

FINsights

Technology Insights for the Financial Services Industry

Governance, Risk and Compliance »



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*

FINsights

Technology Insights for the Financial Services Industry



Leveraging SaaS to manage GRC

Companies are overwhelmed with the task of managing risks and compliance across regulations, functions, regions and lines of businesses. There is increase in scrutiny from regulators and investors. The cost of compliance has risen substantially. Additionally, business environments in many firms have become too restrictive due to too many controls.

Companies can overcome the challenges of Governance, Risk and Compliance (GRC) by adopting an Enterprise SaaS Model.

Ravi Uppaladinni
Senior Associate
Infosys Technologies Limited

Vishakha Chhawchharia
Senior Consultant
Infosys Technologies Limited

Increased risks due to increase in business complexity

In recent times corporations have adopted aggressive growth strategies, both organic and in-organic, that have resulted in the creation of 'extended enterprises'. In the process, companies have exposed themselves to risks across varied regulatory compliance domains, geographical regions and lines of business. One of the critical challenges facing corporations is the convergence of disparate cultures and processes and the associated lack of a unified risk management approach that can result in unfavorable events with widespread repercussions.

Companies are subject to a wide array of cross-sector and sector-specific regulations that pose considerable management challenges. New regulations are emerging at a rapid pace, many with overlapping intent and requirements. Yet, in most companies risk management and compliance programs are run in isolation. Most of the compliance processes are manual, effort-intensive, non-standardized and prone to errors and delays.

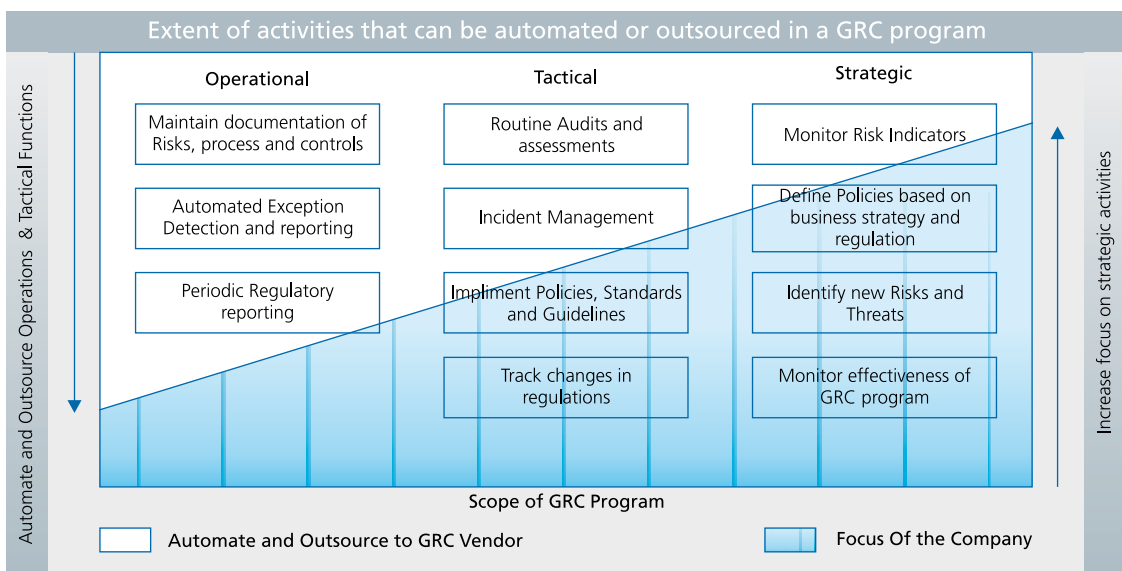
There is additional pressure from directors and investors who are dissatisfied with the current state of governance and believe that they don't have enough visibility about the drivers and risks the company faces. Companies are beginning to establish a risk management organization structure and invest in enterprise-wide GRC technology solutions.

their specific requirements for risk management and regulatory compliance. Adopting such a tactical approach for managing GRC has created its own set of challenges

Monitoring and managing risks across domains, functions and regions: Executives lack holistic information about multifaceted risks which need to be considered for making decisions in today's complex business environment. For example: An executive needs information about a wide range of risks to make an informed decision about sourcing material. He needs to continuously monitor information about political risks in that country, the regulatory risks, foreign currency fluctuations, commodity price risk etc.

Lack of actionable intelligence is often the most important reason for GRC violations. Non-compliances can invoke severe fines, damage market standing and also threaten the sustainability of a corporation.

Escalating cost of compliance: There has been a steep increase in ongoing compliance management costs due to globalization, mounting regulations and pressure from investors. The traditional siloed approach to compliance management is resulting in duplication of efforts for regulations with overlapping requirements. For example, large organizations are impacted by several financial reporting and data privacy related regulations and running separate programs for each regulation results in significant duplication of efforts.



