaesan**  
Senior Consultant  
Infosys Technologies Limited

Ramachandran is a Senior Consultant in the Infosys’ Quality Consultant Practice. He has over 12 years of experience in Management and IT Consulting. He has consulted on quality process improvements to clients in the US, UK, Japan and APAC regions. His area of expertise is in software process and quality engineering.

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

## Global Presence

### North America

Atlanta, Bellevue, Bridgewater, Charlotte, Detroit, Fremont, Houston, Lake Forest, Lisle, Mexico, New York, Phoenix, Plano, Quincy, Reston, Toronto

### Europe

Brussels, Copenhagen, Frankfurt, Geneva, Helsinki, London, Milano, Oslo, Paris, Stockholm, Stuttgart, Utrecht, Zurich

### Asia Pacific

Beijing, Hong Kong, Mauritius, Melbourne, Shanghai, Sharjah, Sydney, Tokyo

### India

Bangalore, Bhubaneswar, Chandigarh, Chennai, Hyderabad, Mangalore, Mumbai, Mysore, New Delhi, Pune, Thiruvananthapuram

For more information, contact [bcm@infosys.com](mailto:bcm@infosys.com)

## About Infosys

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.

**Infosys**<sup>®</sup>  
POWERED BY INTELLECT  
DRIVEN BY VALUES

[www.infosys.com](http://www.infosys.com)