Multifaceted GRC Challenges

Companies recognize criticalities of GRC but continue to suffer regulatory setbacks in spite of executive commitment and large investments in compliance programs. Departments and units within a company have disparate processes and technologies to meet

Fig 1: Extent of activities that can be automated or outsourced in a GRC program

Inability to scale up and respond to non-compliance quickly: Lack of a standardized and repeatable GRC process hinders a company's ability to expand into new markets and regions. Companies are unable to respond

swiftly to regulatory changes that are emerging at a rapid pace. They face difficulties with respect to interpretation of regulatory developments and roll-out of process changes to meet new requirements within set timelines.

Constrained and inefficient business operations: Regulations like Sarbanes-Oxley, Basel II, Customer Compliance and Trade Surveillance have widespread impacts. However multiple stakeholders (process owners, department managers, auditors, senior management, risk officers) added additional controls without analyzing the effect on a company’s operations and the impact of other regulations. Such a scenario has resulted in a business environment that is overly constrained and inefficient.

Key Elements of unified GRC strategy

How can companies overcome GRC challenges and prevent unaffordable regulatory violations? Employees in GRC functions spend significant time doing routine activities like assessments, regulatory reporting, transactions monitoring, document management that are operational and tactical in nature. An organization should explore if such activities can be automated or outsourced.

As shown in Fig 1, there is more scope for outsourcing and automation of operational and tactical activities. An organization can thus improve the effectiveness of their GRC program by partnering with GRC vendors for activities that can be automated and outsourced and have company resource focus on strategic activities. Automation and outsourcing can address many of the GRC challenges. However, before a company can automate and outsource, it would have to do the following:

| Key element | What the company has to do |
|-------------|---|
| Automation | <ul style="list-style-type: none"> ▪ Automate GRC Management including policy management, audit management, incident management and reporting ▪ Automate Control monitoring ▪ Adopt a common framework to integrate multiple risks and regulations ▪ Optimize controls by reducing overlapping and ineffective controls |
| Outsourcing | <ul style="list-style-type: none"> ▪ Outsource monitoring of controls to resources who identify exceptions by using a combination of automation tools and business knowledge ▪ Outsource Incident management and hotline where trained resources capture and respond to incidents |

Leveraging the SaaS Model for GRC

Although automation and outsourcing can be achieved using a traditional build or buy model, the traditional software model does not provide the flexibility, responsiveness and cost efficiencies that are much required.

GRC platform is increasingly being offered on an on-demand (SaaS) model, where the vendor hosts the applications and platform for the customer and charges on a subscription or per use basis. Several large and medium-sized companies have adopted GRC solutions on SaaS model with a great deal of success. According to a Gartner report published in September 2007, “businesses adopt GRC SaaS solutions 15% - 20% of the time over a licensed, on-premise application for regulatory compliance”.

There are significant benefits in adopting SaaS for GRC.

Lower upfront and ongoing capital investment due to a usage based pricing model: Software is treated as an operating expense. The upfront cost investment that is required for an in-house platform is not required. On-demand SaaS applications also enhance the ease and speed of roll-outs and upgrades thus reducing the total ongoing cost of compliance.

Better responsiveness: Since GRC is not a revenue generating activity, risk officers cannot readily command IT support in their organization. Adopting GRC on SaaS model solves this problem. Since a single vendor usually owns the complete process lifecycle, including software, hardware and infrastructure upgrade and maintenance, there is quicker access to newer functionality due to changes in regulations and emerging best practices.

Extensible knowledge or business intelligence services can be tightly integrated with the GRC software platform. The following kinds of services can be provided on the GRC platform:

- Regulatory intelligence
- Continuous monitoring of exceptions (automated monitoring and BPO services)
- Incident Management

As shown in Fig 2, a large number of features can be built using a SaaS platform with maximum benefit accruing in the operational and tactical areas.

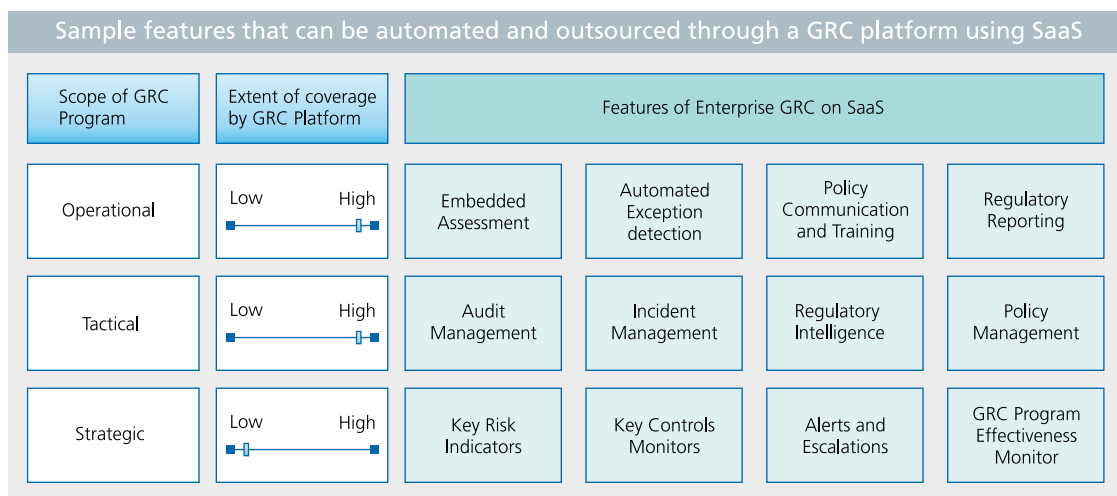


Fig 2: Sample features that can be automated and outsourced through a GRC platform using SaaS

What should be the key components of a GRC Platform using SaaS?

The GRC platform through SaaS should comprise of four key components as shown in Fig 3.

Process-driven Policy Management: Development, documentation and communication of policies, procedures and controls across compliance domains, geographies and business units. Features can include compliance documentation management, collaborative process modeling and training.

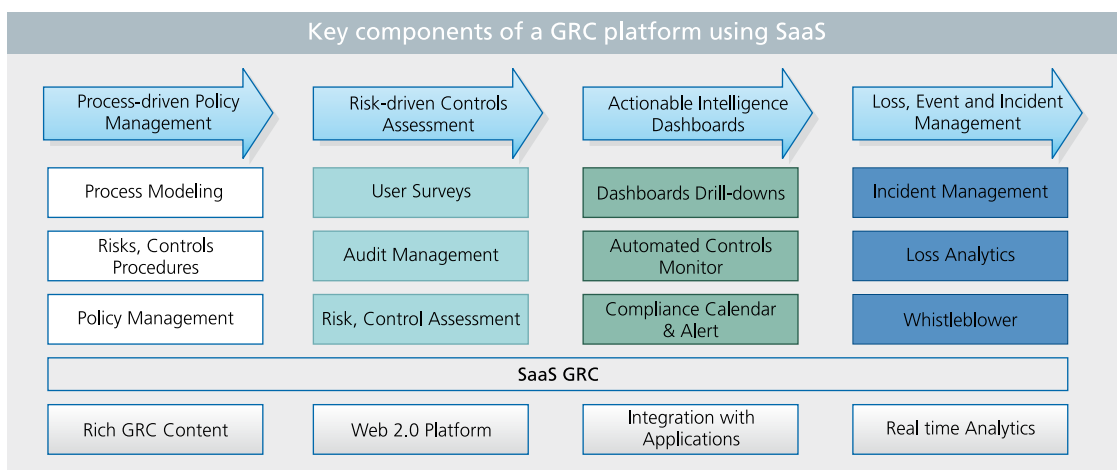


Fig 3: Key components of a GRC platform using SaaS

Actionable Intelligence Dashboards: Role-based dashboards and drill-downs can provide actionable intelligence from existing transaction and silo-ed compliance management systems and provide user interfaces for un-systemized but critical compliance intelligence. Early warning and alerts on process deviations can enable real-time monitoring of GRC performance and prevent regulatory violations through an early-warning escalation mechanism.

Loss, Event and Incident Management: Collection of records for tracking organization losses, events, gaps in controls, audit findings and management of the investigation & response process.

Risk-driven Controls Assessment: Ongoing assessment of risks and controls will be key and this includes identification of problem areas using guided assessment wizard, end-user surveys and hypothesis-based approach.

In addition, it is important that the SaaS model has the following elements to make it suitable for GRC for large organizations

Robust and flexible architecture with high level of security

- Application should be highly configurable and flexible, so that it can meet the diverse requirements of different business units in an organization
- Data for each customer should be stored in independent database instances

- Option to store sensitive data within the firewall of the organization

Extensible with high level of integration

- The GRC SaaS system should be able to integrate with transaction systems and existing GRC systems
- GRC SaaS Vendor should meet the standards for business continuity. The vendor should be financially stable, with a proven track record for delivery excellence
- Vendor should have the ability to integrate software and GRC consulting and knowledge services using the GDM model

Conclusion

Corporations are struggling to manage multifaceted regulatory requirements across compliance domains, geographies and business units. Changes in regulatory requirements and associated increase in compliance costs, increased scrutiny and accountability for regulatory violations necessitate a new approach for managing enterprise-wide regulatory requirements. A unified GRC strategy enabled by enterprise GRC on SaaS model can meet the diverse requirements of GRC and provide strategic advantages from creating good, lasting governance.



Ravi Uppaladinni

*Senior Associate
Infosys Technologies Limited*

Ravi is a Senior Associate with Energy, Utilities and Services Practice of Infosys Consulting. He has over 7 years of industry and consulting experience across diverse sectors. His area of expertise is enterprise risk and compliance management. He is a Certified Information Systems Auditor (CISA), ISO 27001 Lead Implementer and Six Sigma Certified professional.




Vishakha Chhawchharia

*Senior Consultant
Infosys Technologies Limited*

Vishakha is a Senior Consultant with Infosys Software as a Service – GRC Practice. She has over 9 years of software development and consulting experience at Infosys. Her area of expertise is Enterprise Risk Management. She is a Certified Information Systems Auditor (CISA).

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> |